Development of Bring-Your-Own-Device Risk Management Model: A Case Study From a South African Organisation

Ivan Veljkovic and Adheesh Budree
University of Cape Town, Cape Town, South Africa
vljiva001@myuct.ac.za
adheesh.budree@uct.ac.za

Abstract: In recent times, many organisations have difficulties to keep up with a frequent technology changes. On the other hand, their employees continue to bring their own devices in order to access organisational information systems and data. This phenomenon is also known as Bring-Your-Own-Device (BYOD). Although a number of studies have demonstrated that the introduction of BYOD commonly has a positive effect on organisation and employees (e.g. improved optimism, job satisfaction and productivity), this concept appears as still not well understood. This particularly refers to possible risks related to the introduction of BYOD in the organisations. Hence, the intention of this study is to explore potential risks of introducing BYOD in organisations and to propose a model for addressing these risks effectively. The study began with reviewing the pertinent literature that elicited a number of the BYOD related risks that can further be classified into five groups: implementational, technological, policy and regulation, human aspects and organisational concerns. This helped in the creation of the "BYOD risk management model" as the identified risks and the proposed model were consequently tested in a middle-sized South African IT organisation, deploying exploratory case study methodology. The empirical study has corroborated the literature review findings, hence confirming that the BYOD risks identified in the researched South African organisation do not differ from those reported in the reviewed literature. The contribution of this study is seen as twofold: academic and practical. Since there is a very limited BYOD literature in a South African setting, this study added to the contextual body of knowledge on the BYOD phenomenon in general, and in the area of understanding potential risks in particular. The study also provides guidelines for the decision-makers responsible for the introduction of BYOD practice in the organisation.

Keywords: Mobility, BYOD, mobile computing, risk considerations, risk management, security

1. Introduction

The Bring Your Own Device (BYOD) concept belongs to the wider notion of mobile and cloud computing, which is described as "anytime, anywhere, from any device" (Zheng and Ni 2006, p. 19). These authors also assert that in the year 2006, smartphones appeared as a technology predominantly appropriate for corporate use. Due to the global rise of IT consumerization in recent years, BYOD has emerged and in the very short time span grown to become one of the IT industry key considerations. Hence, Keyes (2013, p. 1) highlights that adoption of BYOD phenomenon is "not a question of if. It's not even a question of when. It's a question of, will you be ready?"

Actually, many organisations worldwide are already making considerable efforts to successfully implement BYOD initiative, hence enabling employees to use the latest, predominantly mobile, information and communications technology (ICT) devices of their choice in order to access organisational resources and improve collaboration (Herrera, Ron and Rabadão, 2017). The introduction of BYOD is meant to improve employee's satisfaction and productivity as well as work-place flexibility (Gatewood, 2012; Thomson, 2012).

On the other hand, IT professionals that specialise in security are increasingly worried about the safe use of this concept. Midgley (BCS 2013, p.2) illustratively describes the security implications around the BYOD as the reason that is "causing IT managers to wake up in a cold sweat". Some of the main key concern areas are related to the technological security risks, privacy (Miller, Voas, and Hurlburt, 2012), and legal apprehensions (Osterman Research, 2012; Silvergate and Salner, 2011).

Due to the fast adoption of mobile devices in Africa, which have already overtaken both Western Europe and North America (World Wide Worx, 2012), the BYOD considerations are increasingly present in South Africa. A recent local research reported that the smartphone penetration in 2016 has passed the one-third mark in South Africa, i.e. the penetration of smartphones is between 37% – 45% (My Broadband, 2016). Due to these facts, Meeker (2015) believes that the BYOD trend will continue to rise as South Africans continue to buy the

Reference this paper: Veljkovic, I., and Budree, A., 2019. Development of Bring-Your-Own-Device Risk Management Model: Case Study From a South African Organisation. *The Electronic Journal Information Systems Evaluation,* 22(1), pp. 1-14, available online at www.ejise.com

smartphones. This is echoed by Twinomurinzi and Mawela (2014) stating that BYOD is already happening almost everywhere globally and that South Africa will also follow the suit.

However, due to a lack of understanding the risks which are related to the BYOD, many organisations are still concerned about possible threats coming together with this initiative. Furthermore, a number of authors agree that this subject is not yet sufficiently explored, hence calling for more research (Downer and Bhattacharya, 2016; Garba, Armarego, and Murray, 2015). This is particularly true in the South African context where many organisations do not have a graspable understanding regarding the risks related to BYOD initiative (Twinomurinzi and Mawela, 2014) and many BYOD vulnerabilities are still largely unmanaged (Cisco, 2014).

This study, therefore, set the aim of exploring the BYOD-related risks and devising a model that can help to manage these risks. The intention of this study was to help to bridge the theoretical gap in the subject and also help organisational decision makers to understand implications of risk by answering the question "What are the risks of introducing the BYOD in the South African organisation and what is an effective way to address identified risks?".

This introduction section is followed by the approach to this study, the BYOD elements, the BYOD risks reported in the pertinent literature and how to address these risks. Finally, testing of benefits, identified risks and the proposed BYOD risk management model, will be followed by the concluding remarks.

2. Approach to this study

This study began with the review of the pertinent literature in order to identify risks related to the introduction of the BYOD concept in an organisation. After the risks were identified, the conceptual model "BYOD risk management model" was created. In order to test the literature review findings as well as the proposed conceptual model, the case study methodology was selected as the research strategy. The choice of the methodology was based on: i) the type of research questions asked, ii) the extent of control that a researcher has over actual behavioural events and iii) the degree of focus on present day as opposed to the historical event (Yin, 1994). According to a number of similar studies (Zainal, 2007; Walsham, 1993), it was concluded that the case study methodology can satisfy all these requirements. This research was conducted as the case study of "the intensive investigation of a single unit" (Babbie and Mouton, 2002), in this case, an organisation introducing the BYOD concept.

The empirical study was conducted in a medium-sized South African IT organisation by interviewing 15 employees (purposive sampling) ranging from senior managers to technical support. According to Adler and Adler (1987), this sample is regarded as sufficient. The data is analysed and interpreted using the iterative and inductive cycles of the Interpretive Phenomenological Analysis (Smith et al., 2009).

3. The BYOD elements

The BYOD phenomenon is sometimes described through its elements of mobility, which includes mobile individuals, mobile environment, mobile equipment, mobile and cloud computing. All these elements are also important for understanding possible risks related to the BYOD concept.

Mobility refers to not being tied to a geographic location (Abowd et al., 1997) and making information available whenever it is needed (Heijden and Valiente, 2002). In the BYOD context, "organisations often provided these devices to increase the mobility and productivity of their employees" (French, Guo and Shim, 2014).

Andriessen and Vartainen (2006) define mobile individuals as individuals who are in movement, which is rather ambiguous as virtually all individuals are moving to some extent, thus this makes everybody more or less mobile. However, Mountain and MacFarlane (2007) provide a more descriptive definition by stating that mobile individuals are not only moving through space but that their information needs are more likely to be a product of their surroundings and the environment in which they interact. These mobile individuals often use their own devices for everyday job tasks.

A mobile environment means an environment in which people find themselves in motion, while they themselves are more or less stationary. 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 (Weilenmann, 2003). In the context of this study, mobile environment enables the use of BYOD.

Information Systems Audit and Control Association (ISACA) classified the following devices as essential types of mobile equipment: smartphones (Android, iPhone, Windows Phone, Blackberry, etc.); Laptops; Tablet Computers (Galaxy Tab, iPad); PDA's (Portable Digital Assistants); Phablets (a combination of smartphone and tablets). In the context of this study, equipment used within BYOD initiatives is prone to various hardware related risks (Ghosh, Gajar and Rai, 2013).

Mobile computing, the term that originates from the cellular concept found in 1947 by Don Ring of Bell Labs, 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, any time, and anywhere" (Kumar, 2011). Rouse (2007) refers to mobile computing as 'nomadic computing' while Livingston (2013) describes mobile computing as a technology that allows for the transmission of data, voice, and video via a computer or any other wireless-enabled device without having to be connected to a fixed physical link. Mobile computing is one of the driving forces behind the BYOD adoption.

Linked to mobile computing, cloud computing has emerged as the cost-efficient substitute for managing complex IT systems and, at the same time, created paradigm shift as what was comparable to the replacement of single generators from the centralised power grid (Etro, 2011; Li, Wang, Wu, Li, and Wang, 2011). With BYOD becoming increasingly popular among South African organisations, many small and medium-sized businesses are trying to take advantage of the cloud computing by consuming many cloud computing based services such as Dropbox storage, productivity app Evernote, Google e-mail or Microsoft Office 365 on their corporate mobile devices (Twinomurinzi and Mawela, 2014).

4. The BYOD risks reported in the pertinent literature

Evident benefits of the adoption of the BYOD in an organisation (e.g. mobility, efficiency and effectiveness of employees) are accompanied with certain risks that can undermine these benefits. Song (2013) claims that security is by far the biggest challenge linked to the BYOD initiatives. For example, malware attacks and data leaks may breach consistency of data and lead to absolute loss of important information (Lebek, Degirmenci and Breitner, 2013; Putri and Hovav, 2014; Berghaus and Back, 2014). The BYOD and Mobile Security Spotlight report (Information Security, 2016) confirm Song's (2013) claim by stressing that security (39%) and employee privacy (12%) are the biggest inhibitors of BYOD adoption. Yeboah-Boateng (2013) points out that risk related to security breaches can have the following adverse impact: loss of revenue, loss of corporate image, loss of investor confidence, loss of customer confidence, cost due to security breaches, cost of mitigation or possible business closure.

The reviewed literature discloses that the BYOD related risks can be classified into five categories: i) implementational, ii) technological, iii) policy and regulation, iv) human aspects and v) organisational.

The implementational risks are related to the need of managing a vast number of different devices and applications. Many organisations experience substantial challenges to ensure security, protect data and meet compliance (Reddy, 2012). Downer and Bhattacharya (2016) point out that supporting BYOD devices, while trying to achieve financial savings in overall cost of support, is another major implementational challenge for successful implementation of BYOD. The same authors also stress that another difficulty arises when workers share BYOD devices or their job encompasses many different roles as this behaviour might alter available data in unexpected ways and have a negative impact on the overall consistency of data.

According to the reviewed literature, technological risks create complexities that present the biggest challenge for the successful introduction of BYOD initiative. This challenge is likely to grow even further as according to the recent study by Symantec (2016) the number of devices purchased and used for BYOD is continually on the rise. This trend is confirmed by Statista (2017) reporting that in 2017 there are 4.77 billion users of mobile phones - also predicting that this number will rise to over five billion by 2019. The technological complexity can be illustrated by the fact that five out of six new phones are running Android, with one in seven running Apple's iPhone operating system (iOS) (Symantec, 2016).

These technological risks are further exacerbated by possibilities of infecting the BYOD devices with malware (Felt et al., 2011). According to a report by Alcatel-Lucent (2013) in 2013, approximately 11.6 million mobile devices are infected with malware globally. During the second half of 2016, the increase in smartphone infections was 83% following on the heels of a 96% increase during the first half of the year, according to Nokia's latest Mobile Threat Intelligence Report. Technological risks are also related to the intentional or unintentional installation of malicious software on BYOD devices (Tzoumas, 2013; Ahmad, 2013).

Policy and regulation risks are related to the local government laws and regulations about the organisational data that usually determines rules embedded into organisational BYOD policy (Absalom, 2012). Legislations may severely limit the reign of control that organisations have when it comes to employee personal and mobile devices. Furthermore, global organisations are required to fine-tune their BYOD policies and security for every country in which they are located, in accordance with local laws. In the case of South Africa, organisations need to identify the risk within their businesses simply because most employees use their own devices to access organisational data. Therefore, organisations need to implement the necessary security measures and policies to avoid leakage of the company data while still respecting employee privacy (IT Online, 2014). Another hurdle for local and outside organisations doing business in South Africa is the Protection of Personal Information (POPI) Act. POPI, a mechanism that intends to implement certain restrictions on how organisations and businesses handle personal data, also enables people to impose their privacy rights permanently, on a day-to-day basis. Principles behind POPI make it one of South Africa's most modern and well-founded laws, as the terms of meeting the Act ensure that for all organisations and businesses make certain that their BYOD policies and securities are sound (IT Online, 2014).

The reviewed literature, in most cases, demonstrates that employees are not aware of their personal responsibilities when it comes to the informational security of the organisation. Because of this, organisational information and relevant resources are at significant risk. These human-related risks are, according to the reviewed literature, mainly related to (i) the lack of control over data on the user devices; (ii) stolen or lost BYOD devices; and (iii) identity theft.

Organisational risks are related to the following issues: (i) inadequate user education and organisational security culture; and ii) lack of organisational policies. These risks deserve a brief elaboration.

4.1 Inadequate user education and organisational security culture

User education stems from the organisational need for employees to play a more substantive part in the general preservation of BYOD security. According to Mansfield-Devine (2012), organisations must integrate their employees into security design as employees are alleged to be the most fragile security link when implementing BYOD strategy. Along the same lines, Whitman and Mattord (2012) explicitly emphasise that a culture of organisational security will have an immense impact on the entire security perspective of the organisation. Trim and Upton (2016) support Whitman's and Mattord's view by stating that "immersing managers and their subordinates in a range of training exercises, helps to develop an 'exercise culture' in which personnel expect to be regularly tested on their crisis response skills and knowledge" (p. 2). Also, taking culture as "granted assumption" (Schein, 2010) and failure to develop appropriate security culture in an organisation can, therefore, result in a significant organisational risk when introducing the BYOD.

4.2 Lack of organisational policies

Lack of organisational policies will often expose organisations to various BYOD risks; hence, it is necessary for organisations to establish effective policies to avoid potential security breaches. According to Calder (2013), recent studies have established that 80% of respondents had more than one mobile device, while more than one third did not make use of any password or a PIN code. Therefore, permitting employees to utilise their own mobile devices for BYOD with a lack of suitable policy will unwittingly expose organisations to a significant number of BYOD risks (Calder, 2013). Moreover, several academic researchers place importance on the information and privacy security policies as an effective way to manage related concerns in organisations, including corresponding technological solutions. A clear and well-presented BYOD policy is a valuable step towards the goal of better managing privacy and security in organisations. Employees making use of BYOD should follow appropriate procedures when accessing and using sensitive organisational resources. A particularly important step when drafting organisational BYOD policies is that relevant resources such as information privacy principles, information security, and mobile and portable computing policies are consulted (Garba, Armarego, and Murray, 2015).

The above-described risks are, according to the identified categories, summarised in Table 1.

Table 1: Summarised BYOD Risks (Source: Authors)

PRIMARY RISK CATEGORY	BYOD RISK
Implementational	Protecting data, ensuring security, providing support
Technological	Malware
	Risks and vulnerabilities due to the installation of malicious software
	Cross-over threats
	Contamination of data in cloud storage
	Jailbreaking
	Compromised user accounts
	Phishing and social engineering
	Compromised network
Human aspects	Lack of control over data and devices
	Stolen or lost devices
	Identity theft
Organisational	Inadequate user education / Organisational security culture
	Lack of organisational policies (e.g. security, governance, etc.)
Legislation, regulation and privacy	POPI, ethical issues, tracking of data, breach of normal working hours, liability due to loss of organisational data, etc.

As it can be seen in the table above, technological threats represent the largest group. This is followed by human-related aspects and organisational risks, and lastly, the inadequate BYOD legislation, regulation and privacy risks, as well as implementational risks which might also be a source of concerns for many organisations.

The next step in this study was to adequately address the identified risks and offer a plausible solution, which is presented in the next section.

5. Addressing BYOD risks

Addressing the identified BYOD risks cannot be optional because if not addressed properly, all potential BYOD related benefits will diminish. In that regard, the literature review was conducted in order to identify possible useful theories and models capable of addressing the identified risks.

Frameworks such as COBIT 5, ISO 27001, NIST[1] or ENISA[2], regarded as general cybersecurity frameworks, are popular among many organisations worldwide. However, not all of these frameworks directly address the BYOD security concerns. While COBIT 5 or ISO27001 only implicitly address BYOD concerns through its section of securing mobile devices, two other frameworks explicitly declare the BYOD security.

ENISA has published a valuable set of controls and best practices for managing the risks in a BYOD programme, classifying them into three groups (Cormack, 2013):

- Governance;
- Legal, regulatory and HR; and
- Technological (device, application, user and data).

[1]US National Institute of Standards and Technology - https://www.nist.gov/
[2]European Union Agency for Network and Information Security - https://www.enisa.europa.eu/

In the European Union Agency for Network and Information Security (ENISA) guide to BYOD risk management, the focus is on the owners, not the devices. This is based on behavioural and technological controls and an owner's skills and motivation.

The US National Institute of Standards and Technology (NIST) (2016) has published a "User's Guide to Telework and Bring Your Own Device Security" which presents concrete guidelines for addressing BYOD security concerns. Accordingly, securing a device used for BYOD includes the following actions:

- Using a combination of security software, such as antivirus software, personal firewalls, spam and web content filtering, and popup blocking, to stop most attacks, particularly malware;
- Restricting who can use the PC by having a separate standard user account for each person, assigning a password to each user account, using the standard user accounts for daily use, and protecting user sessions from unauthorized physical access;
- Ensuring that updates are regularly applied to the operating system and primary applications, such as web browsers, email clients, instant messaging clients, and security software;
- Disabling unneeded networking features on the PC and configuring wireless networking securely;
- Configuring primary applications to filter content and stop other activity that is likely to be malicious;
- Installing and using only known and trusted software;
- Configuring remote access software based on the organisation's requirements and recommendations;
- Maintaining the PC's security on an ongoing basis, such as changing passwords regularly and checking the status of security software periodically (NIST 2016, p. vii).

All these recommended actions, as it was the case with the ENISA risk management elements are, in some way, related to the BYOD risks identified by this study.

5.1 The concept of security culture

According to Veiga (2010), "the information security culture is cultivated by the behaviour of employees, which is directly influenced by the information security components" (p. 5). In connection with the BYOD approach, it is imperative for organisations to agree to the right leadership and governance, suitable security policies, and security mechanism that forces the actions of employees into alignment with the organisation's culture, rendering it more security conscious (Vroom and Von Solms, 2004). Flores and Ekstedt (2016) present the well-known fact that employees are the weakest link in an organisation's defence against security threats. However, if the BYOD strategy is accompanied by an efficient security culture, more successful BYOD outcomes will be feasible for organisations. This, then, will not only assist organisations to better manage implementational, organisational and technological risks related to BYOD but also control the inappropriate use of information by employees (Santos et al., 2016).

5.2 Employee education and training

Since organisations gradually lose their grasp over the security of their BYOD devices, employees play an increasingly significant role in the general preservation of organisational security. Proper education of employees is of uttermost significance if BYOD risks – such as the ones related to BYOD implementation, various human aspects, and legislation, regulation and privacy – are to be tackled appropriately.

According to Mansfield-Devine (2012), organisations *must* integrate their staff into their overall security design. Furthermore, a 2012 international study by one of the world's leaders in firewall and network appliances, Fortinet Inc., established that for the most part, employees prefer to utilise their personal mobile devices in their organisations regardless of whether or not this is in opposition to organisational IT and security policies. Employees consider themselves, *not* the employer, liable for any device security problems. Therefore, employees are allegedly the most fragile security link; as such, organisations *must* think about an employee's needs when creating and implementing BYOD policies.

5.3 BYOD and security policies

Taking into consideration that many organisations have either a weak policy or are devoid of a policy altogether and that the problem of leakage of organisational data persists, it is undeniably necessary for organisations to develop some effective BYOD policies to assist in avoiding potential security risks caused by BYOD (Ratchford, 2017).

Due to the continuous burgeoning of BYOD, organisations – at a bare minimum – should have an official BYOD document that is understood and signed by all employees to ensure that all BYOD risks related to legislation, regulation and privacy challenges are addressed suitably. This document should not only deal with the previously mentioned risks but also grant permission for the organisation's IT support to examine each BYOD device for compliance with organisational policy (Semer, 2013). Another complex and important issue which might be of concern to organisations is the data access mechanism and 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 (Semer, 2013).

5.4 Mobile device management (MDM)

Many organisations consider a mobile device management (MDM) technology (also known as enterprise mobility management: EMM) as one of the most effective solutions for managing technological BYOD risks and securing employee devices as a central part of an organisation's BYOD management and security tactic (Semer, 2013). MDM provides organisations with a set of tools that can be utilised to secure both devices and organisational information contained on them (Ketel and Shumate, 2014). Likewise, Arregui et al. (2016) established that the MDM solution may be an efficient tactical answer for the management of many technological threats associated with BYOD, such as weak passwords, data leakage and installation of unapproved applications onto BYOD devices.

5.5 Application security approach

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 of using organisational or other practical applications on their personal 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 a BYOD strategy, security of the BYOD applications used in the organisation needs to be considered seriously, because potential BYOD technological risks arising from unsecure or malicious applications can have devastating effects (Thomson, 2012). Similarly, Baker (2013) establishes that 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 tend to hasten things along to make sure budgets and deadlines are met. However, this 'short-sighted mode' not only places organisational data and technology resources at risk but also exacerbates cost (Baker, 2013).

6. Proposing the final BYOD risk management model

The analysis of the above-portrayed models and frameworks revealed that the risks identified by this study can be addressed by a cumulative model, designed by the authors and presented in Figure 1.

The proposed BYOD risk management model suggests that addressing the identified risks should include a number of considerations. The general security frameworks (e.g. COBIT 5, NIST, ENISA) or standards (e.g. ISO 27000 series) should be considered in combustion to the organisation's approach to the IT and an overall risks management, which includes specific BYOD security models (e.g. CSVA, 2013 or Kearns, 2016).

Technological security, according to the proposed model, should be addressed by introducing the mobile device management technologies, antivirus software and firewalls, in order to identify malicious applications or the malware embedded in legitimate applications.

Having appropriate organisational cybersecurity policies, which include the BYOD related ones and the obeying security compliance is indispensable for addressing the risks identified by this study. In addition, many studies point out the employees are often the weakest cybersecurity link, hence, the education and employee training should be the major part of successfully addressing BYOD risks.

Finally, organisations striving to achieve a satisfactory level of BYOD security should closely pay attention to the development and maintenance of organisational security culture. This ranges from a visible top leadership support to the creating employees' habits of, for example, using encryption, not activating unknown links, or reporting any suspicious activities through cooperation with other employees (collective socialisation).

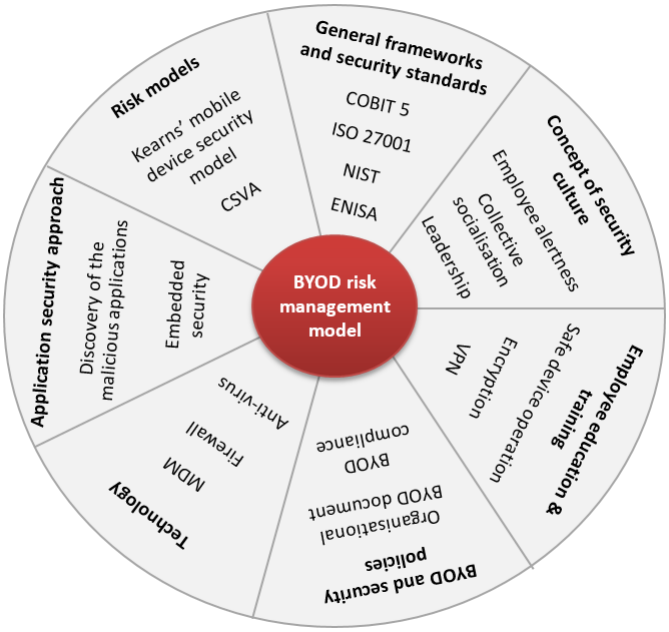

Figure 1: Proposed BYOD risk management model (Source: Authors)

7. Testing of benefits and identified risks

The empirical testing in a South African IT consulting and service management organisation started by exploring general knowledge regarding the BYOD concept and the need for that notion in the researched organisation. In that regard, all interviewees have agreed that the BYOD trend is "unstoppable" freedom of use of the personal device as it is beneficial for their organisation, which corresponds to Reddy's (2012) suggestion.

Starting with the operational BYOD benefits, a typical answer was "*Benefits, there's a lot, especially if your work in a team*". Majority of the interviewees agreed that the most common benefits are flexibility, improved job happiness and satisfaction levels, increased efficiency and productivity, better availability for additional work that needs to be done after hours, enhanced collaboration and communication, increased motivation, and convenience for employees due to fewer devices needed to be carried around. Furthermore, the interview responses were very much in line with the literature review findings regarding flexibility (Song, 2013), boosting employee productivity while increasing job satisfaction and improving creativity (Wood, 2012), speeding up adoption of technology (Calder, 2013) and employees covering for the cost of hardware (Citrix, 2013; Keys, 2013).

Depending on the position within the company, the interviewees' viewpoints varied slightly, however, all have strongly agreed with the existence of BYOD risks elicited from the literature review. The biggest shared concern of all interviewees was related to the technological risks. Malware risks (mentioned in literature by, for example, Felt et al*.,* 2011; Alcatel-Lucent, (2013), risks and vulnerabilities due to installation of malicious software (e.g. Gowda, 2013), cross-over threats (Symantec, 2016), contamination of data kept in cloud storage (e.g. Amoroso, 2013), jailbreaking (e.g. Symantec, 2016), compromised user accounts (e.g. Astani, Ready and Tessema, 2013), and compromised network (Dimitriou and Krontiris, 2016) were the main technological risks mentioned by the interviewees.

Next, the phishing and social engineering, which most frequently use email to deceive users, were also classified by interviewees as technological risk, although they admit that these threats are also closely linked

to the human aspect of BYOD related risks. These risks are very much presented in the reviewed literature (e.g. Dodge, Carver and Ferguson, 2007; Symantec, 2016).

Government laws and compliance requirements (Absalom, 2012) force organisations to consider relevant risks and prevent leakage of the company data while still respecting employee privacy (IT Online, 2014). The interviewees have particularly pointed to the importance of complying with the South African Protection of Personal Information (POPI) Act. Additionally, all interviewees agree that the breach of privacy can have a negative psychological impact on employees utilising the BYOD with regards to their behaviour and acceptance of policy controls – as mentioned by Garba, Armarego, and Murray (2015).

Following typical answers that "*data leakage is the biggest concern*" as "*hackers and theft can happen, especially if you are out of the organisation and you are working in the mall for the example"*, we ranked this human-related BYOD risks as a top priority by all interviewees. The interviewees particularly voiced concerns regarding the data linkage while using open, unsecured wireless networks. This strictly corresponds to the literature review found, which points out that data leakage or loss was a concern of 72% respondents in The BYOD and Mobile Security Spotlight report (Information Security, 2016).

Disscussing the possibility of losing the mobile device that will perhaps never be recovered (EY, 2013), was not a simple concern for the interviewees but, as explained, was tightly related to the possibility of the identity theft. This also corresponds to the literature review finding stating that the identity theft is a major threat to many organisations and their clients (Kahn and Liñares-Zegarra, 2016).

Inadequate users' education and training regarding specific BYOD risks were confirmed as one of the top organisational risks. *"I am not sure if there is anything yet"* was the typical response of one of the interviewees. Leavitt (2013) claims that employees, who are deprived of suitable knowledge on BYOD, may execute actions that are deemed insecure while being completely unaware that they expose their organisation to risk. Whitman and Mattord (2012) claim that the employee's education was of the highest importance for organisations as, by supplying training, they producing awareness, and essentially creating a security culture. Hence, it was no surprise to hear from the interviewees that creating cyberculture is important as organisations with low or no cyberculture at all are at high risk.

The interviewees particularly pointed out the importance of haven and adhering to the security policies and procedures (Cisco, 2013). All the above clearly corresponds to the 'best practice', which advises that the organisational culture can be effectively fostered through education and training (Whitman and Mattord, 2012). In the context of the organisational risks, the interviewees also agreed with the literature finding that the lack of appropriate organisational policies, procedure or governance, can jeopardise BYOD security (Calder, 2013).

Legislation, regulation and privacy were also of the interviewee's concerns but not only as the organisational risks. They clearly pointed out that the use of the Mobile Device Management (MDM) technologies can impact on their privacy: "*So, to use your mobile phone at work, on the network at my company you have to install the program that will watch everything you do, and you have to sign the disclaimer that they can see everything you do*". However, a vast majority of the interviewees have agreed the lack of legislation and regulations can impose risks of the organisations that have introduced the BYOD practice. Garba, Armarego and Murray (2015) establish that if BYOD issues related to legislation, regulation and privacy risks are not managed properly, they can have a negative psychological impact on employees utilising the BYOD and force them to refuse acceptance of the policy controls.

Implementational risks were, surprisingly, found not to be the highest concerns in the researched organisation as these risks were deemed as important to five out of fifteen interviewees. The biggest implementational concern was linked to the number of different devices to be supported: *"So to support so many different devices there are so many variables".* Indeed, Reddy (2012) confirms that, with inadequate control over BYOD devices, many organisations experience substantial challenges for ensuring security, protecting data and meeting compliance regulations.

The tabular view of the perceived criticality to each BYOD risk category, is given in Table 2 below:

Table 2: Summary of categorised BYOD risks with the information from interviews (Source: Authors)

PRIMARY RISK CATEGORY	BYOD RISKS FROM THE LITERATURE REVIEW	BYOD RISKS IDENTIFIED DURING INTERVIEWS	PERCIEVED CRITICALITY OF IDENTIFIED RISKS
Implementational	Protecting data, ensuring security, providing support	YES	LOW (5)
Technological	Malware	YES	HIGH (13)
	Risks and vulnerabilities due to installation of malicious software	YES	HIGH (13)
	Cross-over threats	YES	HIGH (13)
	Contamination of data kept in cloud storage	NO	N/A
	Jailbreaking	NO	N/A
	Compromised user accounts	YES	HIGH (13)
	Phishing and social engineering	YES	HIGH (13)
	Compromised network	YES	HIGH (13)
Human aspects	Lack of control over data and devices	YES	MEDIUM (8)
	Stolen or lost devices	YES	MEDIUM (8)
	Identity theft	YES	MEDIUM (8)
Organisational	Inadequate user education / Organisational security culture	YES	LOW (5)
	Lack of organisational polices (e.g. security, governance, etc.)	YES	LOW (5)
Legislation, regulation and privacy	POPI, ethical issues, tracking of data, breach of normal working hours, liability due to loss of organisational data, etc.	YES	MEDIUM (7)

8. Testing the proposed BYOD risk management model

The proposed BYOD risk management model (Figure 1) was tested in order to establish an optimal approach to addressing the BYOD related risks. The elements of this model were used for posing the interview questions as well as for analysing interviewee's answers and eliciting appropriate themes.

Eight out of fifteen interviewees were unsure if the researched organisation uses any risk compliance frameworks, whereas a further six interviewees were quite confident that the organisation does not have or utilise any. This has confirmed the need of having an appropriate framework but also that it has to be explained and communicated to the employees. This also confirms findings of Twinomurinzi and Mawela (2014) who ascertain that organisations seem reluctant to formally develop BYOD strategies which leave them open to many risks.

It has been empirically confirmed that the identified technological threats can be resolved by deploying the MDM management solution, including additional MDM components such as anti-virus, VPN and data encryption (e.g. Bertino, 2016). Here it is important to mention that the technological risks of "jailbreaking" and "contamination of data in cloud storage" are not definitely confirmed by the interviewees, as some of them were not sufficiently familiar with these risks.

The human aspects of BYOD risk considerations, according to the interviewees' answers, should be addressed by combining certain features from previously mentioned MDM technology (e.g. GPS tracking or remote wipe, for example) with the further development of organisational security culture. The importance of the later was confirmed by Cisco (2013), Whitman and Mattord (2012) and Trim and Upton (2016).

There was strong agreement amongst most interviewees that their organisation has widespread awareness and a security culture, which is a bit of paradox considering that the researched organisation does not appear to have a BYOD or security policy or risk compliance frameworks. This, however, confirms the importance of this element of the proposed model.

The legislation, regulation and privacy risks can be handled by implementing the necessary technological solutions (e.g. MDM and additional components), BYOD and other specially tailored organisational policies (e.g. employee and privacy) to avoid leakage of company data and still respect employee privacy and work

agreements (e.g. Culnan and Williams, 2009; Heimerl, 2012). According to the proposed model, organisational aspects of BYOD security should be addressed by introducing appropriate policies including mandatory education and training of all employees (e.g. Calder, 2013).

When questioned if the researched organisation provides employees with education and training on BYOD, the overwhelming majority of interviewees answered negatively, adding that it can lead to many BYOD risks. Hence, the education and training were confirmed as an important element of the proposed model. This complements findings of Whitman and Mattord (2012) who claim that employee education was the reason for significant differentiation, one that is best circulated through the organisation by supplying training, producing awareness, and essentially creating a security culture.

Lastly, as implementational risks are multifaceted, the interviewees agreed that all elements of the proposed model can be applied as needed and as appropriate.

All the above-discussed practices and activities are aimed at preventing losses possibly caused by BYOD-related risks and the empirical testing has confirmed that the phased approach, (e.g. Yeboah-Boateng, 2013) shown in Figure 2 below, is also appropriate for addressing BYOD-related risks.

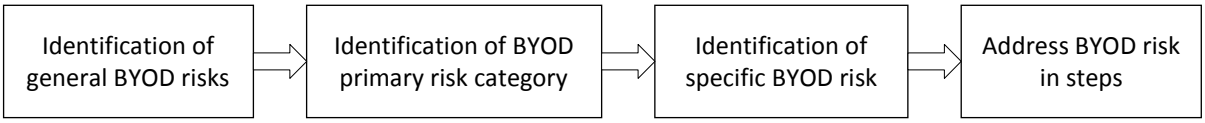

Figure 2. The phased approach to BYOD risk management (source: Authors)

As a final insight, it is relevant to mention that even though the majority of interviewees confirmed that their organisation does not properly utilise the most important mechanisms for managing risks related to BYOD – such as apposite policies, risk and compliance frameworks, education/training on BYOD – they remained confident that their company is doing enough to protect them as employees and the entire organisation. Nevertheless, after all, interviews were completed and all interviewees had a better understanding of the numerous identified BYOD risk gaps in their organisation, some of them expressed open concerns and thanked the researchers for helping them be more aware of possible risks related to the introduction of BYOD in their organisation.

9. Final words

To conclude, this research has established that the successful utilisation of the BYOD phenomenon does not come free of challenges; there is no single 'silver bullet' or universal remedy that will solve all the risks and concerns related to this phenomenon. Hence, introducing appropriate BYOD (e.g. security) and other specifically tailored organisational policies (e.g. employee, privacy) can increase not only overall BYOD security but also the satisfaction and privacy of employees, thereby minimising the overall risk for the organisation. As seen from interviewee responses, it also important that these organisational aspects of BYOD risks are addressed by introducing mandatory BYOD education and training of all employees to further improve the overall organisational security culture and employee confidence in BYOD security mechanisms (e.g. MDM). Likewise, it is recommended that organisations, at a bare minimum, have an official acceptable BYOD usage document understood and signed by all employees to make certain that all BYOD risks related to legislation, regulation and privacy challenges are adequately and suitably addressed. Along with these policies, documents, education and training of employees is imperative for complementing technological solutions: for instance, MDM and its additional components (e.g. anti-virus, VPN, data encryption) and comprehensive BYOD risk management frameworks or models (such as the one proposed in this research) to help organisations mitigate potential risks related to BYOD in an organisation.

In the end, it is worthy of noting that the researched South African organisation can be protected by applying the 'best practice' found in the reviewed literature.

This research has some limitations, primarily seen in the limited sample and a single studied organisation. As BYOD practice is still relatively new in South Africa, it was no surprise that this research established that not much work has been done locally regarding the BYOD risks related phenomenon. Moreover, taking into

consideration limited South African literature on the subject of the BYOD risks, further research is highly recommended. Having in mind the limited sample size in this research, it is suggested that the further studies are performed using a larger sample from different organisations in order to increase the generalisability of the further studies.

References

Abowd, G., Atkeson, C.G., Hong, J., Long, S., Kooper, R., and Pinkerton M. 1997. Cyberguide: A mobile context-aware tour guide, *Wireless Networks*, 3(5), pp. 421-433.

Absalom, R. 2012. International Data Privacy Legislation Review: A guide for BYOD policies. *Ovum*, 1, pp. 1-23.

Adler, P.A., and Adler, P. 1987. *Membership Roles in Field Research*. Newbury Park, CA: Sage.

Ahmad, A. 2013. *"Information Security Risk Management",*[pdf] Information Systems Security Consulting lecture on 6 July 2013, University of Melbourne, Parkville. Online] Available at: https://minerva-access.unimelb.edu.au/bitstream/handle/11343/33345/300314_2013_Tan_Risk.pdf?sequence=1andisAllowed=y [Accessed 21 April 2018]

Alcatel-Lucent. 2013. Kindsight Security Labs: Malware Report - Q4 2013. [pdf] [Online] Available at: http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf [Accessed 10 April 2018]

Amoroso, EG. 2013. From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud. Security and Privacy, *IEEE*, 1, pp. 23-31.

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

Arregui, D. A., Maynard, S. B., and Ahmad, A. 2016. *Mitigating BYOD Information Security Risks*.

Astani, M., Ready, K., and Tessema, M. 2013. BYOD Issues and Strategies in Organisations. Issues in Information Systems, 14(2), pp. 195–201.

Babbie, E., and Mouton, J. 2002. *The practice of social research*. Cape Town: Oxford University Press.

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

BCS. 2013. Bring Your Own Device - The Mobile Computing Challenge, BCS, The Chartered Institute for IT. [pdf] [Online] Available at: http://www.bcs.org/upload/pdf/bring-you-own-device-the-mobile-computing-challenge.pdf [Accessed 28 March 2018]

Berghaus, S., and Back, A. 2014. Adoption of Mobile Business Solutions and its Impact on Organizational Stakeholders, 27th Bled eConference eEcosystems, June 1 - 5, 2014; Bled, Slovenia. [pdf] [Online] Available at: https://www.alexandria.unisg.ch/232052/1/04_Berghaus_Back.pdf [Accessed 21 April 2018]

Bertino, E. 2016. Securing mobile applications. Computer, 49(2), p. 9

Calder, A. 2013. Is the BYOD Movement Worth the Risks?, *Credit Control*, 65.

Cisco. 2014. Cisco South African BYOD research highlights that many organisations in South Africa are still vulnerable when it comes to security [Press release] [Online]. Available at: http://www.cisco.com/web/ZA/press/2014/082514.html [Accessed 22 March 2018]

Citrix. 2012. Workplace of the Future : a global market research report. [pdf] [Online] Available at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf [Accessed 11 March 2018]

Cormack, A. 2013. ENISA Guide to Risk Mitigation for BYOD. [Online] Available at: https://community.jisc.ac.uk/blogs/regulatory-developments/article/enisa-guide- risk-mitigation-byod [Accessed 11 March 2018]

Culnan, M. J., and Williams, C. C. 2009. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, 33(4), pp. 673-687.

Dimitriou, T., and Krontiris, I. 2006. Secure in-network processing in sensor networks. *Security in Sensor Networks*, pp. 275–290.

Dodge, R. C., Carver, C., and Ferguson, A. J. 2007. Phishing for user security awareness. *Computers and Security*, 26(1), pp. 73-80.

Downer, K., and Bhattacharya, M. 2016. BYOD Security : A New Business Challenge. [Online] Available at: https://www.academia.edu/20071329/BYOD_Security_A_New_Business_Challenge [Accessed 22 March 2018]

Etro, F. 2011. The economics of cloud computing. *IUP Journal of Managerial Economics*, 9(2), pp. 7–22.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. 2011. A survey of mobile malware in the wild. Paper presented at the Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. [pdf] [Online] Available at: https://mfinifter.github.io/papers/mobilemalware.pdf [Accessed 21 April 2018]

Flores, W. R., and Ekstedt, M. 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, 59, pp. 26-44.

Fortinet. 2012. Fortinet Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems. [Online] Available at:http://investor.fortinet.com/releasedetail.cfm?releaseid=684183 [Accessed 15 April 2018]

French, A. M., Guo, C., and Shim, J. P. 2014. Current Status, Issues, and Future of Bring Your Own Device (BYOD). *CAIS*, 35, p. 10.

Garba, A. B., Armarego, J., and Murray, D. 2015. Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences*, 10(3), pp. 1279–1287.

Gatewood, B. 2012. The Nuts and Bolts of Making BYOD Work, *Information Management Journal*, 46 (6), pp. 26-30.

Ghosh, A., Gajar, P. K., and Rai, S. 2013. Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4), pp. 62-70.

Gowda, M. 2013. BYOD Security: What is Android fragmentation and how does it affect Enterprise Security and why agentless makes super sense?, Agentless BYOD Discovery and Control.[Online] Available at: http://i7nw.com/byod-security-android-fragmentation [Accessed 7 March 2018]

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.

Heimerl, J. L. 2012. The Evolution of Information Security. [Online]Available at: http://www.securityweek.com/evolution-information-security [Accessed 7 April 2018]

Herrera, A. V., Ron, M., and Rabadão, C. 2017. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. *In Information Systems and Technologies* (CISTI), 2017 12th Iberian Conference on (pp. 1-4). IEEE. doi: 10.23919/CISTI.2017.7975953

IT Online. 2014. Popi and BYOD. Available at: http://it-IT Online online.co.za/2014/12/03/popi-byod/ [Accessed 15 April 2018]

Information Security. 2016. BYOD and Mobile Security Spotlight Report, Information Security LinkedIn Group [Online] Available at: http://crowdresearchpartners.com/portfolio/byod-mobile-security-report/ [Accessed 5 April 2018]

Kahn, C. M., and Liñares-Zegarra, J. M. 2016. Identity Theft and Consumer Payment Choice: Does Security Really Matter?. *Journal of Financial Services Research*, 50(1), pp. 121-159.

Kearns, G.S. (2016). Countering mobile device threats: A mobile device security model. *Journal of. Forensic and Investigative Accounting,* 8(1), 36-48

Ketel, M., and Shumate, T. 2015. "Bring Your Own Device: Security Technologies", *SoutheastCon*, pp. 1-7.

Keyes, J. 2013. *Bring your own devices (BYOD) survival guide*. CRC press.

Kumar, R. Siva. 2011. Paper Presentation on Mobile Computing. [Online] Available at: http://www.scribd.com/doc/48271633/4-mobile-computing [Accessed 7 April 2018]

Leavitt, N. 2013. Today's Mobile Security Requires a New Approach, *Computer*[e-journal] 46, pp. 16-19. DOI http://dx.doi.org/10.1109/MC.2013.400

Lebek, B., Degirmenci, K., and 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. [pdf] [Online] Available at: https://www.iwi.uni-hannover.de/fileadmin/wirtschaftsinformatik/Publikationen/AMCIS_2013_BL_KD_MHB__1521_best_paper.pdf [Accessed 21 April 2018]

Li, Q., Wang, C., Wu, J., Li, J., and Wang, Z.-Y. 2011. Towards the business-information technology alignment in cloud computing environment: An approach based on collaboration points and agents. *International Journal of Computer Integrated Manufacturing*, 24(11), pp. 1038–1057.

Livingston, D. (2013). "Introduction and History of Mobile Computing."Slideshare. Linkedin Corporation.

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

Mountain, D., and MacFarlane, A. 2007. Geographic information retrieval in a mobile environment: evaluating the needs of mobile individuals. *Journal of Information Science* [e-journal] 33(5), pp. 515-530. doi: 10.1177/0165551506075333

My Broadband. 2016. Smartphone penetration in South Africa hits a major milestone. [Online] Available at: https://mybroadband.co.za/news/smartphones/180894-smartphone-penetration-in-south-africa-hits-major-milestone.html [Accessed 22 March 2018]

NIST. 2016. *User's Guide to Telework and Bring Your Own Device (BYOD) Security*. US National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-114r1

Putri, F., and 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. [pdf] [Online] Available at: https://pdfs.semanticscholar.org/dda4/b87f14e3004dca56f727f6669c030fecf88f.pdf [Accessed 21 April 2018]

Ratchford, M. M. 2017. BYOD: A Security Policy Evaluation Model. *In Information Technology-New Generations,* Springer, Cham. pp. 215-220.

Reddy, A. S. 2012. Making BYOD Work for Your Organization. Future of Work, pp. 1–16. [Online] Available at: https://www.slideshare.net/cognizant/making-byod-work-for-your-organization-13450463 [Accessed 22 March 2018]

Rouse, M. 2007. *Nomadic computing.* Mobile computing.

Santos-Olmo, A., Sánchez, L. E., Caballero, I., Camacho, S., and Fernandez-Medina, E. 2016. The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets. *Future Internet*, 8(3), p. 30.

Schein, E. H. 2010. *Organizational culture and leadership (Vol. 2)*. John Wiley and Sons.

Semer L. 2013. Auditing the BYOD Program, *Internal Audit*, February, 70(1), pp. 23-27.

Smith, J. A., Flowers, P., and Larkin, M. 2009. Interpretative Phenomenological Analysis: theory, method and research. *UK: Sage Publishers*.

Song, I. 2013. Driving Business Value with BYOD and Research Contents Developing an Enterprise Mobility Framework, (June). [Online] Available at: http://enterprise.huawei.com/ilink/cnenterprise/download/HW_280603 [Accessed 7 April 2018]

Symantec. 2016. Internet Security Threat Report, Symantec. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [Accessed 8 April 2018]

Thomson, G. 2012. Feature: BYOD: enabling the chaos, *Network Security*, 2012(2), pp. 5-8.

Trim, P., and Upton, D. 2016. *Cyber security culture: Counteracting cyber threats through organizational learning and training.* Routledge.

Twinomurinzi, H., and Mawela, T. 2014. Employee perceptions of BYOD in South Africa: Employers are turning a blind eye?, *Saicsit*, pp. 1–6.

Tzoumas, C. 2013. The BYOD World. *Business West*, 30, pp. 45.

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

Vroom, C., and Von Solms, R. 2004. Towards information security behavioural compliance. *Computers and Security*, 23(3), pp. 191-198.

Walsham, G. 1993. *Interpreting information systems in organizations.* John Wiley and Sons, Inc.

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

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

World Wide Worx. 2012. Internet Matters. [Online] Available at: http://led.co.za/sites/default/files/cabinet/orgnameraw/document/2012/za_internet_matters_final.pdf [Accessed 8 March 2018]

Wood, A. 2012. BYOD: The Pros and Cons for End Users and the Business, *Credit Control*, 33(7/8), p. 68.

Yeboah-Boateng, E. O. 2013. Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, *Integrity and Availability* (CIA). (1 ed.) Institut for Elektroniske Systemer, Aalborg Universitet.

Yin, R. K. 1994. *Case study research: Design and methods (2nd ed.).* Newbury Park, CA: Sage Publications.

Zainal, Z. 2007. *Case study as a research method.* Jurnal Kemanusiaan, 9.

Zheng, P., and Ni, L. 2006. *Smart phone and next generation mobile computing,* San Francisco. Morgan Kaufmann,