BYOD: Risk considerations in a South African organisation

MASTER'S THESIS

Prepared by: Ivan Veljkovic

VLJIVA001 (vljiva001@myuct.ac.za)

SUBMITTED TO THE UNIVERSITY OF CAPE TOWN

In fulfilment of the requirements for the degree

MCom in Information Systems

INF5000W

Supervisor: Dr Adheesh Budree

Department of Information Systems

Faculty of Commerce, University of Cape Town

15th of December 2017

ABSTRACT

In recent times, while numerous organisations have difficulty keeping abreast with the frequent year-on-year technology changes, their employees on the other hand, continue to bring their personal devices to work to more readily access organisational data. This concept is known as Bring Your Own Device (BYOD). Studies have demonstrated that the introduction of BYOD commonly has a positive effect on both organisation and employees: increased optimism, job satisfaction and productivity are some of the perceived positive effects. Furthermore, BYOD can improve employees' opportunities for mobile working and assist with the work flexibility they seek.

This phenomenon, however, is still not well understood. In the South African context, this refers particularly to an inadequate understanding of risks associated with the introduction of BYOD into organisations. Some of the risks associated with this phenomenon are, for instance, related to information security, legislation and privacy issues. Hence, the intention of this research was to investigate, determine and assess BYOD risk considerations in a South African organisation.

Using the available literature on this subject and an interpretative exploratory case study approach, this research explored various facets of BYOD-related risks (e.g. implementational, technological, legislation, regulation and privacy risks, human aspects and organisational concerns) as well as the impact these risks may have on both employees and an organisation. The organisation under investigation – from this point onward referred to as "Organisation A" – is a South African based information technology (IT) security consulting and service management organisation, which has seen increased expansion in its business and thus an increase in the number of its employees utilising their personal devices at the workplace.

Even so, Organisation A was uncertain regarding possible risks that might hinder benefits of BYOD. Hence, this researcher defined the main research question as "*What are the risks of introducing the BYOD in the South African organisation and*

what is an effective approach to address identified risks?". The main objective was to identify and describe BYOD-related risks and to propose an appropriate model for addressing these risks.

To answer the main research question, this researcher reviewed the applicable literature on the BYOD, including the limited South African literature pertaining to the subject. The review elicited the most common BYOD-related risks but also some models, frameworks and standards that may be applied for addressing these risks. Based on these revelations, an applicable BYOD risk management model was created and proposed.

The literature review findings were subsequently tested in the empirical setting (in Organisation A) by conducting comprehensive interviews with research participants. This research adopted a qualitative approach in general and a case study methodology in particular. The collected data were analysed using the interpretative phenomenological analysis (IPA), which aided in providing a comprehensive understanding of the interviewees' responses regarding the BYOD risks. The interviewees were selected based on a purposeful (pre-defined) sampling.

The results of this interpretative research suggest that the interviewees' responses are closely aligned with the information on BYOD risks collected from the pertinent literature. The results show that successful introduction and usage of BYOD in the studied organisation requires the implementation of mixed risk management measures: technological (e.g. mobile device management and its additional components), non-technological (e.g. IT or BYOD security policies), the usage of general risk management frameworks (e.g. ISO 27001), the development of an organisational security culture and skilling of the human factor (e.g. employee awareness, training and education, for example). Additionally, it was found that participation of employees in the development of BYOD policies is an essential and effective tactic for transforming a fragile BYOD risk link (i.e. employees) into a strong risk prevention mechanism. Furthermore, this research also revealed that in the South African context, it is important that an organisation's BYOD security policies are sound, preferably meeting the POPI Act requirements and thereby avoiding legislation risks.

The contribution of this research is twofold: first academic, and second, practical. The academic contribution is realised by adding to the body of knowledge on the BYOD risks – most particularly in terms of understanding potential risks when introducing BYOD in the South African context. The practical contribution manifests through the provision of detailed risk considerations and mitigation guidelines for organisations wishing to introduce BYOD practices or considering ways to improve their current BYOD risk management strategy.

It is acknowledged that this research has some limitations, particularly in regard to the limited generalisation of the findings due to the limited sample provided by only one organisation. Although the results are not necessarily applicable to other South African organisations, these limitations did not impact the relevance and validity of this research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

4G	Fourth Generation Broadband Cellular Network Technology
BYOD	Bring Your Own Device
CSVA	Cyber-Security Vulnerabilities Assessment
EMM	Enterprise Mobility Management
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
ICT	Information Communications Technology
iOS	iPhone Operating System
IPA	Interpretative Phenomenological Analysis
IS	Information Systems
ISACA	Information Systems Audit and Control Association
IT	Information Technology
Mac	Macintosh
MDM	Mobile Device Management
MDSM	Mobile Device Security Model
NFC	Near Field Communication
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
POPI	Protection of Personal Information Act
RFID	Radio frequency identification
SME	Small and Medium Enterprises
SMS	Short Message Service
US	United States
USB	Universal Serial Bus
VPN	Virtual Private Network

DECLARATION

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this thesis “BYOD: Risk considerations in South African organisation” from the work(s) of other people has been attributed, and has been cited and referenced.
3. This thesis “BYOD: Risk considerations in South African organisation” is my own work.
4. I have not allowed, and will not allow, anyone, to copy my work with the intention of passing it off as his or her own work.

Signature: Signed by candidate …….. **Date**: 15/12/2017

Full Name of Student: Ivan Veljkovic

Student Number: VLJIVA001

PROOFREADING CONFIRMATION

Proofreading of Master's Dissertation

30th December 2017
Dr Laura Kleinhans
ChickPea Editing and Proofreading

I, Dr Laura Kleinhans, certify that I have completed the proofreading and correction of the dissertation, **BYOD: Risk considerations in South African organisation** by **Ivan Veljkovic**, submitted in fulfilment of the requirements for the degree **MCom** in Information Systems, **Faculty of Commerce** at the **University of Cape Town.**

My own credentials are as follows: I received a BA in English from North Central College in 1988, an MA in English from Salisbury State University in 1990, and a PhD in English from Northern Illinois University in 1998. I completed a 120-hour TEFL course in 2017. I have been teaching university and high school English in the USA, South Africa and Saudi Arabia for 27 years.

I am currently a high school English teacher at Multinational School in Riyadh, Saudi Arabia. I have also been formally editing and proofreading online since 2010, running ChickPea Editing and Proofreading and assisting over 100 graduate students throughout South Africa and Europe with their dissertation editing.

I believe that this dissertation meets with the grammatical and linguistic requirements for a document of this nature.

Yours faithfully,

Dr. Laura Kleinhans

Dr Laura Kleinhans (BA, MA, PhD, TEFL)

084 618 2095
laurakleinhans1@gmail.com
ChickPea Proofreading & Editing

Certificate of Authenticity

CERTIFICATE: COA0812(IV)

30 December 2017

To Whom It May Concern

This is to certify that "BYOD: Risk Considerations in a South African Organisation" by IVAN VELJKOVIC for the **University of Cape Town** has been professionally edited by Dr Laura Kleinhans of ChickPea Proofreading and Editing Services for Students and Professionals.

Document:

Job Number	Document title
CP 0812(IV)	BYOD: Risk considerations in a South African organisation

Dr. Laura Kleinhans
CEO ChickPea

ChickPea Proofreading and Editing

ACKNOWLEDGEMENTS

A wholehearted ‘thank you’:

- To my supervisor, Dr Adheesh Budree, for his guidance, support and availability whenever needed;
- To my research participants, for their willingness to be involved and provide valuable contributions to this research;
- To my dear friends, for their continuous and unconditional support, trust and understanding;
- To my family, and most of all, my loving wife, Ivana Veljkovic, for always being supportive and believing in me; and
- To my son, Aleksandar Veljkovic, for giving me the strength and graciously allowing me the time to complete this thesis.

CHAPTER 1: INTRODUCTION AND OVERVIEW

This chapter outlines the background, problem statement, main research question and sub-questions, research objectives, research design and methodology, ethical considerations, scope, limitations and finally, the contribution of this research.

1.1 Background

Zheng and Ni (2006) describe the concept of mobile and cloud computing as “anytime, anywhere, from any device” (p. 19). These researchers further assert that in 2006, smartphones appeared as a technology predominantly appropriate for corporate usage. More recently, though, unlike in 2006 where employees previously requested permission of their organisation to buy a new computer or software, employees are now buying these themselves, often bypassing organisational and information technology (IT) departmental regulations entirely; from smartphones to computers, from tablets to any number of software applications, employees have tasted their digital freedom and are enjoying it (Keyes, 2013).

Due to the global rise of IT consumerization in recent years, a new phenomenon, Bring Your Own Device (BYOD), has emerged and in a very short time span, escalated to become one of the primary IT industry subjects undergoing intense study. BYOD refers to employees bringing their personal devices to use for computing in the workplace (Webopedia.com, 2017). In that regard, Keyes (2013) highlights that adoption of BYOD is "Not a question of *if*. It’s not even a question of *when*. It’s a question of, will you be ready?" (p. 1).

Numerous global organisations are already making considerable efforts to successfully implement BYOD strategy, enabling employees to use the latest, predominantly mobile, information and communication technology (ICT) devices of their choice to readily access organisational resources (Herrera, Ron & Rabadão, 2017). These actions, it is thought, ought to improve employee satisfaction, collaboration, productivity and workplace flexibility (Gatewood, 2012; Thomson, 2012). However, Midgley (BCS, 2013) ascertains about the BYOD that:

> IT professionals are wary of it, end users are embracing it and vendors are trying to market it. It's a subject that's dividing opinion, with the security implications alone causing IT managers to wake up in a cold sweat (p. 2).

The previous statement illustrates that regardless of the benefits linked to the BYOD phenomenon, main concerns are related to security implications such as technological risks. BYOD can also create privacy (Miller, Voas, & Hurlburt, 2012) and legal uncertainties (Osterman Research, 2012; Silvergate & Salner, 2011) for both organisations and employees. Nevertheless, Thomson (2012) openly calls for IT organisations to embrace the BYOD phenomenon and adopt a perspective of accepted risk.

As far as the popularity of mobile technologies in South Africa is concerned, a study by the World Wide Worx (2012) established that "on 30 September 2011, the African continent became the world's second-biggest region for cellphone use, reaching 616 million users and overtaking both Western Europe and North America" (p. 1). Likewise, recent research also reports that the smartphone penetration in 2016 has passed the one-third mark in South Africa: the penetration of smartphones locally is between 37% - 45% (My Broadband, 2016).

When it comes to the BYOD phenomenon, Twinomurinzi and Mawela (2014) explain that BYOD is already happening almost everywhere globally and that South Africa is expected to follow suit. Furthermore, Meeker (2015) establishes that in South Africa, the BYOD trend appears to be rising gradually and is expected to continue as the number of smartphones increases even further and employees progressively utilise them in a workplace. However, taking into consideration the previously stated and that there is a strong awareness of the BYOD concept among South African employees (Twinomurinzi & Mawela, 2014), local organisations seem to have many concerns related to the introduction of BYOD (Gustav & Kabanda, 2016) that renders them hesitant to adopt and formally develop BYOD strategies (Irons & Ophoff, 2016). As a result, though, they remain open to many risks.

1.2 Problem statement

Despite the promising significance of embracing the BYOD phenomenon, a detailed literature review of the risks surrounding BYOD, including the limited South African literature (cited in this thesis) together with the published international literature, suggests that many organisations have lingering concerns about potential risks inherent in this phenomenon, grounded in a lack of awareness and understanding. Furthermore, the reviewed literature shows that "very little has been done" by researchers to address this challenge appropriately and comprehensively (Olalere, Abdullah, Mahmod & Abdullah, 2015). Besides, a number of authors (e.g. Downer & Bhattacharya, 2016; Garba, Armarego, & Murray, 2015a) agree that the topic of risk surrounding the BYOD phenomenon requires further and more focused research. This is particularly true in the South African context where many organisations do not have a thorough understanding regarding the risks related to BYOD (Twinomurinzi & Mawela, 2014); consequently, many vulnerabilities related to this phenomenon remain largely unmanaged (Cisco, 2014). This likely explains why South African organisations are reluctant to formally develop organisational BYOD strategies (Irons & Ophoff, 2016) and still have many BYOD adoption concerns (Gustav & Kabanda, 2016).

1.3 Research questions

In accordance with the identified problem, the main research question was delineated as follows:

What are the risks of introducing BYOD in a South African organisation and what is an effective approach to address identified risks?

To adequately determine the answer to the above questions, it is important to consider these sub-questions:

1. What is the nature of the BYOD phenomenon?
2. Why organisations consider BYOD?
3. What risks are associated with the introduction of BYOD?
4. What is the nature of these risks?

5. What is an optimal approach to manage these risks?

1.4 Research objectives

The main objective of this research was to explore risks introduced by BYOD in a South African organisation and to propose an effective approach for managing these risks. To achieve the main objective, the following sub-objectives were established:

1. To explore the nature of BYOD phenomenon;
2. To identify why organisations consider BYOD;
3. To recognise risks associated with the introduction of BYOD;
4. To explore the nature of these risks; and
5. To suggest an optimal approach for managing these risks.

1.5 Research design and methodology

Researchers dealing with information systems (IS) related research may employ different philosophical perspectives to study a specific information system phenomenon (Orlikowski & Baroudi, 1991). As stated by Khosrow-Pour (2008), *philosophy* can be defined as "the critical examination of the grounds for fundamental beliefs and an analysis of the basic concepts employed in the expression of such beliefs" (p. 809). Furthermore, Chua (1986) established that there are "three sets of beliefs which delineate a way of seeing and researching the world: i) beliefs pertains to the notion of knowledge; ii) assumptions about the object of study; and iii) assumptions made about the relationship between knowledge and the empirical world" (p. 604-605). Assumptions about the empirical world are classified as *ontological*. In order to perform an information systems research, positivist, interpretive and critical research philosophies are utilised that are composed from different views of the world and research perspectives accepted by the researchers (Orlikowski & Baroudi, 1991).

The philosophical approach applied in this research was phenomenology and hermeneutics, reflecting its interpretative character (Abulad, 2007) because the aim of this researcher was to understand people's perceptions of the risk introduced by the BYOD phenomenon in a South African organisation. Hermeneutics was selected as the method of interpretation since Butler (1998) suggests that enthusiasm toward this

method in IT research is increasing. Applicable to hermeneutics, interpretation is an attempt to make sense and understand more clearly an item under research (Abulad, 2007). In the context of this research, this researcher needed to comprehend the perspectives of the diverse participants by adopting a compassionate stance (Saunders, Lewis & Thornhill, 2007). Furthermore, adhering to this stance allowed this researcher to generate deep insights into risk introduced by BYOD phenomenon in a South African organisation and gain an astute understanding of interviewees' actions and thoughts.

The approach chosen was an exploratory case study (Baxter & Jack, 2008), performed in a manner that made this research ontologically and epistemologically viable (Sofaer, 1999; Hennink, Hutter & Bailey, 2011; Honderich, 1995; Somers & Gibson, 1994). In order to reach ontological validity (what things are) the widely accepted case study methodology was selected, guiding both collection and analysis of empirical data (Zainal, 2007; Walsham, 1993). The reasoning behind the selection of this approach was twofold: i) the fact that risks surrounding BYOD phenomenon were not clearly understood, defined, explored and managed within a local South African context (Twinomurinzi & Mawela, 2014; Kabanda & Brown, 2014; Cisco, 2014; Irons & Ophoff, 2016; Gustav & Kabanda, 2016); and ii) the intention of this researcher was to investigate a single organisation by making a detailed narrative, based on in-depth interviews, to answer the imperative 'how' and 'why' questions (Yin, 1994).

There are different methods for collecting data. However, the literature regarding the similar topic (Sen, 2012; Twinomurinzi & Mawela, 2014; Kabanda & Brown, 2014) suggests that qualitative data collection, primarily by conducting in-depth interviews, appeared appropriate for this kind of research (Pather & Remenyi, 2005). Hence, this research utilised in-depth interviews, basing the questions on the literature review.

The sample in this research consisted of fifteen employees from Organisation A. According to Adler and Adler (1987), this number of interviewees is sufficient. The research participants were selected based on predefined criteria (purposeful sampling). Yin (1994) suggests that operationally defining the unit of analysis assists with replication and efforts of case comparison; hence, the unit of analysis in this

research was the meaningful answer of the interviewees. The analysis of the collected data was completed by interpretative phenomenological analysis (IPA) (Smith, Flowers & Larkin, 2009) which will be explained in more detail in Chapter 3.

Considering research design, the first step was to review the pertinent literature to build a theoretical or conceptual framework (i.e. model) to answer the research questions. The literature has assisted in determining the authenticity, reliability and reliance of the discoveries (Stake, 1995; Hamel, Dufour & Fortin, 1993). This was then followed by the collection of empirical data and analysis aimed at identifying emerging patterns, which assisted in answering the study's research questions. The final step entailed drawing conclusions and establishing recommendations, as the essential goal of the case study was to build connections, uncover patterns, construct conclusions, and develop a theory, i.e. recommend a solution (Stake, 1995; Hamel et al., 1993; Patton & Appelbaum, 2003).

1.6 Ethical considerations

Scientific research invariably involves studying beings in some form or another. Where research involves the acquisition of material and information provided on the basis of mutual trust, it is essential to protect the rights, interests and sensitivities of those who participate.

These include the following:

- The right to privacy (including the right to refuse to participate in research);
- The right to anonymity and confidentiality: No users' names and/or details will be mentioned in this research;
- The right to full disclosure about the research (informed consent); and
- The right not to be harmed in any manner (physically, psychologically or emotionally).

It is hereby confirmed and agreed that this researcher undertakes to adhere to the above. In addition, no data or information gathered for this research was used outside

the University of the Cape Town or for anything other than these particular research purposes. The informed consent form was provided to all research participants.

1.7 The scope and limitations of the research

This research was centred entirely on a South African medium-sized ICT organisation located in Cape Town and does not necessarily hold any connection to other businesses or parts of South Africa. Consequently, while the scope and the limited sample size might limit generalisation of this research, these did not impact study validity.

1.8 Contribution of this research

The contribution of this research is twofold: i) academic, by adding to the body of knowledge on the BYOD phenomenon in general and filling the existing gap on the available BYOD literature in South Africa, particularly in the area of understanding potential risks when introducing the BYOD initiative into organisation; and ii) practical, as the research has provided detailed risk considerations and mitigation guidelines for organisations that are currently deciding whether or not to introduce BYOD or are seeking to improve current BYOD risk strategies.

1.9 Thesis outline

This thesis is structured as follows:

- Chapter 1: Introduction and overview;
- Chapter 2: Literature review;
- Chapter 3: Research design and methodology;
- Chapter 4: Findings and discussion; and
- Chapter 5: Conclusion and recommendations.

This is accompanied by a comprehensive list of references and supplementary appendices.

1.10 Chapter summary

This chapter has presented the background and the research problem postulated for this research. The main research question was defined from several challenges identified in the South African organisation under investigation and is followed by an endeavour to solve these, and the associated, sub-questions. The subsequent chapter provides an extensive literature review as a means of gathering insight into BYOD.

CHAPTER 2: LITERATURE REVIEW

In this part of the research, the origins, key concepts and elements of the BYOD phenomenon are firstly recognised, as these terms can have multiple meanings. Therefore, it is imperative that readers understand precisely how these terms are used. Next, theory related to mobile individuals and equipment, mobile and cloud computing, and IT consumerization is introduced. Then, the benefits and risks of BYOD phenomenon are identified and explained. Next, a review of the related BYOD risk models is presented, followed by the description of the proposed model for addressing the identified risks and concerns. Lastly, through the analysis of the pertinent literature, the research sub-questions are answered theoretically.

2.1 Origins of BYOD

The 'Bring Your Own Device' phenomenon has received prominence with the maturing of mobile and cloud computing technologies. As mentioned in earlier chapter, Zheng and Ni (2006) describe the concept of these technologies as "anytime, anywhere, from any device" (p. 19). These researchers also explained that in 2006, smartphones appeared as a technology predominantly appropriate for corporate use. However, compared with 2006 where employees once used to ask their organisation for permission to purchase a new computer or software, they are now acquiring these themselves, introducing BYOD into their organisations. Furthermore, by bypassing organisational and IT departmental regulations by means of utilising the BYOD concept at their workplace, employees have effectively joined the global mobile computing technology 'revolution' and are reaping the benefits of digital freedom (Keyes, 2013).

The idea behind BYOD can be traced back to the early 80s when multiple organisations recognised that the ultimate employee not only needs to possess initiative, creativeness and determination but is also able to get things done across geographical boundaries (Dawson, 2012). However, the propensity toward the utilisation of privately owned devices was introduced globally in January 2007, when Apple co-founder Steve Jobs revealed the iPhone to the world. The iPhone, the first smartphone created with a multi-touch interface, swiftly became a global success.

Following Apple's footsteps, other mobile manufacturers also pushed forward the global mobile computing phenomenon. As a result, the smartphone became the most sought-after piece of consumer technology, marking the start of rapid adoption by the general public. Over time, the smartphone, including other mobile computing devices such as tablet computers and phablets, gradually found their way into numerous global organisations (Kim, 2011).

The first case of BYOD in a business environment was officially reported in 2009 by Cisco when, recognising the benefits of BYOD, they decided to permit employees to access business resources via their personal devices (Harkins, 2013). However, it was not until 2011 that other IT service providers acknowledged the advantages of this phenomenon and set in motion the series of events which brought BYOD to the forefront of the IT industry (Garba et al., 2015a).

Today, with the constant progress and affordability of consumer technology, organisations are more than ever faced with the challenge of implementing a BYOD strategy into their IT infrastructure. However, organisations are increasingly concerned about the risks that BYOD can introduce. Nonetheless, the 'genie is officially out of the bottle' as BYOD brings the promise to further improve employee satisfaction, productivity and workplace flexibility while at the same time enabling the organisation to be more customer-focused and agile. These benefits appear to be a key in developing competitive leads in a present-day economy based on knowledge and technology; however, the challenge for organisations is to embrace the changes that the BYOD approach requires, while successfully mitigating the risks (Reddy, 2012).

2.2 Elements of BYOD

BYOD, like most other phenomena, is a complex notion. To understand its complexity, the reviewed literature suggests focusing on the following main elements of BYOD: i) mobility; ii) mobile individuals; iii) mobile environment; iv) mobile equipment, and v) mobile computing.

2.2.1 Mobility

Abowd et al. (1997) explained that not being tied to a geographic location is an important characteristic of mobility. Yet another attribute of mobility identified by Heijden and Valiente (2002) is that it can be derived from a chronological feature that is often related to making information available whenever it is needed and thus is one of the most important factors behind the adoption of BYOD phenomenon.

Weilenmann (2003) differentiates between movement and mobility when she said that movement is merely a physical relocation of a person or object, while mobility deals with the use of technology related to the social dimension of that movement. Moreover, Heijden and Valiente (2002) establish that mobility can be seen and used differently in information and communication technology; various technologies in a variety of ways support activities determined by the type of mobility in use. Weilenmann (2003) also adds that mobility can be an activity, such as the remote communication between individuals or the local integration of individuals with each other. In the BYOD context, “organisations often provided these devices to increase the mobility and productivity of their employees” (French, Guo & Shim, 2014).

2.2.2 Mobile individuals

Taniar (2008) states that “human beings cannot conceive themselves as individuals solely standing without the world” and that the answer to this dilemma is the technology, or more specifically, the mobile device, thus enabling individuals to be mobile and to interact with the world around them. According to Andriessen and Vartainen (2006), *mobile individuals* are defined as individuals who are in movement, which is a rather ambiguous definition as virtually all individuals are moving to some extent, making everyone more or less mobile. Therefore, Mountain and MacFarlane (2007) provide a more descriptive definition by stating that mobile individuals are not only moving through space but also that their information needs are more likely to be a product of their surroundings and the environment in which they interact.

The term *mobile* is often associated, not only with individuals but also with groups. For instance, a group can be mobile (to some degree) when during work all or some of the group members move at some point (Andriessen & Vartainen, 2006). Even though it

seems that the definition of mobility appears quite broad, the description provided by Mountain and MacFarlane (2007) is suitable for this research.

2.2.3 Mobile environment

A mobile environment is an environment where people find themselves in motion, even while they might be more or less stationary. Such environments may be, for instance, 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, not dependent on their surroundings (Weilenmann, 2003). Likewise, Samar and Wicker (2004) state that *mobile environment* is the environment where 'nodes' are moving around with different velocities. Similarly, Huang and Garcia-Molina (2004) ascertain that in a mobile environment, both the information providers and the consumers tend to be mobile and that events can be generated by movement sensors or users while subscribers can request delivery of information to handheld and/or mobile devices. For this research, mobile environment enables the usage of BYOD devices.

2.2.4 Mobile equipment: types and uses

Technopedia[1] defines a *mobile device* as "a handheld tablet or other device that is made for portability, and is therefore both compact and lightweight." However, since mobile devices can mean a number of different things, Information Systems Audit and Control Association (ISACA) classified the following devices as essential types of mobile equipment, in an article entitled "Securing Mobile Device" (2010):

- Smartphones (Android, iPhone, Windows Phone, Blackberry, etc.);
- Laptops and netbooks;
- Tablet computers (Galaxy Tab, iPad);
- PDAs (Portable Digital Assistants);

[1] Technopedia. (n.d.). What is a Mobile Device? Retrieved from https://www.techopedia.com/definition/23586/mobile-device

- Portable Universal Serial Bus (USB) devices for storage (such as “thumb drives” and MP3 devices) and for connectivity (such as Wi-Fi, Bluetooth and HSDPA/UMTS/EDGE/GPRS modem cards);
- Digital cameras;
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification and asset management; and
- Wireless printers and smart cards.

The mobile equipment listed above not only permits users to communicate with each other from anywhere at any time, but also enables them to take advantage of different computer networks, access organisational emails and documents, and provides them with various multimedia and photographic capabilities (Ghosh, Gajar & Rai, 2013). In the context of this research, mobile equipment that is typically used for BYOD includes smartphones, tablet computers, laptops and similar.

2.2.5 Mobile computing

According to Kumar (2011), *mobile computing,* an important part of BYOD, is defined as “an umbrella term used to describe technologies that enable people to access network services any place, anytime, and anywhere” (p. 2). Moreover, he explains that mobile computing originates from the cellular concept founded in 1947 by Don Ring of Bell Labs. The concept, as demonstrated in Figure 1, is fairly simple and relates to a network of communication cells that cover a large geographical region used for communication.

Additionally, each mobile device uses a dedicated short-lived radio channel to talk to each cell site, which then enables the cell site to communicate with many mobile devices at once while using one channel per mobile.

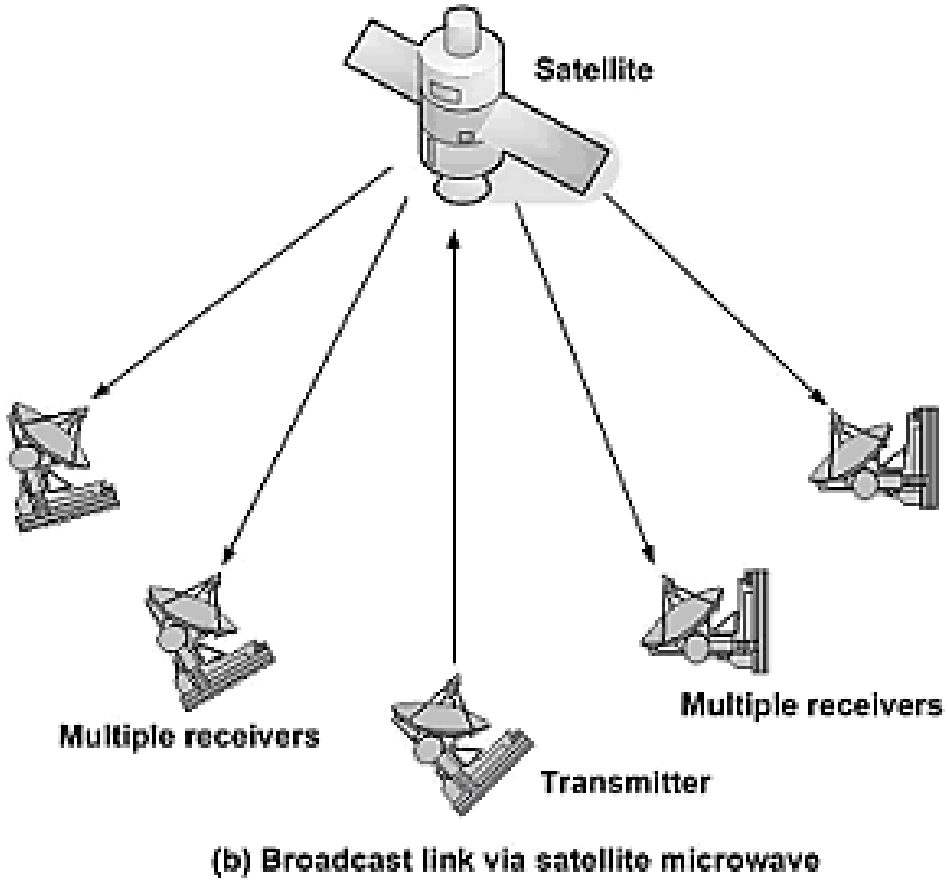


Figure 1. Cellular connection concept. Reprinted from “Paper Presentation on Mobile Computing” by Kumar, R. Siva., 2011, p. 4. Copyright 2011 by R. Siva Kumar.

Rouse (2007) refers to *mobile computing* as ‘nomadic computing’ because this term sometimes gets outlined as the utilisation of various portable computing devices with communication technologies based on the mobile technology. Similarly, Livingston (2013) describes *mobile computing* as a technology that is able to transmit voice, data and video via any device that has wireless capabilities.

2.2.6 Summarised BYOD elements

The above-discussed elements of BYOD are summarised in Table 1, which also includes relevant references.

Table 1.

Summarised BYOD Elements

ELEMENTS OF BYOD	REFERENCES
Mobility	Abowd et al., 1997; Heijden & Valiente, 2002; Weilenmann, 2003; French, Guo & Shim, 2014
Mobile individuals	Taniar, 2008; Andriessen & Vartainen, 2006; Mountain & MacFarlane, 2007
Mobile environment	Weilenmann, 2003; Samar & Wicker, 2004; Huang &Garcia-Molina, 2004
Mobile equipment: types and uses	ISACA, 2010; Ghosh et al., 2013
Mobile computing	Kumar, 2011; Rouse 2007; Livingston, 2013

Although they cannot be classified as elements of BYOD, there are two other important concepts – cloud computing and IT consumerization – that also helped propel expansion of this phenomenon into many organisations.

2.3 Cloud computing

While not necessarily an element of BYOD, but still an important term when it comes to this phenomenon, *cloud computing* along with BYOD allows for organisational innovation in a multitude of ways. Cloud computing has emerged as the cost-efficient substitute for managing complex IT systems while simultaneously creating a paradigm shift comparable to the replacement of single generators from the centralised power grid (Etro, 2011; Li, Wang, Wu, Li, & Wang, 2011). In the past, many organisations required internal computer networks to run their business. However, the challenge was managing these networks successfully as it required unique expertise that many organisations simply lacked or were unable to afford. This gap is now being filled by cloud computing as organisations can focus on their primary strengths and let cloud computing service vendors manage all their computing requirements. This is how cloud computing is different from traditional ICT and why is important for BYOD; the users and creators of information are not necessarily present at the same location (Klie, 2011; Mahesh, Landry, Sridhar & Walsh, 2011).

From the beginning, the cloud computing model has been attractive to many organisations because it offers a flexible model with the ability to grow capacity when

needed and reduce capacity when services are no longer required. Additionally, organisations only pay for the services they need and use (Srinivasan, 2014). Some of the leading providers in the international cloud computing industry today are Amazon, Google and Microsoft. Although all these providers are United States (US) based, cloud computing is available globally and is gaining popularity in South Africa as well. Furthermore, with BYOD becoming increasingly popular among South African organisations (Meeker, 2015), many local businesses are seeking to benefit from cloud computing by consuming cloud-based services such as Dropbox storage, productivity application Evernote, Google e-mail, Microsoft Office 365 and the like, on their devices used for BYOD (Twinomurinzi & Mawela, 2014).

2.4 IT consumerization and BYOD

Besides cloud computing, *IT consumerization* has played an integral role in the adoption of the BYOD phenomenon. The term itself gained popularity in the early 2000s as a description of how ground-breaking IT solutions for organisations are being created from the technology used by consumers (Clevenger, 2011). IT consumerization is regarded as the changing force behind the traditional ICT landscape and the way organisations use technology, as conventional lines between personal life and work continue to vanish (Reddy, 2012).

According to Midgley (BCS, 2013), principal strategist at Intel, the first adoption of the new software in the past would happen in the organisation, followed by employee adoption. He stresses, however, that nowadays, these circumstances are overturned; the consumer computing modernisations are now leading the drive-in business computing. Additionally, he believes that the reason behind this driving force is the affordability of technology and further points out that the technology makers have shifted their ambitions to the consumer market which demands the same convenience and ease of use as the business environment (BCS, 2013).

However, as organisations increasingly gain awareness that they are no longer in a position to dictate to their employees which devices they need to use for work, many are considering the best way to introduce BYOD to further advance their strategic agenda (Reddy, 2012).

Although the consumerization of IT in general and BYOD, in particular, offers potential financial and operational opportunities, this also introduces risks related to costs (e.g. lost device), legislation, regulation and privacy (e.g. control of organisation compliance and governance over devices owned by employees) or even risks related to data confidentiality, integrity or availability (e.g. potential loss of organisation's data) (ENISA, 2012). For instance, widely 'consumerized' Android devices were attacked four times more in 2016 than in 2015 (ENISA, 2017; KSN, 2016).

2.5 Benefits of BYOD

The major benefit of BYOD phenomenon is that it appears to be an impeccable model to accompany the ever-changing paradigm of work. Today, with its influence, the transition from traditional to mobile style working is materialising at a remarkably fast rate. This change brings many benefits for both employees and organisations that can be grouped into three categories: i) operational; ii) financial; and iii) organisational (Song, 2013).

2.5.1 Operational benefits

The results of a successfully implemented and supported BYOD strategy will not only improve operations of the organisation but also increase the overall satisfaction levels of the organisation's workforce. The times when employees were satisfied to sit behind their desks from "8 to 5" are nearing the end. Employees now require more flexible working hours and expect IT departments to provide suitable technology to support such work-related arrangements (Song, 2013). According to Reddy (2012), the BYOD approach seems to be the solution for the flexibility that employees seek. By enabling BYOD in an organisation, employees are able to work while they are out of the office and respond in a timely manner, since their personal devices have corporate mobile applications that allow collaboration essentially anytime, anywhere. This freedom to use the personal device of choice for work purposes not only improves operational efficiency but also escalates satisfaction levels and improves the motivation of employees (Reddy, 2012).

Similarly, Wood (2012) suggests that BYOD can boost an employee's productivity while increasing job satisfaction and improving creativity. Recent studies, for example,

claim that roughly 70% of global organisations already utilise BYOD and concur they experience improvements which include both enhanced morale and efficiency of employees (Downer & Bhattacharya, 2016). McLarty (2012) cautions that organisations not fulfilling the employees' BYOD expectations might experience unnecessary risks such as reduced productivity and dissatisfaction. The same researcher also states that such organisations risk upholding an 'old-fashioned' corporate image, which can prove detrimental, especially from a recruitment perspective.

2.5.2 Financial benefits

One of the first factors organisations discuss when thinking about BYOD is, not surprisingly, the cost. Generally, though, BYOD shifts part of the cost from organisation onto employees, who typically pay for their own devices and internet connectivity (Keys, 2013). Moreover, Wood (2012) also claims that financial benefits related to the decline of hardware investment are one of the key reasons why organisations decide to implement BYOD. Likewise, Calder (2013) states that desire of employees to annually upgrade their personal devices not only speeds up the adoption of cutting-edge technology but also immensely reduces organisational costs related to the maintenance and upgrade of technology. Yet another financial benefit for organisations outlined by Song (2013) is that BYOD appears to be a great way to increase the overall productivity, without increasing often associated capital expenditure.

Reddy (2012) claims that if organisations want to benefit from the lower total cost of ownership, they must necessitate one-time upfront investment to create BYOD support infrastructure. Similarly, Pillay et al. (2013) state that even though expenses related to purchasing of hardware is reduced, the costs related to security, infrastructure and compliance tend to increase. Furthermore, Song (2013) points out that organisations occasionally experience difficulties when they try to identify all the associated costs related to voice, data and support, which is why it is necessary to move beyond mobilising persons and rather mobilise the process, to better measure the impact BYOD has on business (e.g. sales, conversion rates and the like).

Additionally, benefits of cost sharing are also stressed in a number of business and academic reports. For instance, the ICT vendor Citrix (2013) claims that the primary benefits are the ability to reduce costs by having people pay part or all the cost of various BYOD devices used for work purposes. Correspondingly, Mutwiwa, Kamau and Gikandi (2017) established the following:

> As students realign their mindsets to increasingly joining the BYOD networks, benefits begin to trickle in for the learning institutions. The need to purchase and service their own computers is eliminated and the associated costs of power that could otherwise have been consumed by standalone organizational computers drastically reduce; the need for replacement of obsolete systems also fades translating into improved financial savings for institutions (p. 13).

2.5.3 Organisational benefits

Baker (2013) determines that from an organisation's point of view, increased mobility of employees not only boosts job efficiency but also opens new partnership possibilities with suppliers, customers and business units. Reddy (2012) distinguishes another set of organisational benefits: supporting, attracting and retaining the most talented employees. Many millennials, those who are soon expected to become the main segment of the workforce, openly seek employers that allow them to utilise the technology and tools they prefer.

The next organisational benefit is the effect BYOD has on transforming the workplace. The previously mentioned combination of cloud computing with BYOD devices means organisations can enable access to key corporate resources for their employees, anywhere and anytime. This convergence of BYOD, mobility and cloud computing is shaping the way employees work today, allowing them to collaborate and be creative in ways previously unimaginable (Reddy, 2012).

Similarly, Portela, Moreira da Veiga and Santos (2018) claim that BYOD represents the consumerisation, pervasive and ubiquitous side of IT that provides organisations with benefits such as real-time smart environment, positive transformation of the

workplace and improved remote work (i.e. freedom to work when and where needed). A well-planned BYOD strategy, therefore, one aligned with an organisation's IT policy, should deliver noticeable results that can drive the business toward its strategic objectives (Song, 2013).

2.6 Risks of BYOD

In contrast with previously distinguished benefits, BYOD can also introduce potential risks into an organisation. For instance, malware attacks and data leaks may breach the confidentiality of data and even lead to complete loss of important information (Lebek, Degirmenci & Breitner, 2013). Song (2013) claims that for most organisations, security is by far the biggest obstacle to the successful introduction of BYOD.

In general, the reviewed literature points out that risk related to security breaches can have the following adverse impact: loss of revenue, harm to investor confidence, damage to corporate image, loss of customer confidence, increased costs due to security breaches, unplanned costs of mitigation and possible business closure (Berghaus & Back, 2014; Putri & Hovav, 2014; Yeboah-Boateng, 2013).

The BYOD and Mobile Security Spotlight report (Information Security, 2016) confirms the above findings by stressing that security (39%) and employee privacy (12%) are the biggest inhibitors of BYOD adoption. The same report further states that primary security concerns related to BYOD include data leakage or loss (72%), unauthorised access to company data and system (56%), user downloads of unsafe applications or content and malware (52%).
Furthermore, for organisations, unsecured or not properly managed BYOD approach can introduce numerous risks, for ease of understanding grouped into five categories: i) implementational[2] risks; ii) technological risks; iii) legislation, regulation and privacy risks; iv) human aspect risks; and v) organisational risks.

[2] Implementational = Pertaining to the implementation http://www.yourdictionary.com/implementational

2.6.1 Implementational risks

The sheer number of diverse devices used for BYOD creates implementational complications that are, in most cases, overwhelming for organisations. Furthering the complexities, all these organisational devices need to be part of the BYOD implementation, while remaining secure and compatible with the latest corporate software applications. However, with inadequate control over BYOD devices, many organisations experience substantial challenges for ensuring security, protecting data and meeting compliance regulations (Reddy, 2012). Furthermore, Downer and Bhattacharya (2016) claim that supporting BYOD devices while trying to achieve financial savings related to the overall cost of support is yet another major obstacle to successful implementation of BYOD. Additionally, when BYOD policies are being considered, many organisations have difficulty determining exactly where and how dedicated BYOD policy is necessary.

Another difficulty for BYOD implementation arises when employees share BYOD devices, or their job encompasses many different roles. As a consequence, this behaviour might alter available data in unexpected ways and have a detrimental impact on overall BYOD implementation (Downer & Bhattacharya, 2016).

2.6.2 Technological risks

According to the reviewed literature, technological risks generate complexities that present the biggest challenge for the successful introduction of BYOD. Moreover, this challenge is likely to be even further exacerbated, as according to the recent study by Symantec (2016), the number of devices purchased and used for BYOD is continually escalating. Symantec reports that more than 1.4 billion smartphones were sold in 2015, a significant increase of 10% when compared to previous years. Additionally, Symantec (2016) claims that the Swedish networking and telecommunications corporation Ericsson predicts that “there could be as many as 6.4 billion smartphone subscriptions by the end of 2020, almost one per person” (p. 10).

Simultaneous with this rise in the number of smartphones, technology continues to march forward. Various mobile devices are now imbued with powerful computing abilities and, with fourth-generation broadband cellular network technology (4G), they

also have internet connectivity capable of fast speeds. With a rapid increase of mobile devices, the number of ways for their use also increases. For example, Apple launched Apple Pay in 2015, with Samsung and Android also contending to manage people's payments with their solutions in various countries. Similarly, other upcoming mobile payment systems such as Walmart Pay are likely to follow this trend. All of this intensifies the attractiveness of smartphones and other mobile devices used within the BYOD phenomenon to criminals, hackers and other potential attackers (Symantec, 2016).

2.6.3 Malware

Malware, already a renowned risk to all mobile devices, is swiftly increasing as a result of the introduction of BYOD. Its goal is to penetrate the mobile device to steal users' information, spy, delete data or cause other intentional damage. Malware can consist of viruses, zero-day threats, Trojans, worms and the like. In the same way, mobile users are often tricked to deploy malicious software applications on their personal device thinking they are installing clean and legitimate applications (Felt, Finifter, Chin, Hanna & Wagner, 2011).

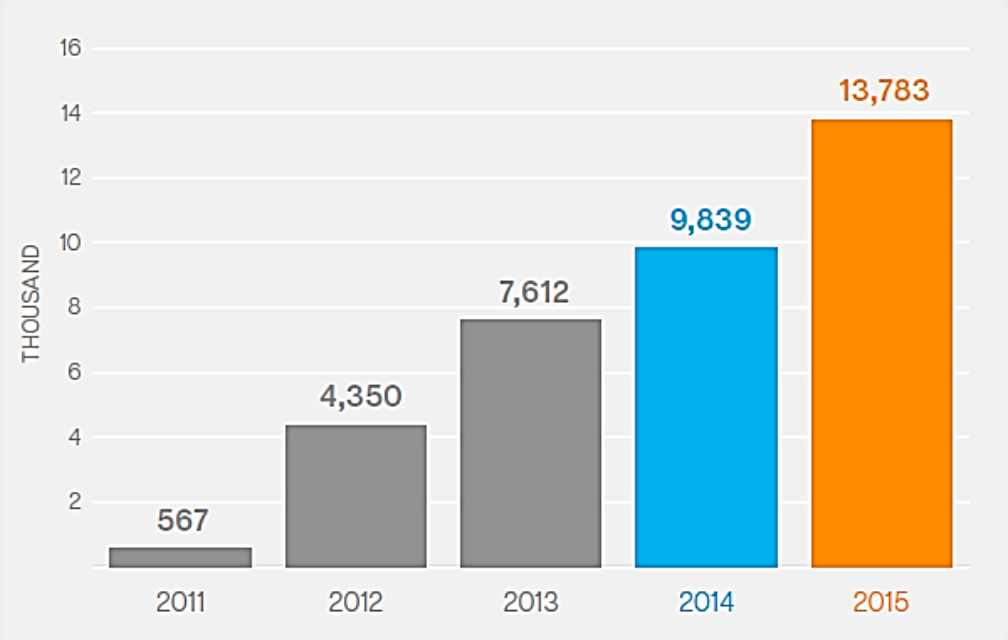


Figure 2. Cumulative Android mobile malware variants by year. Reprinted from "Internet Security Threat Report" by Symantec, 2016, p. 11. Copyright 2016 by Symantec.

According to a report by Alcatel-Lucent (2013), at any given time, approximately 11.6 million mobile devices are infected with malware globally, numbers which appear to increase substantially each year, as revealed in Figure 2.

To make the current security situation even more complicated, malware is becoming stealthier and can now be found embedded in numerous legitimate applications (Figure 3). Consequently, authors of malware for Google's operating system (OS), Android, have started to obfuscate code to bypass various anti-virus software. Their malware has the ability to check if it is running on real smartphones or the kind of emulators (i.e. sandboxes[3]) security researchers utilise. Additionally, some major smartphone OS manufacturers such as Apple are constantly trying to tighten control over operating systems and application stores in an attempt to prevent further threats to their devices (e.g. iPhones or iPads) (Symantec, 2016).

Up and until 2015, Apple devices were promoted as the safer choice for consumers, simply due to less exposure to malware and other security threats. However, Symantec (2016) recognised nine brand new threats for Apple's iPhone operating system (iOS) in 2015, compared with only four in 2014. One of those threats, Xcode Ghost, infected the software usually used by developers and was later found inside 4000 various applications that were installed by an unknown number of users.
Likewise, the YiSpecter malware found a way to take advantage of enterprise application provisioning framework and effectively bypass the Apple's application store security measures. Furthermore, Symantec's researchers determined that a threat named Youmi was embedded in 256 iOS applications (Symantec, 2016).

[3] Tech Target. (2005). What is sandbox? - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/sandbox

	2013	2014	2015
Total Apps Analyzed	6.1 Million	6.3 Million	10.8 Million
Total Apps Classified as Malware	0.7 Million	1.1 Million	3.3 Million
Total Apps Classified as Grayware	2.2 Million	2.3 Million	3.0 Million
Total Grayware Further Classified as Madware	1.2 Million	1.3 Million	2.3 Million
Malware Definition	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.		
Grayware Definition	Programs that do not contain viruses and that are not obviously malicious, but that can be annoying or even harmful to the user, (for example, hacking tools, accessware, spyware, adware, dialers, and joke programs).		
Madware Definition	Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.		

Figure 3. Application analysis by Symantec's Norton Mobile Insight. Reprinted from "Internet Security Threat Report" by Symantec, 2016, p. 15. Copyright 2016 by Symantec.

2.6.4 Risks and vulnerabilities due to installation of malicious software

Technical aspects of mobile operating systems, such as Apple's iOS and Google's Android, also have undesirable repercussions for BYOD. For instance, to be noticeable amongst the fierce competition in the smartphone market, Android tablet and smartphone manufacturers add their own applications of choice to the OS. Similarly, many mobile network providers do exactly the same; they supplement their custom applications on top of the default software that is already present on the device.

However, because security is not the strongest area of concern for these manufacturers and mobile network providers, the devices potentially become exposed to many risks (Gowda, 2013).

Now, the potential for additional vulnerabilities can increase even more, purely because the IT staff does not necessarily have complete visibility and control over all employees' personal devices. Employees, for example, might decide to install any software of their choice on their device, unaware that they might accidentally download disguised malware (Tzoumas, 2013). This risk normally occurs when employees install mobile applications that are not approved by their organisation (Madzima, Moyo & Abdullah, 2014). Moreover, the malware can spread through an entire computer network, exposing organisational information systems' 'backdoors' to attackers to steal valuable organisational data. Therefore, BYOD can be an easy target for potential attackers through vulnerabilities introduced by malicious software that can either be downloaded or sent directly by an attacker to an employee's personal device (Ahmad, 2013).

The diversity of devices utilised for BYOD augments organisational challenges for developing and implementing suitable protection measures against this risk. Likewise, advanced features of many BYOD devices, such as large storage capacity or high-resolution cameras, can be easily utilised to evade many traditional IT security mechanisms (Reddy, 2012).

2.6.5 Cross-over threats

With many options available via application stores, users are able to browse, remotely install and purchase applications from their desktop computers, while simultaneously creating a unique opportunity for a number of cross-over threats. For instance, Google allows consumers to browse their application store from their computer using an ordinary web browser and then send preferred applications directly to their Android compatible device. However, recently discovered Windows malware has abused this feature by accessing infected computers and using so-called browser cookies (i.e. the saved consumers' credentials) so that malicious applications can be installed remotely on the victims' BYOD devices without their awareness or approval (Symantec, 2016).

2.6.6 Contamination of data in cloud storage

Taking into consideration that cloud computing-based services and applications enable access to information anytime and from any place, protecting organisational data in cloud storage can be a serious challenge (Subramanian, Maguire & Stephanow, 2011; Sahu, Sharma, Dubey & Tripathi, 2012; Amoroso, 2013). Furthermore, an organisation utilising BYOD usually has modest or no control over data for the reason that information is typically stored on an employee's personal mobile device or in the cloud-based network (Olalere et al., 2015). When this cloud-based information is handled by BYOD devices, it is exposed to the identical security concerns as the device itself, such as software-based attacks, hacking and data contamination. Additionally, these devices can aggravate other BYOD related security challenges such as controlling, containing and monitoring the circulation of data (Rodríguez, Murazzo & Chavez, 2012).

The failure of organisations to control the transfer of data in cloud storage produces security loopholes also known as *cloud sprawls*[4] (Tech Target, n.d.). Cloud storage data contamination, then, typically occurs as the consequence of uncontrolled access to organisational data by employees using BYOD, resulting in loss of intellectual property and serious financial consequences for the organisation (Olalere et al., 2015).

2.6.7 Jailbreaking

The number of vulnerabilities on mobile devices has increased significantly since 2014, particularly on Apple IOS devices, as presented in Figure 4. When compared to Android, iOS vulnerabilities were more frequently linked to an unsafe practice known as *jailbreaking*. Jailbreaking enables the user to bypass the integral security of Apple's operating system and install applications that are not normally authorised by Apple. It is considerably more challenging to compromise non-jailbroken devices via malicious application because Apple is famous for its stringent security screening (Symantec, 2016).

[4] Uncontrolled proliferation of an organisation's cloud instances, services or providers.

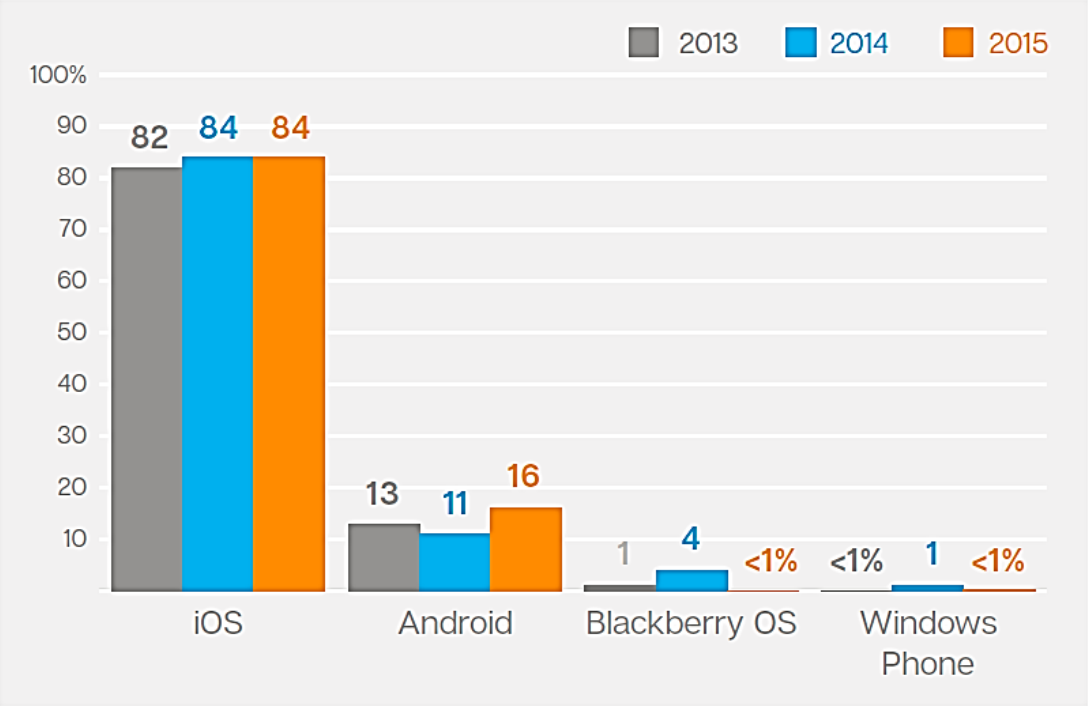


Figure 4. Vulnerabilities on the iOS platform have accounted for the greatest number of mobile vulnerabilities in recent years. Reprinted from "Internet Security Threat Report" by Symantec, 2016, p. 15. Copyright 2016 by Symantec.

In 2012, the first example of a malicious iOS application, Finfish, was discovered in the Apple Store. This application was able to access compromised Apple devices and steal all the information from users. Then in 2014, the next generation of malicious applications emerged. For instance, Wirelurker enabled its creators to run even on non-jailbroken iOS devices and utilised attacks on users via ordinary USB connections to either a Macintosh (Mac) or Personal Computer (PC). Likewise, attacks using Xcode Ghost and YiSpecter development software, first discovered in 2015, were not required to be jail-broken or have any vulnerabilities in order to compromise an Apple mobile device (Symantec, 2016).

2.6.8 Compromised user accounts

Compromised risks, usually related to specific attacks that involve unaware employees, are risks whereby user accounts are used to breach organisational security. This normally happens when employees access websites or organisational data share that are already infected, as that is all that is needed to compromise their account or BYOD device (Schneider, 2012).

Challenges related to this risk vary according to location, number of employees and size of the organisation. Therefore, organisations need to determine exact privilege levels for each employee's account when allowing access to valuable resources or internal networks (Astani, Ready & Tessema, 2013; Bradford Networks, 2012).

Implementing appropriate security measures can be challenging as employees may have many different personal devices utilised for BYOD, each with a different operating system and hardware, meaning that the security requirement of each employee needs to be equally supported (Chen, Li, Hoang & Lou, 2013).

2.6.9 Phishing and social engineering

Phishing and social engineering are well-planned types of deception that attackers use to collect confidential information about users with the intention of carrying out fraudulent activities at a later stage. The most frequently used methods include email messages, usually sent from individuals who are familiar to recipients with an invitation to enter personal details on a fake website or provide them via Short Message Service (SMS). Another method popular by attackers is to request from an employee to download onto their BYOD device an attachment which has a concealed keylogger software (Dodge, Carver & Ferguson, 2007).

Besides these and other somewhat familiar deceits, attackers are now utilising increasingly sophisticated techniques to garner financial gains from their victims. For instance, researchers from security vendor Symantec have exposed a new phishing Trojan for Android devices that deceives users into entering their banking credentials by presenting them with a fake login page over top a genuine banking application. Furthermore, the latest Android ransomware that sabotages documents and makes them unusable imitates the design of Google's applications so it appears genuine and entirely threatening when false Federal Bureau of Investigation (FBI) notices appear on users' lock screens. Similar to desktop and server versions, phone ransomware is also starting to encrypt all users' files and then demand payment, as compared with early instances when it merely changed a phone's Personal Identification Number (PIN). Unfortunately, ransomware decryption is not possible using conventional removal tools (Symantec, 2016).

2.6.10 Compromised network

Compromised network risk is a result of the attacker who has access to the internal organisational network. In most cases, the attacker can be a trusted individual such as employee, partner or contractor. Methods used to compromise networks differ in general, but the goal is almost often the same: thievery of sensitive information to make a profit. Since these types of attacks typically occur inside the internal organisational network and are executed by users with the highest administrative rights, they cannot be detected by conventional security methods designed to prevent attacks from the outside (Kumar & Kumar, 2014). Dimitriou and Krontiris (2016) further elaborate that a compromised node can authenticate itself to the network and send false identification information, affecting the aggregation result. This behaviour makes detection very challenging as it requires a specific application (semantics) or specific knowledge. Additionally, Zhou and et al. (2015) establish that as most conventional network security mechanisms are incapable of overcoming the increasingly complex and severe security issues related to this problem, this can produce a situation in which attacks are easier than defence.

2.6.11 Legislation, regulation and privacy risks

Local government laws and regulations related to organisational data usually determine 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).

Although POPI was signed into law on 26 November 2013, it is not yet officially effective as a commencement date has not yet been formally established. Nonetheless, the legislator has been appointed recently and organisations, while still having some time to prepare for the implementation of the POPI Act, do not have much longer, according to the Cedric Boltman, executive of the Jasco Enterprise. He stresses that "POPI is likely to be legislated towards the third or fourth quarter of 2017, after which organisations will be given a grace period of one year to become compliant" (BBrief, 2017). Evidently, organisations and businesses need to begin planning and initially implement BYOD policies and strategies accordingly, to meet the looming deadline and avoid any last-minute panic that POPI Act might create.

Turning to privacy and ethical issues, they appear to correspond with said legislation and regulatory implications. Research by Fiberlink (2012) determined that 82% of the staff studied believed that tracking of their personal devices by their organisation is a direct invasion of their privacy; over 80% demonstrated fears about the likelihood that their organisation is able to track resources they access via internet and also record the complete history of their devices while they are not at work; and 76% of the staff disagreed that their organisation needs to have a reach to all applications installed on their devices. This ostensible breach of privacy can have a negative psychological impact on employees utilising the BYOD with regards to their behaviour and acceptance of policy controls (Garba, Armarego, & Murray, 2015b).

Moreover, according to Silvergate and Salner (2011), the practice of BYOD can potentially result in a breach of 'normal working hours' as employees "stay connected to their jobs on nights, weekends and even vacations" (p. 41). In line with this, one possible consequence is that employees might demand additional payment for their bonus working hours. Similarly, many employees have concerns related to potential

liability if the important organisational information is lost due to theft, loss or unintentional damage to their device.

Hence, it can be established that possible legal concerns and implications arising from BYOD risks related to privacy are exceptionally complex (Kaneshige, 2012). Likewise, it is important to note that legal risk can also present itself in the shape of the security procedures and technological control measures that are key when deploying the successful BYOD strategy (Garba, Armarego, & Murray, 2015b).

2.6.12 Human aspects risks

According to the reviewed literature, in most cases, 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.

2.6.13 Lack of control over data and devices

Misuse of organisational IT resources can increase in a BYOD environment and compromise security. For instance, certain employees can deliberately circumvent imposed organisational security measures (e.g., BYOD policies and passwords) for the simple convenience of utilising their personal devices at their workplace as they please (Potts, 2012). Furthermore, when employees access sensitive organisational data outside of the internal network, they engender risk for an organisation that can lead to loss of control over data. Likewise, employees habitually use public cloud services (e.g., Google Drive and Dropbox) to store organisational data, while failing to realise the real consequences of ownership and data control (McAfee, 2012; Niehaves, Köffer & Ortbach, 2012).

One example of a common but serious data control violation is the auto synchronisation feature that Apple offers its iCloud users. According to Howie (2012), once Apple's auto synchronisation is on, the document is no longer within an organisation's reach. Similarly, Phifer (2013) stresses that emails which are open over

the mobile network on BYOD devices are no longer controlled by the organisation either. Another example of the lack of control of data on BYOD devices is revealed in a statement by CEO of IT Governance Company, Rick Dakin, who claims that for many executives, it has become habit to use the unsecured wireless network on their mobile devices while on an airplane to access sensitive sales data (Pillay et al., 2013).

In light of this lack of control, in 2012, IBM banned all its employees from using any personal device to access company data as they concluded that many smartphone and tablet features offered to its users by default, can and will compromise security (Mont, 2012).

2.6.14 Stolen or lost devices

Another common and yet important risk related to the BYOD phenomenon is a loss of organisational data associated with stolen or lost devices. Millions of smartphones and other BYOD devices are stolen or lost every year. It is assumed that roughly 22% of the produced mobile devices will be either stolen or lost throughout their lifespan, with over 50% of these devices never being recovered (EY, 2013). Furthermore, many devices used for BYOD, particularly smartphones, are increasingly popular targets of potential thieves as they are compact in size and offer high resale value (McAfee, 2012).

According to Gest (2013), many experts on this subject agree that risk related to the stolen or lost devices is a high priority risk of BYOD. Similarly, Reddy (2012) claims that for organisations, tracking lost or stolen BYOD devices as well as deleting sensitive data retained on them is a leading challenge. The high number of lost and stolen BYOD devices also means that they might end up in the hands of potential attackers who may utilise this opportunity to obtain physical access to hardware features of the device. This scenario poses a different risk model when compared to traditional IT hardware such as the stationery workstations or servers, where attackers were not able to gain physical access (Reddy, 2012).

It is much more challenging for organisational IT departments to secure a device once attackers have physical access. In a BYOD environment, this risk is emphasised for

every organisation that does not implement appropriate policy and minimum support of device requirements for all BYOD devices. Similarly, it is to be expected that such organisations will have a higher probability of insecure devices being able to access sensitive information (EY, 2013).

2.6.15 Identity theft

Identity theft, covered significantly in the media, is classified as a major threat to many organisations and their clients (Kahn & Liñares-Zegarra, 2016). This risk refers to an illegal activity whereby someone acquires or otherwise assumes the identity of another entity for the use in fraudulent activities. These types of illegal activities can often have negative financial repercussions for the organisation (Iovan & Dinu, 2014). However, it is important to note that the entirety of damage sustained by the victim is *not only* limited to the financial loss (Barker, Amato & Sheridon, 2008; Eisenstein, 2008) as the emotional cost and reputation damage is frequently the more harmful end result (Burns & Stanley, 2002).

2.6.16 Organisational risks

The reviewed literature disclosed that organisational risks are related to the following issues: (i) inadequate user education and organisational security culture; and ii) lack of organisational policies.

2.6.17 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. Thus, it is recommended that an organisation conducts sessions dedicated to the education of employees, elucidating the importance of their role in keeping their BYOD devices secure and the consequences of failing to conform to the organisational policy (Cisco, 2013). Additionally, Whitman and Mattord (2012) state 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 of knowledge.

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.

2.6.18 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).

According to Acronis (2013) and Guan (2012), there are a plethora of vendor-based solutions that can be utilised to manage BYOD; however, the more specific procedures and policies that address many privacy and security related issues are lacking in many organisations. Security of information and privacy, one of the primary concerns for organisations, should consist not only of vendor-based technological systems but also of procedures, policies and all other aspects that are required (Heimerl, 2012; Culnan & Williams, 2009).

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, & Murray, 2015a).

2.7 Future BYOD risk trends

According to one of the biggest security vendors in the world, Symantec (2016), mobile threats will continue to flourish over the next few years. PC-like hacking and exploit kits for mobile devices are likely to be developed for commercial use and sold on the black market. Simultaneously, the two largest global IT and mobile companies, Apple and Google, are working around the clock to increase the security of their operating systems and close potential security gaps. In particular, Symantec (2016) anticipates advances in the field of methods used to authenticate and sign software applications, including the mechanism for delivering applications to the end user. BYOD users can expect frequent and numerous application and operating system updates but also a new mandatory requirement for a security software on their own devices.

Many companies today offer various ‘always-on’ devices that continuously listen and record consumer voice to provide advertising companies with valuable data. This data will later be used around the web to create personalized profiles and serve ads to consumers. However, advertising companies are also evolving and experimenting with a combination of audio and web-based approaches for better tracking of consumers. Arstechnica (2016) describes these recent developments as “another disturbingly science fictional way: with audio signals your phone can hear, but you can’t. And though you probably have no idea that dog whistle marketing is going on, researchers are already offering ways to protect yourself” (para. 1).

This latest technology, known as ‘ultrasonic cross-device tracking’, implements certain high-frequency tones that are completely inaudible to humans, but which can be used in web pages, various advertisements or physical locations like retail stores. These

ultrasound tones are transmitted via certain ‘beacons’ such as ordinary speakers or even mobile device microphone that can also be used to detect the signal and create an overview of all advertisements a consumer has seen, websites and physical locations. Currently, Google’s Android or Apple’s iOS mobile operating systems require applications to first request permission to use a device’s microphone; however, in most of cases, the majority of consumers aren’t aware that by granting that permission, applications that use this technology can easily access their microphone and record everything (Arstechnica, 2016).

In addition to above worrying trends, earlier in October 2017, software engineer Christopher Moore publicly exposed misconducts of internationally popular Chinese smartphone manufacturer, OnePlus. They were secretly collecting a huge amount of personal data from their customers – IMEI codes, phone numbers, WIFI network details and MAC addresses – without consent. Moore discovered this behaviour during a holiday hack challenge when he noticed that his device was frequently transmitting large amounts of device data to OnePlus servers (Gizmodo, 2017). According to the Moore, OnePlus was also collecting data when its mobile device customers were opening applications, tracking what they were doing in those applications. After being exposed, an OnePlus representative provided this public statement (Gizmodo, 2017, para. 3 - 4):

> The reason we collect some device information is to better provide after-sales support. If you opt out of the user experience program, your usage analytics will not be tied to your device information. We’d like to emphasize that at no point have we shared this information with outside parties. The analytics we’re discussing in this post, which we only look at in aggregate, are collected with the intention of improving our product and service offerings.

According to OnePlus, the company will stop collecting user’s personal during October 2017, and will provide customers with an option to not participate in its ‘user experience program’. However, as Gizmodo (2017) noted after testing the opt-out provisions, it appears that the data collection cannot be stopped as opt-out just removes tags which links the data to a specific device.

Even though Symantec (2016) expects that number of security attacks on BYOD devices will increase even further over next few years, there is also an optimism that correct preventative measures can help organisations increase overall security levels and enable employees to enjoy the numerous benefits that BYOD brings.

2.8 Summarised BYOD risks

This section summarises the identified risks related to the introduction of BYOD in the organisation. A detailed literature review has revealed that such risks can be grouped logically into five different categories, as presented in Table 2.

Table 2.

Summarised BYOD Risks

PRIMARY RISK CATEGORY	BYOD RISK
Implementational	Protecting data, ensuring security, providing support
Technological	Malware
	Risks and vulnerabilities due to 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.

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. All these, then, must be adequately

addressed. The following section discusses the possible ways of addressing these potential BYOD risks.

2.9 Addressing BYOD risks

As discussed previously, addressing the identified BYOD risks cannot be optional, because if not addressed properly, all potential BYOD related benefits will diminish. Hence, this section explains the measures and methods for effectively addressing the identified risks. The literature review was conducted concerning possible theories and models capable of addressing these identified risks.

2.10 General frameworks and BYOD security

Frameworks such as COBIT 5, ISO 27001, NIST[5] or ENISA[6], 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.

2.10.1 ISO 27001 and BYOD security

ISO 27001, the leading information security standard, does not clearly stipulate requirements for BYOD security. Nevertheless, some experts in this field (e.g. Kosutic, 2015) suggest the use of certain ISO 27001 controls for rendering the BYOD solution more secure. For example, Kosutic (2015) suggests the use of controls that are adjacent to BYOD:

> A.6.2.1 Mobile device policy – this control requires the development of a security policy for using mobile devices in order to reduce risks. Therefore, the BYOD policy must be based on identified risks;

[5]US National Institute of Standards and Technology - https://www.nist.gov/

[6]European Union Agency for Network and Information Security - https://www.enisa.europa.eu/

A.6.2.2 Teleworking – since employees' personal mobile devices are used not only in company offices but also at home, this control is also applicable for BYOD. The control requires the implementation of security measures for information access, processing and storage, meaning that the BYOD policy must cover all those three areas;

A.13.2.1 Information transfer policies and procedures – this control require writing documentation for the protection of information that is transferred through any communication equipment, including employees' personal mobile devices. So, if you didn't write separate policies or procedures for information transfer, you can cover these requirements in the BYOD policy;

A.13.2.3 Electronic messaging – again, if you didn't define through some other document how electronic messages will be protected, then the BYOD policy is the right place to do it (para. 2).

Furthermore, Kosutic (2015) suggests that there are other factors that need to be considered not necessarily related to a BYOD approach. For instance, "A.8.1.3 Acceptable use of assets (defining rules on how each asset is to be used)" and "A.8.2.3 Handling of assets (defining rules on which protection measures are to be used according to information classification" (para. 2).

2.10.2 ENISA and 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).

In *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. Cormack (2013) gives an example by explaining that "it may be

cheaper and more effective to support staff in the appropriate use of social networking tools rather than to try to impose software on all their devices to prevent loss of business information" (para. 1). He further explains that ENISA advises that a BYOD programme "should be voluntary, with owners making a positive choice to share their devices with their organisations, understanding and accepting the responsibilities that brings" (para. 1). According to ENISA, this can be accomplished by encouraging participation in the programme, including the provision of support, the offer of additional services or even financial benefits.

Furthermore, providing or recommending services through the BYOD (e.g. webmail or online storage) can enforce security options that satisfy the security requirements of both employees and the organisation. Keeping organisational and personal use separate from relevant security policy and in technological practice is another ENISA pointer for sound BYOD security. Cormack (2013) explains that "an explicit policy that organisational support staff and management software will only look at organisational data and applications should help staff/owners trust that their privacy is being respected and encourage them to respect the organisation's interests in return" (para. 1).

Generally, ENISA suggests that organisations should work with their employees to incorporate BYOD into existing organisational systems for managing information security, as this will benefit both the organisation and its employees.

2.10.3 NIST and BYOD security

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 (p. vii).

Furthermore, NIST (2016) recommends a set of general principles for securing BYOD mobile devices:

- Limit access to the device, such as setting a PIN or password not used elsewhere, and automatically locking a device after an idle period;
- Disable networking capabilities, such as Bluetooth and Near Field Communication (NFC), except when needed;
- Ensure that security updates, if available, are acquired and installed at least weekly, preferably daily;
- Configure applications to support security (e.g., blocking activity that is likely to be malicious);
- Download and run apps only from authorized apps stores;
- Do not jailbreak or root the device;
- Do not connect the device to an unknown charging station; and

- Use an isolated, protected, and encrypted environment that is supported and managed by the organisation to access the organisation's data and services (p. viii).

For securing information, this NIST (2016) framework recommends the following:

- Using physical security controls for telework devices and removable media (e.g. organisation might require that laptops not be left unattended when taken to hotels, conferences);
- Encrypting files stored on telework devices and removable media such as CD and flash drives in order to prevent attackers from readily gaining access to information in the files;
- Ensuring that information stored on telework devices is backed up;
- Ensuring that information is destroyed when it is no longer needed;
- Erasing information from missing devices at its end of the lifetime cycle (p. 7).

Additionally, in practical terms, NIST (2016) recommends the following:

- Limit access to the BYOD device (e.g. setting PIN or password);
- Disable necessary networking capabilities except when they are needed (e.g. disabling Bluetooth in crowded public areas);
- Keep devices updated (e.g. update or patch software and hardware to eliminate known security flaws);
- Configure applications to support security (e.g. disabling unneeded application features and configuring applications to stop or block activity that is likely to be malicious);
- Download and run apps only from authorized app stores (e.g. games downloaded from unfamiliar website can result in 'drive-by' downloading malicious software);
- Do not connect the device to an unknown charging station (e.g. someone may have altered a charging station, such as one in a public area so that it attempts to automatically gain unauthorized access to the data, applications, services, and other resources on mobile devices that attach to it); and

- Use an isolated, protected, and encrypted environment that is supported and managed by the organisation to access the organisation's data and services. The environment isolates the organisation's stored data, applications, and other files on the mobile device so that the organisation can maintain control over them without having any access to the teleworker's personal information or files on the same mobile device (p. 25-26).

2.11 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 & 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-Olmo, Sánchez, Caballero, Camacho & Fernandez-Medina, 2016).

Von (2000) explains 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" (p. 3). Similarly, Schlienger and Teufel (2003) describe that security culture:

> Encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee. The cultural concept helps to increase trust between the different actors concerning information security within an organisation (p. 1).

The surfacing of a security culture has been recognised by numerous academics in a variety of ways. On the other hand, though, it can be said that there is no specific technique or any one unique factor to identify security culture inside an organisation. Academics have, in fact, established a variety of factors implicated in managing information security within an organisation. For instance, Sasse, Brostoff and Weirich (2001) point out that the classification and design of key characteristics can push security culture, including consequence, security consciousness and business impact. For the most part, they explain a fear-based method with the purpose of promoting adequate security operation.

Adams and Blandford (2005) point out that security culture must side with organisational policy and integrate into normal operational practice. Additionally, they indicate that the crucial tactic should be to inspire employee alertness. Thomson, Vol Solms and Louw (2006) argue that a security culture is largely determined by organisational culture and jointly connected to it. They also emphasise the constant education of employees as a critical factor to ensure understanding of security concerns. Furthermore, these researchers indicate that collective socialisation could present a significant feature, as individuals usually gain knowledge while studying one another. Ruighaver, Maynard and Chang (2007), describing how an organisation's inner culture has a vast influence on security culture, suggest that it might not be suitable to consider security culture in absolute segregation from general organisational culture. Likewise, Santos-Olmo et al. (2016) establish that once information security becomes an ordinary part of employees' behaviour and daily routine, it will contribute towards the protection of organisational data.

This concept, if appropriately applied, can address organisational BYOD risks related to organisational security culture by supporting security governance and policies aimed at staff awareness, education and training as well as adhering to security technological measures.

2.12 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 (2012) 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.

It can be established that it is of utmost importance for organisations to train all employees and increase their understanding of BYOD security to make certain that they only relay organisational information on their devices in a safe environment. Employees' actions are strongly influenced by the organisation's information security culture and as a result, technological mechanisms, in conjunction with employee awareness and behaviour (organisation security culture), are necessary for dealing appropriately with BYOD risks. The central goal of employee training is to express prospects which make personal devices acceptable for use, confirm perception of risks, and explain which security practices are desirable (Gladyng, 2013).
On the other hand, Chen et al. (2013) claim that an employee's unpredictable emotions and reactions related to BYOD training and security policies are constant challenges for organisations. In most cases, employees have a predisposition to overlook rules set by training or security policies and are ignorant of changes. This highlights the incessant requirement of continuous training and security policy reinforcement to successfully raise employee awareness of safety standards as well as the regulations for BYOD devices (Markelj & Bernick, 2012). According to Arregui, Maynard and Ahmad (2016), employee BYOD education should also include these factors:

- safe device operation (e.g. configure password and PIN codes, avoid borrowing the device to third parties);
- methods to store important organisational data (e.g. make use of encryption, avoid uploading to the cloud);
- secure networks used for access (e.g. public WI-FI hotspots are not allowed, Virtual Private Network (VPN) connection with a two-factor authentication needs to be established first); and
- security protocols followed in cases of lost or stolen devices (e.g. immediately inform the organisation and open the case with the police).

In particular, employees deprived of suitable knowledge of BYOD may execute actions that are deemed insecure while being completely unaware that they are exposing their organisation to risk (Leavitt, 2013). Tu, Turel, Yuan and Archer (2015) point out that social learning, which includes friends, colleagues, family and various social media, has a substantial role in the overall BYOD security of the organisation. However, they also condemn methods of social learning as the information security collected there can not be deemed as security best practice (Tu et al., 2015). Additionally, Ruighaver, Maynard and Warren (2010) establish that notion of consequential ethics may be connected to employee training. Ketel and Shumate (2014) contend that organisations require, not only a clear set of BYOD strategies, but also mandatory information security training for all their employees as they need to be made aware of exactly what is expected from them if they wish to utilise their personal BYOD devices in the workplace.

2.13 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).

2.14 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 & 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.

Although not really the latest technology, MDM (Figure 5) has only recently grown in complexity as a result of the advanced trending of the BYOD that is bringing privately owned devices into the organisation. MDM offers a span of security features that permit organisations to preserve "centralized, scalable visibility and control" of BYOD devices (Phifer, 2013; Semer, 2013). For instance, organisations can deploy various administration policies (e.g. disable email and disable VPN) that will allow for prompt reaction to potential threats. With MDM, organisations also have the option of using a built-in Global Positioning System (GPS) to track mobile devices, thereby addressing

device loss and giving organisations clear visibility of their BYOD environment.

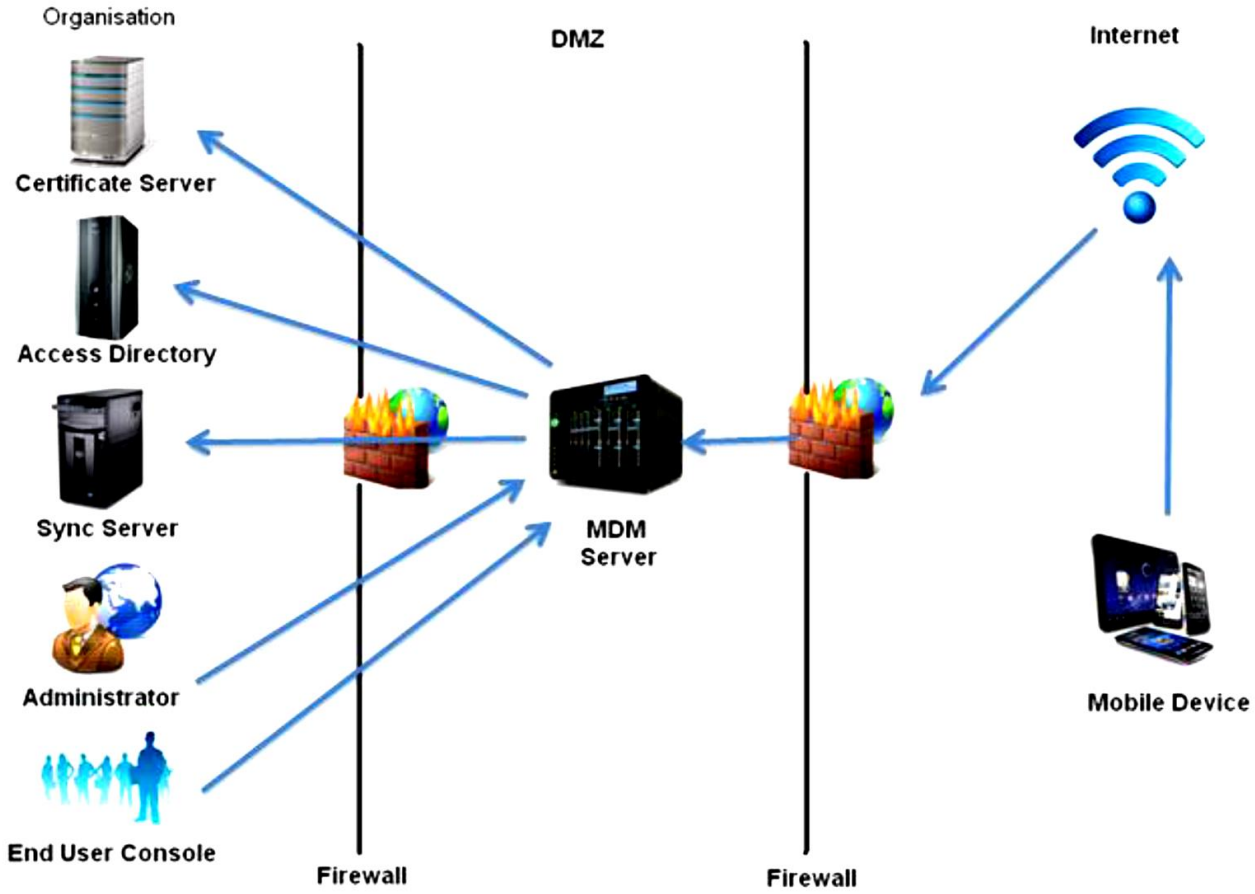


Figure 5. Typical MDM architecture. Reprinted from "Bring your own device (BYOD): Security risks and mitigating strategies" by Ghosh et al., 2013, p. 68. *Journal of Global Research in Computer Science*, *4*(4), 62-70. Copyright 2013 by Journal of Global Research in Computer Science.

Moreover, an MDM solution can be utilised with additional components for dealing with risks, such as malware detection mechanisms (i.e. anti-virus), encryption, device PIN and lockout control, jailbreak and remote wipe (Semer, 2013). On the other hand, it is well known that BYOD also introduces information ownership concerns as the organisation's data is the property of the organisation while the mobile device and personal data on it belong to the employee. However, most MDM solutions can address this challenge by having separate containers for employee and organisation data, thereby permitting devices to be deactivated without damaging any data (Phifer, 2013).

2.15 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).

Thomson (2012) points out that one of the requirements of the BYOD approach is the flexible and innovative solution for employees to preserve security while permitting access to combined technology. He further indicates that to ensure that employees are operating in a functional and secure domain with their personal devices, work and security applications must coexist. Consequently, it is imperative to find a sense of balance between risks and benefits so that security is not blocking business progression (Steven, 2013).

2.16 Cyber-security vulnerabilities assessment model

Exploring cybersecurity issues within small and medium enterprises (SMEs) in developing countries, Yeboah-Boateng (2013) has constructed a multifaceted cyber-security vulnerabilities assessment model (CSVA). As Yeboah-Boateng explained, the unique distinction of this method is that instead of physical quantities of cybersecurity, alleged or abstract concepts are assessed.

The CSVA model helps the risk assessor to understand how to characterise weaknesses and consequently recognise the distinguished threats associated with the IT. Moreover, Yeboah-Boateng (2013) claims that this model is intuitive, easy-to-use and does not require an enormous budget for successful implementation. The CSVA model (Figure 6) includes four layers:

- *Cyber risks layer:* used to explain occasionally vague associations between the other minor layers. Once evaluation of the extent of the weaknesses and the possibility of their exploitation is presented, this layer qualitatively estimates the resultant risk and its severity;
- *Cyber assets layer:* presents tangible or intangible assets that are used to expedite the conduct or engagement in various business events in the present cyber market. The aim of this layer is to evaluate cyber assets so that their cumulative estimated value is provided. The estimation process involves identification and classification of assets and is dependent on factors such as actual asset value, sensitivity, business risk and requirements related to compliance and governance;
- *Cybersecurity threats layer:* evaluates any situations, events or actions that can reveal the gaps in IT systems and create a potential risk to a dedicated cyber asset. In addition, this layer is also utilised to evaluate the possible threats which can be technical (e.g. operational or systemic), human (e.g. consumer) or environmental in nature; and
- *Cybersecurity vulnerabilities layer:* addresses flaws in the essential elements of the IT infrastructure, such as networks, systems and applications. The goal of this assessment is to estimate the level to which these elements are prone to attacks while taking into consideration the possibilities of multiple threats. As a result, this assessment can provide an estimation of the combined effects of sequential and multiple incidents.

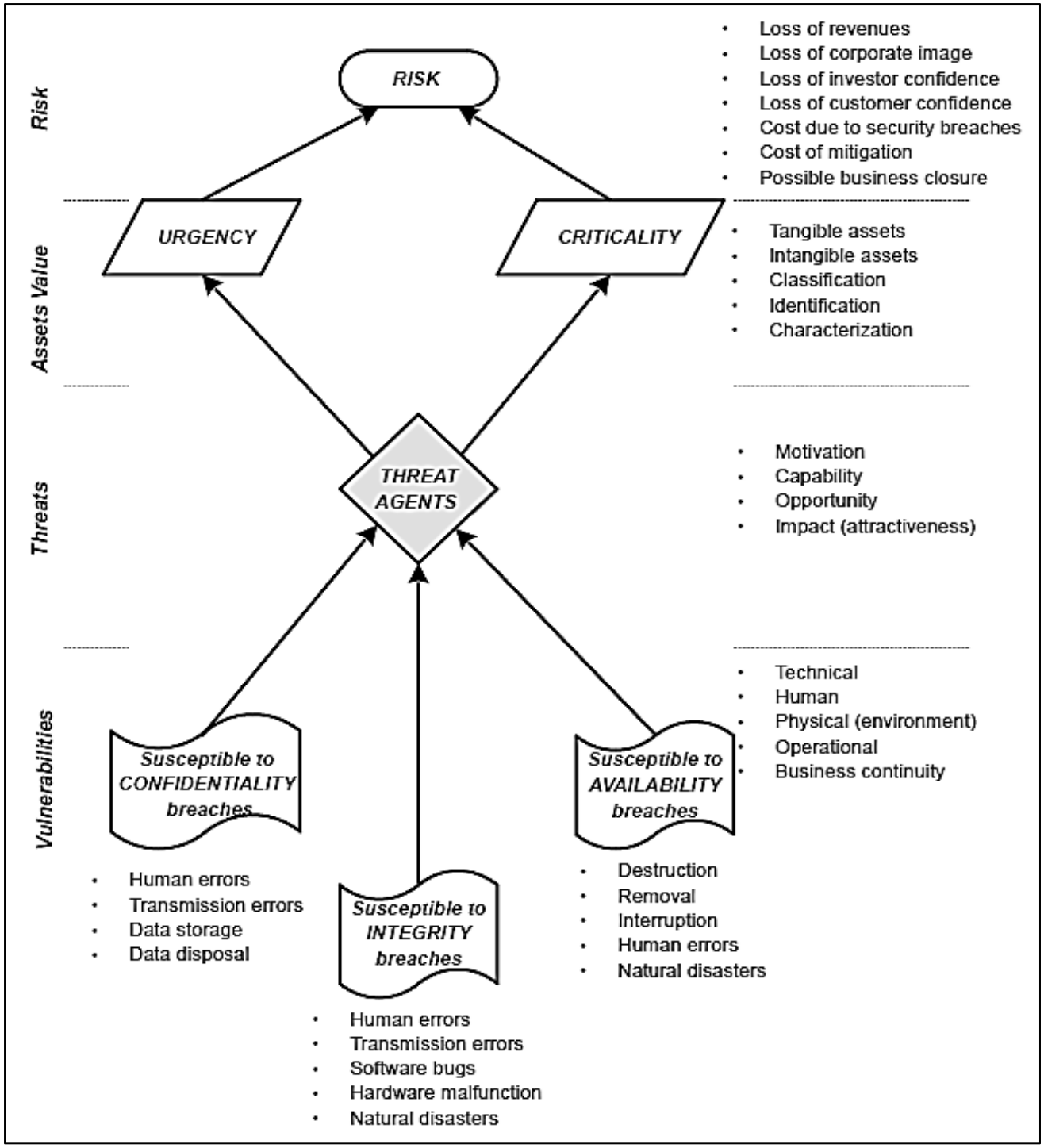


Figure 6. Multi-faceted cyber-security vulnerabilities assessment (CSVA) model. Reprinted from "Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)" by Yeboah-Boateng, E. O., 2013, p. 115. Institut for Elektroniske Systemer, Aalborg Universitet. Copyright 2013 by Aalborg Universitet .

2.17 Mobile device security model

While researching how to counter mobile device threats in various organisations worldwide, Grover Kearns (2016) created a seven-stage mobile device security model (MDSM). According to Grover Kearns, the aim when developing a security model to address risks is to produce a model that is not only extensive and efficient but also transparent. The uniqueness of this approach is that this transparency can promote improved communication through all IT departments (e.g. support, consultants, management and executives). The MDSM model (Figure 7) includes seven stages:

1	2	3	4	5	6	7
Develop Mobile Security Policy	Inventory Devices and Platforms	Inventory Applications	Assess Risk and Loss	Classify According to Risk/Loss matrix	Actions to Limit Risk and Loss	Educate Employees

Monitor and evaluate for revisions to policy and risk/loss profile

Figure 7. Stages in developing a mobile security framework. Retrieved from "Countering mobile device threats: A mobile device security model", p. 44. Kearns, G.S., 2016, Journal of Forensic & Investigative Accounting, 8(1), 36-48. Copyright 2016 by Journal of Forensic & Investigative Accounting.

Stage 1: To develop a personal device security policy, employees need to be asked which applications and devices they require to complete their work. The organisation needs to state clearly that it reserves the rights to monitor and manage all personal devices used for work and brought into the environment. Furthermore, the organisation must make sure that if these devices are lost or stolen, sensitive information can be remotely wiped by an MDM solution. Lastly, an organisational 'acceptable use policy' needs to be generated and presented to all employees (Netstandard, 2013).

Stage 2: All devices and operating systems need to be added to organisational inventory to define which ones are in use. Ideally, these records should also be differentiated by personal and corporate-owned devices because policies for personal devices need to be fairly stringent.

Stage 3: All software applications used by both personal and corporate mobile devices need to be added into organisational inventory. Next, the organisation needs to be certain whether this software is essential for daily business-related tasks.

Stage 4: Risk of device, application and platform loss. These risks can be characterised as low, medium and high to provide adequate data to generate an operational security model (Figure 8).

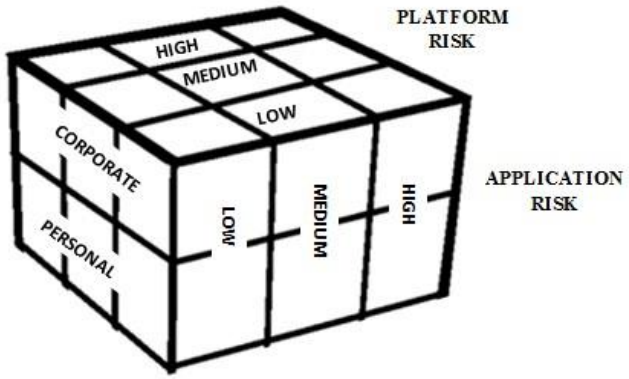


*Figure 8***.** Identification of risk levels for mobile devices**.** Reprinted from "Countering device threats: A mobile device security model", p. 45. Kearns, G.S., 2016, Journal of Forensic & Investigative Accounting, 8(1), 36-48. Copyright 2016 by Journal of Forensic & Investigative Accounting.

Stage 5: According to the risk model displayed in Figure 8, device, application and platform can be categorised into eighteen different risk categories. These categories represent if the mobile device is personal or corporate owned and various risk levels for applications and platforms. For instance, according to Greenburg (2012), Android OS should be categorised as high-risk because it is highly likely that it will be affected by malware. On the other hand, corporate applications are normally low-risk due to limited exposure to application stores such as Google Play or iTunes. Still, if corporate applications are being utilised on employee's Android-based BYOD device, then risk levels might be elevated. This will, in return, render it either medium or high-risk.

Software applications that can be ignored are the ones which do not require access to the organisational data repository. However, risk policy may demand that personal and corporate applications do not run on the identical device, in order to lower the possibility of the introduction of malware or threats into the organisation. Ideally, as organisations should decide how to best manage risk profiles, Kearns (2016) suggests

a starting point in Table 3 below.

Table 3.

Possible Risk Evaluation of Devices, Platforms and Applications

Corporate Device			Employee Device		
Application Risk	**Platform Risk**	**Overall Risk Level**	**Application Risk**	**Platform Risk**	**Overall Risk Level**
High	High	High	High	High	High
High	Med	High	High	Med	High
High	Low	Med	High	Low	High
Med	High	Med	Med	High	High
Med	Med	Med	Med	Med	Med
Med	Low	Med	Med	Low	Med
Low	High	Med	Low	High	High
Low	Med	Low	Low	Med	Med

Note. Retrieved from Countering mobile device threats: A mobile device security model (p. 46), Kearns, G.S., 2016, Journal of Forensic & Investigative Accounting, 8(1), 36-48.

Stage 6: It is necessary to take explicit steps to lower risk and loss potential. This can be achieved by categorising the general risk factors from previously described risk models and matching them with the possible loss. Large levels of details are not required to successfully measure the probability for the loss, and the specified categories (low, medium, high) are adequate to make security-related decisions.

Next, by applying the loss/risk decision matrix in Table 4, the crossing of loss and risk will provide the organisation with a score of one, two, or three. The lowest level of security should be focused in the direction of those loss/risk combinations ranked one, whereas the highest level of security should be ranked three, thereby permitting effective utilisation of security assets to achieve stronger protection of organisational resources from mobile device related risks.

Table 4.

Risk/Loss Decision Matrix for Use of Mobile Devices

LOSS			
RISK	**Low**	**Medium**	**High**
High	2	3	3
Medium	1	2	3
Low	1	1	2

Note. Retrieved from Countering mobile device threats: A mobile device security model (p. 46), Kearns, G.S., 2016, Journal of Forensic & Investigative Accounting, 8(1), 36-48.

Stage 7: It is of utmost importance that employees are trained and educated in device security practices and policies, noticing potential consequences for any violations. A survey by CheckPoint Technologies (2014) established that IT professionals who specialise in security firmly believe that inconsiderate employees are in fact a larger risk to BYOD security than hackers or cybercriminals. Likewise, the same survey reflects opinions of many IT professionals who believe employees are likely the weakest link when it comes to vulnerability of BYOD devices and related data leaks.

2.18 Proposed model to address BYOD risks

While a CSVA (Yeboah-Boateng, 2013) model provides effective information concerning how to complete an initial cybersecurity vulnerability assessment and the MDSM model by Kearns (2016) expounds on the steps for countering certain mobile device threats, neither includes all the additional BYOD risks or their respective categories that this researcher has identified from an extensive literature review (e.g. implementational, cross-over threats, contamination of data in cloud storage, jailbreaking, legislation, regulation and privacy risks, for example), nor the suitable methods for managing these risks. This brings forth the second part of the main research question "*What is an optimal approach to manage the BYOD related risks?".*

Table 5.

Combined Risk Categories

GENERAL RISKS	PRIMARY RISK THREAT CATEGORY	BYOD SPECIFIC RISK
Loss of revenue Harm to investor confidence Damage to corporate image Loss of customer confidence Increased costs due security breaches Unplanned costs of mitigation Possible business closure	Implementational	Protecting data, ensuring security, providing support
	Technological	Malware
		Risks and vulnerabilities due to 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.

This section answers this question by proposing a risk management model to address BYOD risks based on the comprehensive literature review. Table 5 above depicts the identified common BYOD risks that here proposed BYOD risk management model is capable to address effectively.

Since BYOD risks might vary in different organisations, the general steps for identifying these risks are given in Figure 9. This identification essentially revolves around the classification of general risks into the primary BYOD risk category. Next, these categorised BYOD risks are further matched with specific risk for a given organisation and lastly, comprehensive steps to address these identified risks are provided.

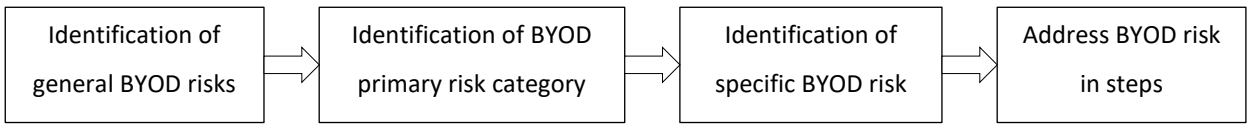


Figure 9. Steps to address BYOD risks. Adapted from "Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)" by Yeboah-Boateng, E. O., 2013, p. 115. Institut for Elektroniske Systemer, Aalborg Universitet. Copyright 2013 by Aalborg Universitet.

The final step in the above figure (i.e. steps to address BYOD risks) includes a selection of appropriate risk models, frameworks, technologies, education, training, standards and policies for introducing or further improving security culture inside the organisation. All these elements are portrayed in Figure 10 as an optimal approach for managing BYOD related risks.

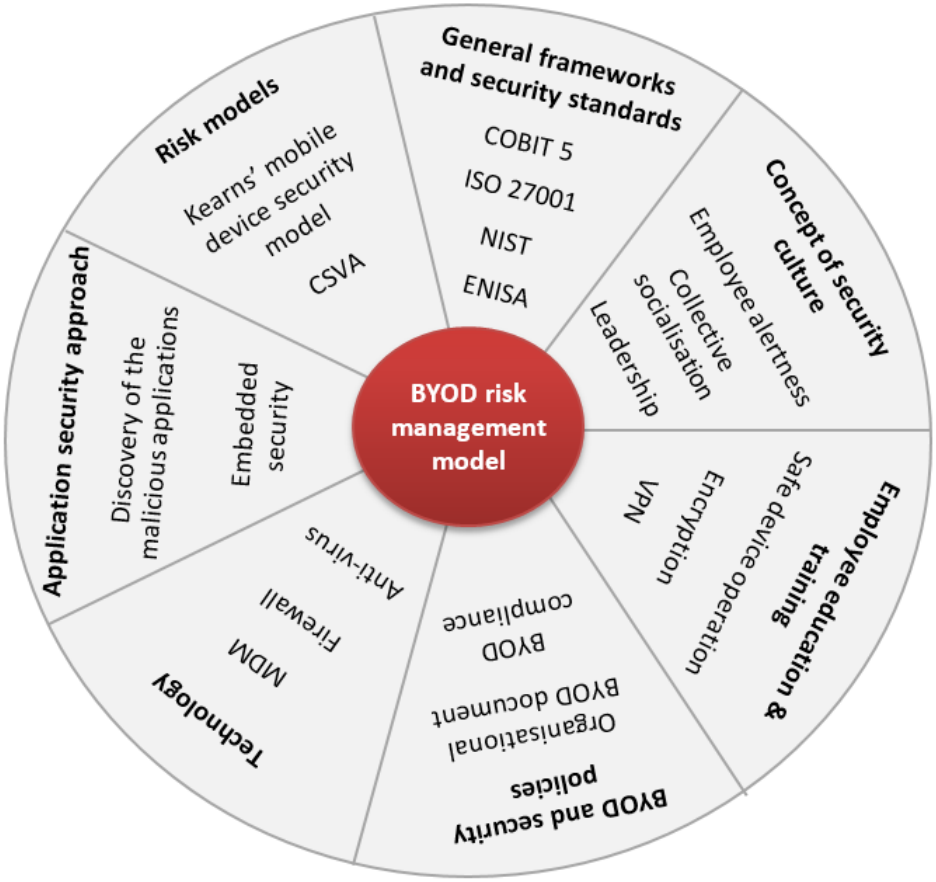


Figure 10. Proposed BYOD risk management model. Copyright 2017 by Author.

While the combinations of BYOD risks and suggested solutions can be considerable in number and can vary from organisation to organisation, the general approach of using the proposed risk management model is provided in the following paragraphs.

Implementational risks are multifaceted; therefore, all the elements of the proposed model can be used as needed and appropriate. For instance, to protect organisational data during the BYOD implementation phase, specific policies can be supported by the technological solution. Likewise, providing support and ensuring security can be regulated by policies but also maintained by well-established organisational security culture.

The identified technological threats can be resolved by deploying the MDM solution, including additional MDM components such as anti-virus, VPN, data encryption and the like. However, MDM itself will not be sufficient to manage *all* identified technological risks; hence, organisations also need to institute appropriate BYOD and security policies and determine that employees are trained and educated with regularity on this matter.

Legislation, regulation and privacy risks can be handled by implementing the necessary technological solutions (e.g. MDM and additional components, for example), BYOD and other specially tailored organisational policies (e.g. employee, privacy, etc.) to avoid leakage of company data and still respect employee privacy and work agreements. Additionally, local and any organisations doing business within South Africa need uncompromising BYOD policies and sound security to meet deadlines and avoid the last-minute panic before the POPI Act is legislated.

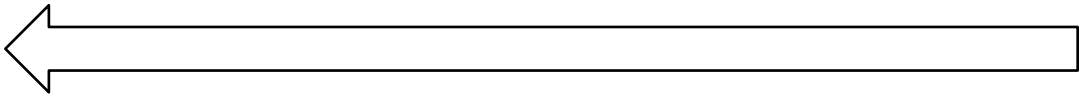
The human aspects of BYOD risk considerations should be addressed by combining certain features from previously mentioned MDM solution (e.g. GPS tracking and remote wipe) with the introduction or further development of organisational security culture.

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. The solution for this aspect overlaps to a certain extent with the solutions for the technological risks, underscoring the importance of appropriate education and continuous training of employees. Required policies should be based on 'industry best practice', usually given in standards or widely recognised models and frameworks such as those described in this chapter (e.g. ISO 27001, COBIT 5, NIST, ENISA).

Although it is outside the scope of this research, the approach to create organisational policy (i.e. BYOD) can be, for instance, adopted from the 7-step model by Kearns, presented in Table 6 below.

Table 6.

Approach to Create Organisational BYOD Policy in 7 Steps

1	2	3	4	5	6	7
Establish BYOD policy and strategy	Inventory all devices and software platforms used for BYOD	Inventory all applications used within the organisation (include personal and corporate applications)	Assess possible risk and loss, and classify according to risk/loss category	Provide actions to limit risk and loss (include technological and other methods)	Finalise and implement BYOD policy and strategy	Introduce all employees to BYOD policy and keep them informed frequently
Monitor and evaluate for revisions to policy and strategy including the risk/loss category 						

Note. Adapted from Countering mobile device threats: A mobile device security model (p. 44), Kearns, G.S., 2016, Journal of Forensic & Investigative Accounting, 8(1), 36-48.

2.19 Chapter summary

At the end of this chapter, it was established that the research sub-questions one to four are thus far answered theoretically (i.e. through the analysis of pertinent literature). A detailed literature review that included limited South African literature (cited in this thesis) in conjunction with international literature, elicited not only the most common BYOD-related risks but also several models, frameworks and standards that can be applied for addressing the mentioned risks.

Based on these revelations, the applicable BYOD risk management model was proposed. To empirically test the proposed model, the next research step was to select an appropriate research design and methodology for data collection, subsequent analysis and the compilation of research findings.

CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY

Research usually comes as a result of a certain requirement to fulfil the particular purpose (Bless & Higson, 1995). Natural science research is determined by the production needs, industry and commerce, whereas social science research is deep-rooted in the prerequisite to conceive questions concerning control of social affairs and general management. According to Singleton, Straits and Straits (1993), research is carried out to: (i) to explore a phenomenon; (ii) to describe a particular community; and (iii) to examine or formally test relationships among variables. In information systems (IS), research can deliver a rich range of analysis because of its trans and multi-disciplinary nature (Pather & Remenyi, 2005). Likewise, personal and social constructs also have a significant impact on the way technology is used (Mercer, 2001); therefore, this research proceeds along an interpretative pathway in the analysis of data.

Neuman (1997) claims that theory and research are interrelated. The same author also states that theory not only conceptualises and provides basic assumptions about the way we look and think about an issue, but that it also directs us to ask certain questions and assess data received regarding an issue being studied. The principle underlying the methodological approach of this research is informed by the philosophical strands of hermeneutics and phenomenology and which lies behind interpretative phenomenological analysis (Smith et al., 2009).

Risk considerations related to the various categories of Bring Your Own Device phenomenon such as technological and organisational form part of the analytical framework for formulating research questions based on the IPA approach. The idea behind the research in adopting the IPA approach was that themes or concepts should arise from an employee's own experience and then establish common connections with well-known constructs or factors from the literature. In terms of this research, such connections are necessary since the theoretical underpinnings that inform the data collection process was focused on risk factors related to the introduction of BYOD in

a South African organisation. However, to successfully conduct empirical research, it was necessary to explore a philosophical approach, available research methodologies and suitable methods of data collection, including analysis. This was then followed by constructing a research design plan which guided the empirical research step by step. Hence, this chapter precedes by presenting the research design, methodology and methods used in this research.

3.1 Motivation for the qualitative approach

Because the nature of this research was bound within various risk considerations related to the introduction of BYOD in the South African organisation, a qualitative approach is adequate for providing the basis of an enquiry, considering that perception of social information is not best recognised when numerical and statistical methods are utilised (Pather & Remenyi, 2005). According to Willig (2001), qualitative researchers are those who are interested in "how people make sense of the world and how they experience events. They aim to understand what it is like to experience particular conditions…and how people manage certain situation" (p. 8), and this also reflects situational circumstances in this research. On the other hand, Mangan (2004) and Singh and Bartolo (2005) highlight that research related to information systems is moving away from technological to managerial and organisational issues, with an increased interest in qualitative research methods. Likewise, Denzin and Lincoln (2000) describe qualitative research as a situated activity that finds the observer in the world with a series of representations such as interviews, conversations, field notes, photographs, memos and recordings.

To understand how humans make sense of the world, qualitative research can be used as a method to explore the area of human experience; in this case, that was human experience regarding perceived or actual BYOD risks. This allowed the author of this research to identify and describe topics or relatively unknown phenomenon in South Africa (BYOD) and to explore the scope, including the meaning of such phenomenon (BYOD risks) (Priest & Roberts, 2010).

Orlikowski and Baroudi (1991) classify the three research methodologies used in IS research as follows: I) positivist; ii) interpretative; and III) critical. Positivism can be applied to isolate the whole into constituent parts, while research can be conducted to

test for casual relations and verify hypotheses based on any number of variables to support an empirical assumption of the 'whole'. The critical research paradigm aims to understand the range of possible ambivalence or contradiction consisting within a given reality. Interpretative research origins are derived from hermeneutical and phenomenological philosophical foundations and characterised by interpreting a human experience within a particular social reality (Navarra, 2006). However, a number of researchers report that IS research has shifted from positivist to interpretive, which is discussed in the following section.

3.2 Interpretive research

Roode (2003) and Pather and Remenyi (2005) ascertain that when it comes to usage, implementation and development of IS, the interpretive researcher is able to recognise many important issues which concern people personally. They also claim that the social world around researcher presents an enhanced platform which can be utilised for close studies of the phenomenon (e.g. BYOD risks) to obtain many more relevant results (e.g. managing BYOD risks) when compared to the results obtained from the purely physical world of technology (e.g. a technological component of BYOD risks). In addition, Roode (2003) also establishes that because the social world is recognised as a human creation with many characteristics that simply cannot be measured or observed via quantitative methods, the interpretivist purposely expands free observation to more subjectively understand these constructs. This observation is frequently performed through active participation, rather than through alleged objective or independent observation, because understanding is the key part of the interpretivist, not the estimate, and in the case of this research, understanding of employees from Organisation A regarding possible risks introduced by BYOD phenomenon.

Interpretive research has increasingly been viewed as an important approach linked to information systems research (Klein & Myers, 1999; Walsham, 1993). Klein and Myers (1999) claim that IS research is interpretive when the assumption is made that knowledge of reality is derived from social constructions such as language, consciousness, shared meaning, documents, tools and other artefacts. The interpretive methods of research in IS, according to Walsham (1993), are "aimed at

producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (p. 4-5). However, some authors criticise interpretive research, claiming that it often lacks the ability to generalise or does not have sufficient reliability. In disagreement with this criticism, Kelliher (2005) argues that the interpretive approach is also known to provide additional value in the form of contextual depth. Analysing pros and cons of interpretive approach, this researcher has adopted a method to explore and understand people's perceptions of possible risks introduced by BYOD in the South African organisation.

3.3 Hermeneutics and phenomenology

As mentioned previously, the philosophical strands that run through this research are hermeneutical and phenomenological, underscoring the interpretive nature of this research. According to Schwandt (2000), hermeneutics implies that "understanding is interpretation…Thus, reaching an understanding is not a matter of setting aside, escaping, managing, or tracking one's own standpoint, prejudgements, biases, or prejudices. On the contrary, understanding requires the engagement of one's biases" (p. 194). Likewise, Gadamer (1976) and Klein and Myers (1999) agree that the process of hermeneutical engagement of understanding is continuous, from the complete to the part and back to the complete. Applied in this research, the indicated refers to the understanding of BYOD in the Organisation A as a whole phenomenon and its relation to the BYOD risk considerations as parts of the whole. This is also known in the hermeneutic circle as enabling visiting and re-visiting between detail and sense of the whole, allowing for the ontological structure of human understanding (Gadamer, 1976; Boland, Newman & Pentland, 2010).

In the sense of being phenomenological, this researcher was aware of his own measures of reflectivity and bias as far as assuming an insider perspective in the interpretation of the phenomenon (BYOD risks) (Fade, 2004). As such, interpretive researchers must recognise that the research participants can be (and were actually) perceived as interpreters or analysts just as much as the researcher (Klein & Myers, 1999). Phenomenology is implicitly relating and recording human experiences in all social practices such as work, speech, action, and one may include thought processes. In that sense, phenomenological inquiry begins by understanding the

research participants according to their own interpretations of reality (Mouton, 1996; Smith et al., 2009), which in this research, was completed by allowing the interviewees to interpret their perceptions of BYOD and the related risks as a phenomenon and its parts (Leedy, 1997; Marais & Kruger, 2005).

Furthermore, this research adhered to Mouton's (1996) view of phenomenology, the interpretation of reality as best situated within a methodology designed by the following:

- Unstructured and open interviewing (the research subject determines the outline);
- Thick and idiographic descriptions (in-depth and thorough using small amount of cases);
- Qualitative analysis (IPA selection for this research); and
- Objectivity which is defined as the inter-subjective conceptions of the 'insider'.

3.4 Principles of interpretive field research

This research also considered Klein and Myers' (1999) set of interpretive principles that can be applied in the evaluation of interpretive field research:

- *Hermeneutic circle,* which reflects upon the interrelationship between the part and the complete and gains a holistic view of the phenomenon being studied;
- *Contextualisation* as an important reflection of the historical and social background within which the research proceedings are conducted;
- *Interaction between researcher and research participant* as a critical appreciation of the interaction between researcher and research participant in the collecting of data;
- *Abstraction and generalisation* as examination of the idiographic detail through the cycle of hermeneutic reflection, reaching correlates that can be generalised with broader concepts, theories and other research;
- *Dialogical reasoning* as a constant interaction and review to ensure that concurrence is present when integrating the theoretical underpinnings guiding

the research with the data observed, gathered and assimilated into the research;

- *Multiple interpretations* reflecting awareness of the account of many witnesses perceiving the same phenomenon, with each having an own interpretive stance on the experience; and
- *Suspicion* as implying that the researcher must be circumspect and prudent in the critical appraisal of data despite bias or distortions that will occur in the data collection process.

This mentioned set of interpretive principles underpinned the hermeneutical process of this research in acquiring depth of meaning from the interviewees' lived experiences. Besides, this research was also interpretive because it reflected upon the meaning interviewees made about their perceived reality (i.e., BYOD risks). Taking advantage of interpretive approach, this researcher ensured that the interviewees were also informed about the subjective nature of the research. The advantage of this inter-subjective awareness provided not only a richer experience but also a deeper and intimate feel for the information regarding BYOD risks that were gathered.

3.5 Interpretative phenomenological analysis (IPA)

This qualitative research used interpretative phenomenological analysis (Smith et al., 2009) to analyse the data which was collected as the case study methodology does not possess any 'built-in" analysis tool. *IPA* is defined as "an attempt to unravel the meanings contained in accounts through a process of interpretive engagement with the texts and transcripts" (Smith, Jarman & Osborn, 1999, p. 189) – the transcribed interviews in the case of this research. IPA has been applied mainly in the context of psychology. However, this research was of the view that IPA can be applied to information systems and the BYOD phenomenon as part of it since IS intersects with human experiences and draws on interpretive research to make sense of the process. IPA was involved in a detailed examination of a person's lived experience.

The aim of this approach was to examine the experience of the person expressed in his own terms rather than according to a set of pre-existing constructs, themes or factors. Themes refer to those common strands that flow within and between

narratives. The creation of themes that emanated from the discourse provided a deeper and richer interpretation of interviewees' own lived experience, and this researcher could, upon those descriptions, better understand people's perceptions of the risk possibly introduced by BYOD in the South African organisation.

IPA is underpinned by theories from three philosophical knowledge areas: i) phenomenology; ii) hermeneutics; and iii) idiography. As discussed previously, *phenomenology* refers to the study of experience, or the lived processes involving the interpretation and meaning people attach to what they are going through (Smith et al., 2009; Trochim & Donnelly, 2001). *Hermeneutics*, as also discussed, is the theory of interpretation, which means making sense of the phenomenon as it appears within the context of this research. *Idiography* is the third major influence of IPA which concentrates on the particular (i.e., in the first instance idiography is concerned about detail) and IPA is concerned about examining the details to get to the main themes that will shed light on the person's experience. IPA draws from these strands to establish itself as being phenomenological in that it seeks to provide an insider perspective of the lived human experience, while in being interpretive it involves a double hermeneutic process: the researcher, on the one hand, is trying to make sense of the research participant, who (the participant) is in the process of trying to gain meaning or understanding of the lived experience. This creates an ongoing hermeneutic cycle as both are involved in an interpretative process (Smith et al., 2009; Fade, 2004).

This researcher adopted the IPA approach as this research sought to provide the BYOD risk considerations in the South African organisation, without revealing to interviewees known BYOD risk scenario constructs from which they could choose to answer a list of questions. IPA is a process in the sense that data analysis searches for and constructs themes to relate the way a phenomenon is understood or experienced (Willig, 2001). The research process, using IPA, is inductive in approach, aiming not to test hypotheses or to assess a set of assumptions but to allow interviewees the freedom to narrate and interpret, and gain an understanding of their own lived experience of a phenomenon.

This approach permitted this researcher to gain a detailed understanding of each interviewee's perception and experience with BYOD, and from that, to establish the meaning of the phenomenon studied (BYOD risks). The case study approach provided an appropriate fit within which IPA was employed as IPA questions should always be asked in an open and expansive manner, allowing for the case study's 'thick narrative'. The aim of the research was to establish how creating themes from analysing the data matched with constructs or factors that were found from the literature review on BYOD phenomenon, and even more specifically, its risks. IPA was useful in this respect as it helped in the analysis of data by constructing content themes that emanated from an interviewee's perceived experience regarding the BYOD risks.

Another advantage in using IPA was that it allowed the interviewee to hear his or her own interpretative proclamations, and to avoid what Dreyfus (1998) called the 'tendency to over-rely on rationality'. It instead allowed scope for the emergence of intuitive wisdom and helped this researcher learn more about this. Additionally, the interviewees were able to create the meaning of phenomenon (BYOD) in their lives and better understand related perceived risks.

3.6 Case study as method of choice

According to Yin (1994) the selection of the research methodology depends on three factors: 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. This research has adopted a case study approach as it is extensively applied in similar areas and disciplines, including IS and technology research (Zainal, 2007; Walsham, 1993). Case study methodology appropriately suited the focus of this research – BYOD phenomenon in the South African organisation, with a particular concentration on risk considerations. This methodology helped to induce (through in-depth interviews) and interpret (through IPA) the studied phenomenon through rigorous study of "a single unit for the purpose of understanding a larger class of similar units" (Gerring, 2004, p. 342).

There are three approaches mainly used in case studies: exploratory, explanatory and descriptive. Exploratory case studies are usually undertaken in the early stages of the

research process to establish the research questions and hypotheses, which was the case with the introduction of BYOD and the associated risks. Explanatory case studies are best suited when causal studies are undertaken. Descriptive case studies work around formations of a descriptive theory and expect the possibility that problems may occur during the research project (Tellis, 1997).

Babbie and Mouton (2002), describing case studies as the intensive investigation of a single unit that may include the examination of multiple variables, mention six different types of case studies:

- Individual/single case study;
- Community case study;
- Social group study;
- Studies of organisations and institutions;
- Studies of events, roles and relationships; and
- Studies of countries and nations.

There are two reasons why social scientists view case studies as useful (Thacher, 2006): the first is that they help to identify causal relations, and the second is that they provide an understanding of the worldview of a person being studied. The former approach is associated with comparative case study research, while the latter is associated with hermeneutics, aimed at understanding the subjective meaning people attach to their experiences, which was the case in this research. Yin (1994) asserts that case studies are applied to understand complex social phenomenon because they allow the researcher to study real-life events while retaining their holistic and meaningful characteristics.

Tellis (1997) expounds on case studies as being multi-perspectival, meaning that a researcher's approach in analysing data considers not only the views and perspectives of an actor, but the researcher remains aware of other relevant groups of actors and the interaction that occurs between them. A case study's unique virtue is the depth or otherwise the richness, completeness and wholeness in the processes of analysis, providing a better understanding of complex social phenomena (Gerring, 2004), such

as explored in this research, as the introduction of BYOD in an organisation is not solely technological but also a social (e.g. technological culture) and organisational occurrence.

3.7 Limitations of qualitative case study method

The criticism against case studies is that (i) they fail representativeness in observations of social phenomena and (ii) they lack strictness in the collection, analysis and construction of data. In other words, the first criticism against case studies is that it is difficult to make generalisations using the method, and in the second instance, the biased nature of the researcher will impact the rigour of the research in progress (Hamel et al., 1993; Patton & Appelbaum, 2003). Table 7 below represents the strengths and weakness of case studies (Marzanah, 2009).

Table 7.

Case Study Methodology: Strengths and Weaknesses

Strengths	Weaknesses
Excels in understanding complex issue or object and can extend experience or add strength to what is already known through previous research	Lack of control variables
Captures the local situation in greater detail and with respect to more variables than is possible	Different interpretations by different people
Applicable to real life, contemporary, human situations and its public accessibility through written reports	Unintentional biases and omissions in the description due to intense exposure to the study
	Study of a small number of cases can offer no grounds for establishing reliability or generality of findings
	Case study research as useful only as an exploratory tool

Note. Retrieved from An investigation into methods and concepts of qualitative research in information research (p. 53), Marzanah, A. J., 2009, Computer and information science, 2(4). Copyright 2009 by Computer and information science.

However, Gummesson (1991) criticizes natural sciences' own shortcomings and suggests that case studies create the opportunity to gain a complete view, instead of the reductionist-fragmented view of the research process. Riege (2003) establishes

that qualitative methods such as case studies follow a mode of inquiry for discovering new relationships of realities and for explaining the meaning the experiences rather than verifying results based on predetermined hypotheses.

Andrade (2009) refers to Yin (1994) who, as a positivist scientist, warned about case study's weaknesses in that the methodology has its limitations to achieve adequate precision, objectivity and rigour. Moreover, Yin (1994) cautions that for the interpretive researcher this warning should apply even more if the aim is to construct a case study designed to satisfy criteria such as reliability, internal and external validity and provide its own set of problems to positivists (Andrade, 2009). The difference between the qualitative approach in case studies and the quantitative approach is that in the natural sciences the methods of reasoning are deductive, whilst qualitative methods use inductive approaches in the processes of analysing data (Patton & Appelbaum, 2003; Benbasat, Goldstein & Mead,1987). Lubbe (2003) mentions that case studies can rarely be unbiased, offering three obstacles why unbiased testimonials are difficult to obtain:

- Individuals encounter difficulties to remember accurately;
- Individuals are inhibited to disclose important feelings; and
- Individuals are suspicious to reveal information that reflects poorly on them or their seniors.

However, Andrade (2009) supports the argument by Orlikowski and Baroudi (1991) that case studies based on an interpretive approach and used in IS research have produced viable interpretive knowledge into human/technological interaction in a natural social setting. A researcher engaged in the qualitative and interpretive case study is actively part of the procedure used for data gathering and analysis (Morgan & Smircich, 1980; Morse, 1994; Creswell, 1998; Klein & Myers, 1999), and this close involvement with the research participants causes the researcher to become a 'passionate participant' (Guba & Lincoln, 1994). Therefore, being so enthusiastically part of the research is advantageous as interpretive research can provide the researcher with the chance to document his or her "point of view and translate it into a form that is intelligible to readers" (Neuman, 1997, p. 72).

3.8 Measures to strengthen qualitative case study

In qualitative research, the measures to positivism are that credibility becomes the accepted measure of internal validity, transferability over external validity and dependability is exchanged for reliability. Whereas internal validity is the degree to which variations in a result can be connected to variations from a controlled variation in a dependent variable, reliability must confirm that representation of a causal relationship is truthful in mirroring the way things really are (Guba & Lincoln, 1989; Sørnes, 2004). In this research, reliability was applied by exploring the relationship between causes of BYOD risks and their possible adverse effects on organisation using the BYOD.

External validity is the description and applicability of findings to a generalised field, whereas transferability is the ability of the researcher to give sufficient detail (e.g. interpretations, explanations and predictions) from their results to compare with the research of other settings. In relation to this research, enough detail for external validity will be given in this study, allowing other researchers to validate the findings in another setting.
Reliability refers to a trusted technique that can deliver the same result several times over to the same object, offering data that is stable and reliable over time, while dependability has as its goal the documentation of the decisions and interpretations arrived at about the processes followed and conclusions reached (Guba & Lincoln, 1989; Sørnes, 2004). In this research, reliability is ensured by selecting a trusted research methodology (case study methodology) which ensured epistemological reliability.

3.9 Case study research design framework

Patton and Appelbaum (2003) developed an action process, or roadmap, when doing case study research, which includes the following steps:

- **Determine the object of research**: the researcher must decide on the topic of the case;

- **Select the case**: the researcher will strategically identify the applicable case that fits the object of research;
- **Build initial theory through a literature review**: the literature will assist to frame the case study and to establish the validity/reliability and confidence in the findings;
- **Collect and organise the data gathering**: establish appropriate instruments and protocols that focus on the object of the research to avoid being flooded with overwhelming amounts of data;
- **Analyse the data and reach conclusions**: The ultimate goal of the case study is, having established the context, to proceed with data in uncovering patterns, establish meanings, formulating conclusions and building theory.

Welman and Kruger (1999) suggest that a number of aspects must be considered when conducting case studies:

- The case must be studied within specified parameters;
- Irrespective of the data collection techniques used, the purpose of case studies is not to describe what is observed, but to inductively identify recurring patterns and consistent regularities; and
- Triangulation is frequently used in discerning such patterns (e.g., tape recordings, semi-structured interviews, newspaper reports, documentation, archival records and physical artefacts are ways to corroborate findings of a research project).

There are several methods for collecting data for a case study. The format and pattern of the research determine the nature of the data collection methods and its execution. Qualitative data collection utilises rich and diverse data to answer questions on the variability and complexity of human life. Yin (1994) illuminates six different sources of evidence, presented in Table 8 below.

Table 8.

Case Study Method – Sources of Evidence

Source	Types
Documents	Communiqués and written reports Administrative documents Formal studies or evaluations Newspaper and articles from mass media
Archival records	Service records Organisational records Maps, charts and lists Survey data and personal records
Interviews	Open-ended nature Focused Survey
Direct observation	Formal data Casual data
Participant-observation	Being resident in a neighbourhood Functional role in an environment Staff member in an organisational setting Being a key decision maker
Physical artefacts	Technological device Tool or instrument A work of art Other physical evidence

Note. Adapted from *Case study research: Design and methods* (p. 10), Yin, R. K., 1994, Newbury Park, CA: Sage Publications, 2nd Edition.

For most case studies, semi-structured in-depth interviews are vital sources of evidence, while questionnaires, documents, archival records and physical artefacts are used to support and corroborate the evidence found by interviewing participants. This researcher used primarily in-depth interviews and written information (e.g. documents such as IT policy and the like) and adopted the idiographic case study approach that permitted for a small sample of the interviewees' lived experiences (Smith et al., 2009).

3.10 Generalisation and validity issues

This research developed themes or concepts to interpret its findings. According to Punch (1998), case studies can offer results for general applicability in one of two ways: by conceptualising or developing propositions. *Conceptualisation* is the creation of concepts or themes as a means of defining complex issues emanating from qualitative studies of an in-depth nature. In the second instance, a researcher develops propositions around a hypothesis that seeks to link factors or themes within a particular case.

This research adopted the first approach in developing themes or concepts, and to generalise the results in relation to the constructs or factors from user satisfaction theory. In other words, this research explored connections from themes emanating from IPA with BYOD risk-related factors or themes found in the literature. This research did not seek to create linkages between the concepts or themes emanating through IPA and what exists in the literature. Instead, it was to find connections across case and literature references as a way to provide a richer description of the phenomenological reality of the interviewee. IPA is not an inductive approach in the way that grounded theory is, namely, working toward creating a theory, nor does it follow a deductive pattern aimed at establishing linkages or correlations with a particular hypothesis or theory (Punch, 1998). Thus, IPA is rather producing an in-depth study of experience seeking for meaning and formulating a unique set of themes particular to the case being studied through a process of hermeneutical enquiry which is deeply specific to the phenomenon under investigation.

This research focused on BYOD risk considerations as an interpretative experience, from which users create meaning about that experience. User experience emerges throughout the phenomenological awareness through an inductive process describing the perceptions of possible risks introduced by BYOD.

3.11 Sample description

The sample of any research project is to provide linkages with the purpose of the research and is selected based on certain variables in order to corroborate a theory or

hypothesis. In qualitative research, the sample is derived from an array of social data categories that in terms of findings are recorded as statements of subjectivism rather than statements of objectivism.

According to Bless and Higson-Smith (1995) *sampling* is the selection of "objects, persons, events… from which information will be drawn" (p. 85). We can differentiate between probability and non-probability sampling: with probability sampling, there is a fair expectation that the selected sample can be determined based on certain variables against that of the whole population; with non-probability sampling, there is no certainty that outcomes of the findings are representative of the whole population.

Although the advantages of probability sampling are higher than that of non-probability sampling, in terms of generalisation, non-probability sampling is useful as it can save on cost by enlarging the sample in homogeneous groups. As the latter is frequently used in social sciences, this research's sample selection corresponds with its non-probability categorisation; and for good reason, since IPA contends that idiographic case study allows for in-depth exploration of a phenomenon (Bless & Higson-Smith, 1995).

The sampling was completed by selecting fifteen employees from Organisation A, a medium sized South African-based IT security consulting and service management organisation which has recently experienced business expansion and thus an increase in the number of its employees utilising their personal devices at work-place. The chosen interviewees were selected based on predefined criteria (purposeful sampling). Although the interviewees involved five females and ten males, the gender element did not play any significant part in this research.

3.12 Data collection

As described previously, the data collection process was focused on risk factors related to the BYOD in the South African organisation. In that regard, the data is collected by following the case study methodology guidelines (i.e. the main method of data collection was in-depth interviews). This approach allowed for "detailed descriptions of situations, events, people, interactions, and observed behaviours;

direct quotations from people about their experiences, attitudes, beliefs and thoughts, and excerpts or entire passages from documents, correspondence, records and case history" (Patton, 1990, p. 22).

The data gathering techniques include the following: (i) literature review, focused on BYOD related risk considerations; (ii) in-depth interviews; and (iii) documentation to the implementation process of BYOD.

The data collection process allowed for the following:

- Establishing general information criteria (job designation, department, male, female etc.);
- Exploring IS user satisfaction issues (computer self-efficacy; IS training related experiences; motivation and drive in IS usage etc.);
- Exploring IS interactive phenomenon (listening to the user's narrative on BYOD risks); and
- Exploring shared meaning between IS/Institutional and user objectives (searching for a common understanding between institution's IS objectives and users IS behaviour in this respect).

When collecting data for this research, careful attention was given to accuracy, appropriate methods and integrity of the collected data. This research used semi-structured, in-depth interviews, conducted in a manner that allowed participants to enjoy freedom in determining the process of enquiry. This is acceptable in IPA as the interview schedule was used in a flexible manner, and even "when it is preferable to abandon structure and to follow the concerns of the participant" (Smith et al., 2009, p. 64). Likewise, Jarratt, (1996) expresses that interviews can follow an open structure to enable the exploration of "unexpected facts or attitudes" that may emerge.

3.13 Analysis and interpretation of data

According to Inglesant (2007), an analysis is not of a user's experience alone, but of the user interacting with technology: the dialogical encounter between self and other. This research moved deeper into this perception while seeking to identify and interpret

that moment when a user assumes the meaning of the experience is or has occurred; this is what is meant with IPA.

The researcher must, in the use of qualitative methodology, possess certain personal qualities – insight, imagination, logic, judgement, and the ability to form accurate impressions and see relationships. In terms of the interpretation of data, inductive reasoning methodology was applied as already discussed. Inductive reasoning works by scanning the detailed field of information, then moving toward more abstract generalisations and ideas or themes. The IPA approach provided the foundation for the generation of themes that formulate the research findings (Neuman, 1997).

In the final analysis, it is the detailed interpretation of the transcripts that establish what generalisations can be arrived at in terms of user perspectives on user satisfaction measures of success. Although this researcher was the one doing the analysis, the understanding remained that the interviewee who was undergoing the experience was the one who created the experience (Geven, Schrammel & Tscheligi, 2006).

With IPA the transcripts were analysed individually to identify themes and afterwards to integrate and create meaningful clusters within which themes were categorised based on the cross-sectional analysis. There are a number of steps to follow when adopting IPA. An analysis is typically described as being an iterative and inductive cycle. Furthermore, according to Smith et al. (2009), this cyclical process may involve a number of strategies:

- A line by line analysis of experiential claims, concerns and understanding of each interviewee;
- Identifying emergent themes;
- Coding data as a result of dialogue between researcher and interviewee of the meaning of aspects emerging within the interview;
- Constructing a framework illustrating relationships between themes;
- Developing a format showing the process from start to end in the development of themes, from initial comments to a final list of the identified themes;

- Collaborating with the help of others to establish coherence and plausibility of interpretation; and
- Creating a narrative of the themes to describe the interpretive meanings of the data.

3.14 Stages of analysis and interpretation

A series of stages were followed when analysing each individual transcript. The initial stage included reading and re-reading individual transcripts. This stage placed the interviewee as the focus of analysis, while this researcher tried to make sense of the world as perceived by the interviewee (Smith et al., 2009). Next, this researcher interacted with the text remembering instances of the interview experience itself and recording some observations from the transcript, which were then scribbled into a digital notebook and bracketed off to prepare for analysis.
In this phase, this researcher remained focused on the data and proceeded to read and re-read the texts until the structure of the interview begin to take shape as a 'listened' narrative was unfolding. Additionally, this researcher experienced the ebb and flow of statements shifting from the generic explanations to communicating about more specific examples of a particular event.

The next stage of the analysis involved a more detailed exploration of semantic content and language usage. This researcher needed to understand the way the interviewees thought about, talked about, and understood a particular issue. Although the analysis of the text was freestyle, not having to assign meaning units and comments to every part of the text, the function of this initial noting was to extract and provide descriptive core comments that have a clear phenomenological focus, such as key issues related to the risks of BYOD phenomenon that matter to the interviewees and provide meaning to them (Smith et al., 2009). This researcher was then able to follow an interpretive cycle by picking up on language and thoughts and identifying abstract conceptual constructs on which to build his own narrative of the meaning portrayed within the research.

The third stage was to accumulate a vast set of data from the comprehensive notes of exploratory comments. Next, while working through this data, emerging themes were

generated. The task to identify emerging themes was to map the interrelationships, connections and patterns between the exploratory notes. (Smith et al., 2009). At this stage of theme building, this researcher was more analytically engaged with the exploratory notes, proceeding with the analysis of data in meaningful chunks, rather than becoming too attached to the original transcript. Themes were corresponding to the data since the meaning of the data was clearly captured within the themes.

The next stage of the analysis was to create connections across the themes. Themes needed to fit together when there was a shared meaning with the interviewee's narrative; otherwise, this researcher decided not to incorporate themes that were not relevant (Smith et al., 2009). Then, this researcher pored over each transcript and scanned for shared themes from the rich data sources to integrate common issues identified among interviewees.

The reason for integrating themes is to establish the structure of the salient aspects of the interviewee's account. The researcher's influence on the theme building structure, and what it suggests about the processes of data analysis, falls within the hermeneutical journey for making sense of the interviewee's account. As such, this researcher approached the text strictly adhering to what the interviewee was describing. This is also supported by Schneiders (1999) who asserts that "meaning arises in the interaction between texts and readers" (para. 3). Correspondingly, Myers (1994) establishes that similarly to a literary text, data gathered via in-depth interviews also composed from text that can be further analysed. Following this, keywords, motifs and themes were created by analysing the gathered data in this research. Therefore, the final analysis resulted in connections made across the research (Smith et al., 2009).

In the above regard, this researcher identified and defined the themes within this research, assisting in the meaning-making of each interviewee's account, while also keeping in mind the original focus of the research – risk considerations related to the BYOD in the South African organisation. Lastly, themes developed through IPA have guided the combined literature review and empirical answers to the research questions of this research.

CHAPTER 4: FINDINGS AND DISCUSSION

The reviewed literature in Chapter 2 uncovered possible benefits and risks that may emerge from the introduction of BYOD. This chapter presents the findings of the interviews completed by utilising IPA. Alongside the main question, there were five sub-questions in this research. The first sub-question was answered by extracting and analysing data from the literature review and remaining four were answered by combining a literature review and empirical research analysis. The answers to these sub-questions are reported in this chapter.

4.1 BYOD in Organisation A

In the introductory part of the interview, all interviewees confirmed using some form of mobile device in their organisation. Moreover, most reported having two different personal mobile devices, such as a laptop and smartphone, which they use for both work and personal purposes. For instance, when asked about the utilisation of personal mobile device in the workplace, Interviewee 2 confirmed "*I use my own smartphone as well as a laptop*".

This high presence of mobile technology in the personal lives of the individuals employed in Organisation A is in agreement with the previous research conducted in South Africa by World Wide Worx (2012) and presented in Chapter 2. According to that research, it was projected that around 10 million mobile phones would be sold in South Africa in 2013 and it was estimated that this number would increase significantly every following year. More recently, it was reported that 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).

Additionally, Meeker (2015) established that in South Africa, the BYOD trend appears to be rising gradually and is expected to continue growing as the number of smartphones increases even further and employees progressively utilise them in their work-place. In line with the interviewees' responses, it was determined that Meeker's projections have been fairly accurate and that interviewed employees of Organisation A are a good example for the advancement of the BYOD phenomenon in South Africa.

4.2 Awareness and general knowledge of BYOD phenomenon

When questioned if they have ever heard about BYOD, all interviewees except interviewee 10 responded with "*yes*". Interviewees were from different departments within Organisation A and were not asked to define the BYOD term in detail as it was not required for the purposes of this research.

On the other hand, the literature reviewed in Chapter 2 established that there is a strong awareness of the BYOD concept among South African employees (Twinomurinzi & Mawela, 2014). This was confirmed during the interview with employees from Organisation A as they provided a variety of opinions on this subject, corresponding with the findings from the literature review. Furthermore, this wealth of information provided by the interviewees was also a confirmation that the selection of interview participants from Organisation A was appropriate for the purposes of this research.

4.3 Importance of allowing employees to use their personal mobile devices in the work-place

Eleven out of fifteen interviewees shared a common viewpoint on the importance of allowing employees to use their personal mobile devices in their work-place. For instance:

"*I think at the end of the day it... [sic] It allows the employee to be more productive because he is working with the tool that he is used to and he knows the look and feel*". (Interviewee 9)

"*I think it's quite important. I mean everybody uses a phone now days [sic] so obviously you want to be able to use it*". (Interviewee 7)

"*If the company does not supply the employees with the phone they feel that is required, then to stay with technology most employees has got [sic] a phones that they would like to use and then they use [sic] to the benefit of the company even if it's their*

own device. I would say it's a good thing". (Interviewee 2)

These interviewees' viewpoints were also supported by the literature review. For instance, Reddy (2012) stated that 'the genie is officially out of the bottle' as BYOD brings the promise to further improve employee satisfaction, productivity and work-place flexibility while at the same time benefiting the organisation.

On the other hand, four out of fifteen interviewees were of mixed opinions and expressed certain concerns, mostly related to security risks, IT support challenges and productivity. For illustration, even though Interviewee 6 pointed out the importance of allowing personal devices in Organisation A as positive, he was still concerned about potential challenges that technical support might experience when supporting employee's BYOD devices:

"*Mixed opinion. So, in terms of personal, they are linked to their personal world and I think it is very important because the world we are living in is very connected and that's become the norm. So, to cut people off from that on work would be unreasonable and not a place I would desire to work in. To use their personal mobile device for work specifically, I feel there's a bit of challenges there and it becomes difficult for the support infrastructure."*

The response recorded from Interviewee 6 was consistent with research by McLarty (2012), as he cautioned that employers who do not fulfil the employees' BYOD requirements might experience unnecessary risk having an 'old-fashioned' corporate image, and Downer and Bhattacharya (2016), who claim that supporting BYOD devices while trying to achieve financial savings related to the overall cost of support is another major obstacle for successful implementation of BYOD.

Similarly, two interviewees outlined the benefit of improved communication while also expressed their apprehension:

"*It got [sic] its benefits, you can at least chat to someone quickly if you need to talk to somebody out of your organisation…but obviously it's got [sic] its risk especially in security company*". (Interviewee 5)

"*Bringing it to work is fine, otherwise it's a big security risk and it distracts employees as well*". (Interviewee 13)

Additionally, Interviewee 12 believed that only certain employees should have the opportunity to use their devices for business purposes:

"It is a good idea in some instances but not for everybody. If you need 24-hour access then it's good, but otherwise, no".

These findings were mirrored in studies by Reddy (2012), Keyes (2013), McLarty (2012) and ENISA (2012,2017) as presented in the literature review. In general, the majority of interviewees agreed that it is vital to allow personal mobile devices in the organisation, not only because of the benefits that BYOD introduces but also for the reason that it's the norm of this interconnected and technological world in which we are living.

4.4 Benefits of BYOD

Starting with the operational BYOD benefits, most interviewees agreed that the most common ones 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.

For instance, Interviewee 2 stressed the importance of being able to choose your own device, which in return might provide additional convenience and boost employee productivity and motivation:

"*It's also the question of what technology to follow, what operating system you [sic] more familiar with; if you like Android and you are forced to use Apple, then you are*

going to be unhappy and vice versa…By using a device, that you are comfortable with you [sic] most likely will [sic] be working after hours and be available pretty much 24/7".

Interviewee 5 pointed out the benefit of team collaboration:

"*Benefits, there's a lot, especially if your work in a team. You [sic] use WhatsApp and you create a group, send a message 'Guys I got a problem' and someone will help you out without you having to phone them*".

Furthermore, interviewee 9 agreed with colleagues, claiming that benefits of BYOD phenomenon outweigh possible risks:

"*Benefits once again it comes down to familiarity; it also comes down to the fact that, if I have my email, for example, coming to my favourite device, which I like, and I like the feel, I am going to look at email and see what is about and within a few seconds am [sic] going to know what email is about and reply or maybe reply to it later [sic]. Where if this is not available to you, you only see it once you get home... Open up your laptop; you need to dial a VPN or something to access your mail...Yeah, I just believe that benefit outweighs the negative, in that instance*".

The importance of familiarity with a preferred device that was mentioned by Interviewee 9 was echoed by two other interviewees:

"*From the productivity point of view, users are able to use a handset they are familiar with; they only have to carry around one device because if you have the corporate a device you provide, employees will end up having their personal one and a corporate one they need to carry around. So, from the user perspective definitely benefits if they can use their own device* ". (Interviewee 11)

"*I think benefits are fairly obvious to me. The training is one of the things because it's nicer and easier to train, people already know how to use their own personal devices... And it puts technology in their hands* ". (Interviewee 6)

Much of what was previously analysed and established in the literature review with regard to the operational benefits of the BYOD was also confirmed by interviewees, as seen from the previous examples. For instance, Song (2013) outlined that employees now require more flexible working hours and expect IT departments to provide them with appropriate technology to support such work-related arrangements. Moreover, Reddy (2012) established that freedom to use personal devices of choice not only improves operational efficiency but also provides higher satisfaction levels and motivation of employees, and Wood (2012) ascertained that BYOD can help boost employee productivity while increasing job satisfaction and improving creativity.

Next, the financial benefits of BYOD as presented in the literature review were also widely recognised by almost all interviewees. However, views were slightly divided as the six out of fifteen interviewees were confident that BYOD financially benefits the organisation – decline of hardware investment (Wood, 2012), speeding up adoption of technology (Calder, 2013), employees paying for the cost (Citrix, 2013; Keys, 2013) – whereas five out of fifteen interviewees were of opinion that BYOD provides more benefits for employees – increased productivity and remote working (Song, 2013). For instance:

"*For the company very clear financial benefits as they get the user to buy the hardware. For the end user I can't see any financial benefits it's actually almost the transfer of the cost to you and it raises the question like "What happens now if there is a problem with your phone?".* (Interviewee 6)

"*From the costing perspective, not having to purchase handsets specifically for employees is the cost benefit to the company but just to mention that in contrast to that there is an additional cost that needs to be considered from the support perspective*". (Interviewee 11)

Concerns stated by Interviewee 11 relating to support also align with research presented in Chapter 2. For instance, Reddy (2012) stressed the need to create dedicated BYOD support infrastructure; Pillay et al. (2013) warned about increased cost related to infrastructure and compliance; Song (2013) explained difficulties

organisations experience when trying to identify costs related to voice, data and support.

Organisational BYOD benefits were delineated in the literature review and also commonly recognised by interviewees:

"Organisational benefits it [sic] would most definitely make employees more efficient. If you have to take out your laptop or have the workstation and every time the mail [sic] comes in you are not around your laptop then you are going to wait until you are actually back at front [sic] so its something that can be dealt [sic] very quickly". (Interviewee 2)

"There is a big organisational benefit. One of our challenges is to get everybody onto a unified system for collaboration…". (Interviewee 6)

"And when we use our phones like in my team, we will message each other on WhatsApp to tell each other quickly, 'what's going on?'. So obviously we can collaborate quicker and find out quicker what's happening with other people in our team". (Interviewee 7)

"I think it is actually very good, also especially with working hours and also partnerships and that also very good [sic]. In terms of client base, I mean it is exactly what the client need especially, say for after-hours and that [sic], to basically have your own device". (Interviewee 4)

The main conclusion, evident from this portion of the interview was that there is a consensus among interviewees regarding potential benefits introduced by the BYOD. This is reinforced by the different academic views presented in the literature review. Furthermore, all interviewees confirmed that this researcher has sufficiently covered this topic in the literature review by agreeing with the listed benefits (Appendix C).

Finally, it can be established that while these previously mentioned and perceived benefits of BYOD are the main reasons why organisations consider this phenomenon,

alongside that this concept also appears to be the norm of this contemporary interconnected and technological world in which we find ourselves. Additionally, this provided an answer to sub-question number two of this research.

4.5 Risks associated with introduction of BYOD and their nature

This section summarises the identified risks that can be introduced by BYOD phenomenon and provides an answer to the research sub-question number three. A detailed literature review has revealed that these risks can be logically grouped into five categories, as revealed in Table 9. Additionally, for more clarification, this researcher assigned a perceived criticality to each BYOD risk category, according to the information gathered from the interviewees of Organisation A.

All interviewees strongly agreed with categories of BYOD risks as presented by the researcher and covered in the literature review. However, their responses and viewpoints varied slightly as there were different concerns amongst them, all depending on their position within the organisation and how they perceive risks of BYOD. Nevertheless, the biggest shared concern of all interviewees was related to the technological risks, as confirmed by thirteen out of fifteen interviewees, also indicated in Table 9 along with the perceived criticality (i.e. the number in the brackets, last column). Technological risks were followed by human aspects (eight interviewees) and legislation, regulation and privacy risks (seven interviewees).

In contrast, implementational and organisational risks were found to not be the highest concerns in Organisation A; however, they were deemed as important as confirmed by five out of fifteen interviewees. Lastly, technological risks such as “jailbreaking” and “contamination of data in cloud storage” that were identified in the literature review, were not definitely confirmed during interviews with employees from Organisation A; this researcher therefore suggests that additional research pertaining to similar subjects be undertaken in organisations in South Africa to confirm validity and applicability in the local context.

Table 9.

Comparison of Previously Categorised BYOD Risks with the Information from Interviews

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 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 policies (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)

Turning to the aspects of the human risks, Interviewee 1 was worried about his personal data on the BYOD device and potential personal financial damage:

"*The data they can steal, they can get access to your banking account…*".

Similarly, while Interviewee 11 was concerned about the data leakage, he was even more concerned about the possibility that his phone can be compromised via unknown malicious application (technological risks) without him knowing about it:

"*Data leakage is the biggest concern. If device gets stolen… any potential person picking up your phone can have access to your corporate data. However, if a phone gets compromised via a malicious application, that's a second risk where data can be extracted without even someone knowing and that is even a larger risk*".

As mentioned previously, concerns related to various technological risks posed the single biggest apprehension recorded by a number of interviewees from Organisation A. In addition, Interviewee 4 was concerned about using insecure public WI-FI connections when he is out of the office:

"*Hackers and theft, especially if you are out of the organisation and you are working in the mall for the example*".

Interviewee 9 had similar concerns related to technological risks, more specifically to organisational mobile devices that might be infected by unknown viruses and a chance that a virus might spread through the entire network of Organisation A:

"*With mobile devices, we are seeing viruses and those type of stuff happening there. Now you are bringing those devices inside your network so now, of course, you are exposing your network, your infrastructure to the viruses that it [sic] might be coming in, through a way that you don't have control over in a traditional sense. You know that users got [sic] his Android or iPhone, you don't necessarily know what virus is lurking on those devices and once that connects to your network it might just spread to your entire network…* ".

On the other hand, Interviewee 6 expressed his unhappiness about the fact that in his department it is mandatory to install MDM application on a personal device used for BYOD to access organisational email. Furthermore, he also pointed out privacy concerns when using the BYOD concept in Organisation A (legislation, regulation and privacy risks):

"*This is where I feel very strongly negatively in favour of BYOD and based on my interaction with this in the past… You need to install the MDM app to get access to your email and all of those, but I am not comfortable with it as it becomes a device administrator on your device… So, I would love to have access to my email but I don't want something taking over my phone and requiring all these security measures... And it is very difficult to divorce that from your personal use of the phone... And also, it is monitorable so I can only trust that policy of security team that they are not monitoring my personal data, but they have complete access to it if I accept the policy*…

In addition, the same interviewee articulated concerns related to the implementational risks:

"Yeah, I think risks there are fairly high in my opinion so and specifically from my background...So to support so many different devices there is so many variables. For me, it increases the cost of support because I have to eliminate the bunch more variables now due to varied nature of the hardware. Because if they are using the company's hardware in the company's office they are all constant they are not variables. So, it increases support and in terms of policy will be just training and compliance. The cost of doing that will be quite high."

Similar to Interviewee 6, concerns related to the legislation, regulation and privacy were also echoed by another interviewee:

"*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. All your emails, all your Facebook [sic], everything and for me it's such a huge privacy issue that I don't bother to put that on*

my cell phone because I don't want them to have access to my personal information". (Interviewee 7)

The responses provided by Interviewee 6 and 7 (legislation, regulation and privacy risks) show that their unhappiness with current BYOD approach in Organisation A and refusal to install MDM application can potentially have negative risk implications. This is also supported by the literature review, as for instance, Garba, Armarego and Murray (2015b) 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. In addition, Leavitt (2013) claims that employees which 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.

Therefore, it is recommended that organisations, at a bare minimum, have an official BYOD document that is understood and signed by all employees to make certain that all BYOD risks related to legislation, regulation and privacy challenges are suitably addressed. Likewise, it can be said that it is important to provide BYOD education and training to employees, to find a sense of balance between risks and security so that business progression is not blocked (Steven, 2013).

Turning to Interviewee 5, he appeared to be most worried about organisational risks:

"*Organisational risk; from company's perspective, it's quite a big thing I think. The company should insure that all policies are setup and all users are educated because if you don't have that and the user do whatever they want on their phone within the network of the company they could compromise the entire system. I mean if you can get through or onto a network you are potentially in [sic] everything that the company holds; be it in this office, the data centre you will gain access to that, so it is quite important for company to make sure they have policies setup and educate users from the start*".

In view of the findings above, it can be established that most risks related to the BYOD phenomenon are predominantly technological in nature and that security of BYOD is as important as the functionality and cost when developing and implementing a BYOD solution. This also provides an answer to sub-question number four of this research.

Moreover, this research confirmed that BYOD strategy that does not consider needs and concerns of employees can lead to their unhappiness and potentially force them to be less productive at work, and subtly encourage them to bypass organisational BYOD security mechanisms (e.g. MDM solution – Interviewee 6 & 7). Consequently, the organisation may be exposed to serious risks.

Concluding the previous sections, the interviewees confirmed a validity of identified risks from the literature review, illustrated below in Table 10 in the final form. Having confirmed the identified risks from the literature review, the next step was to empirically test the proposed BYOD risk management model.

Table 10.

Empirically Confirmed BYOD Risks

PRIMARY RISK THREAT CATEGORY	BYOD SPECIFIC RISK
Implementational	Protecting data, ensuring security, providing support
Technological	Malware
	Risks and vulnerabilities due to 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.

4.6 Optimal approach to manage and minimise BYOD related risks in Organisation A

The proposed BYOD risk management model (Figure 10, Chapter 2) was applied to establish an optimal approach to address BYOD related risks. The elements of this model were used for posing the interview questions as well as for analysing interviewee answers and establishing appropriate themes.

4.7 Securing mobile applications

In this part of the interview, thirteen interviewees overwhelmingly confirmed that either they do not think their organisation is utilising any methods to secure mobile applications or they were not certain what those methods are. For instance:

"They should actually enforce it in our company as well which up to now, they've not done so ahhm [sic], I don't really have a view because there is no policy in place". (Interviewee 2)

"As to what those steps are I don't know". (Interviewee 9)

"No, there is no prevention of any of it". (Interviewee 12)

Only interviewees 5 and 8 somewhat confirmed that their organisation is utilising a technological solution such as MDM to secure mobile applications:

"We have MDM we use for BYOD app testing". (Interviewee 5)

"I definitely think that mobile device management and the firewall are pretty strict. This is adding to the security of mobile applications" (Interviewee 8)

Even though MDM itself is a good technology for these kinds of risks, it is not sufficient on its own; hence the sound security of mobile applications is an important factor for lowering risks related to the BYOD. For instance, Syed Hussain and his colleagues (as cited in Bertino, 2016, p. 9) which are considered to be leading academics in the

field of application security, recently proposed an algorithm that monitors database applications for anomalous behaviours. Furthermore, Bertino (2016) recommended a similar approach for BYOD to secure mobile device applications that employees freely download from the public application stores (e.g. Google Play, iTunes, etc.) in addition to an MDM solution. For instance, when using static application lists that are normally available via various MDM solutions, a list of the expected behaviours of the mobile application can be created and monitored at runtime for anomalies (Bertino, 2016).

4.8 Risk compliance frameworks

Eight out of fifteen interviewees were unsure if Organisation A uses any risk compliance frameworks, whereas a further six interviewees were quite confident that Organisation A does not have or utilise any. Moreover, Interviewee 9 provided a very interesting piece of information, helping this researcher better understand the current state in Organisation A when it comes to the implementation of risk compliance frameworks:

"*We've got ISO 27000. We are looking at that, it is once again something. It is within our organisation but if you would like, if you ask me to have a look at our ISO 27000 document, we won't be able to give you a document. We might give you a little bit of snippets and you would be able to make out "Ok we can actually see where they are coming from... So once again it is something that it's there, but it is not something that is actively being driven*" (Interviewee 9).

This provides valuable input to the researcher, confirming findings from the literature review by Twinomurinzi and Mawela (2014) who ascertain that organisations seem reluctant to formally develop BYOD strategies which leave them open to many risks. The same situation seems true in Organisation A considering information provided by interviewee 9 and other interviewees.

Despite the fact that many risk compliance frameworks do not address directly the BYOD risks and concerns, they are popular among organisations worldwide because they can be a valuable tool for the reduction or mitigation of BYOD risk in general. Additionally, they can also be a starting platform for developing an organisational risk

management model. Kearns (2016) points out that a risk management model should not only be detailed and efficient but also transparent as well, as transparency can promote ease of communication through all levels of IT departments (e.g. support, specialists, management, executives and auditors).

It can be established that Organisation A should be practising this approach to successfully implement a risk compliance framework and minimise risks related to the BYOD phenomenon.

4.9 BYOD and security policies in Organisation A

Amongst the interviewees, there were different perspectives on the existence of a BYOD and security policy within Organisation A. Five out of fifteen interviewees stated that Organisation A *has* both BYOD and security policy:

"Yes, we have both". (Interviewee 1)

"Yes, you cannot access the network unless you are plugged in and via you know internet cable or if you are or you have specific security thing on your laptop". (Interviewee 7)

"Yes… We have both". (Interviewee 8)

Similarly, two interviewees assumed that Organisation A *has* both policies but were not entirely confident:

"I assume we have". (Interviewee 5)

"I think we do". (Interviewee 15)

Another two interviewees stated that Organisation A is *still busy* developing BYOD and security policy:

"Once again it is not something that is enforced but there are guidelines…I think there are guidelines around that…". (Interviewee 9)

"That's currently in development". (Interviewee 11)

On the contrary, six interviewees confirmed that Organisation A *does not* have any BYOD or security policy:

"I might be wrong, but I don't think we do have one". (Interviewee 2)

"No". (Interviewee 3)

"I don't know". (Interviewee 10)

"Not that I know of". (Interviewee 12)

This confusion and lack of confidence amongst interviewees regarding the existence of a BYOD and security policy in Organisation A suggests that Organisation A needs to verify with certainty that these policies (if they indeed exist) are appropriately distributed throughout the organisation so that employees can familiarise themselves with the context in order to elevate general awareness and improve an overall security culture. Furthermore, according to the information presented in Chapter 2, lack of organisational policies can often expose organisations to various BYOD risks, so it is necessary for Organisation A to establish some effective policies to avoid potential security breaches (Calder, 2013).

Additionally, Culnan and Williams (2009) and Heimerl (2012) establish that in an organisation, information security and privacy should be a multifaceted system that includes all procedures and policies as well as any additional aspects besides technology (e.g. MDM). A dedicated and well-written BYOD policy is necessary to control the security of BYOD environments; clearly, then, this should be taken into consideration for Organisation A.

4.10 Security awareness and security culture

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 Organisation A does not appear to have a BYOD or security policy or risk compliance frameworks. For instance:

"*Yes we do it quite well. It is mandatory for any new employee and course is also mandatory*". (Interviewee 6)

"*It is something we are always aware of. We always try to be redundant so that the mitigation can happen, some form or another...We do have a risk mitigation that needs to be enforced for those users that are making use of additional services*". (Interviewee 9)

"*Yes, there is definitely a culture and awareness; the people don't open randomly attachments for example*". (Interviewee 10)

Interviewees 12 and 14 stated that there is no organisational security awareness and security culture, while interviewees 5 and 13 were not sure about it.

As can be seen from the literature review, organisational security culture plays an important role in keeping organisational and employee devices secure (Cisco, 2013). Furthermore, Whitman and Mattord (2012) have explicitly stated that an organisational security culture can have an immense impact on the entire security perspective of the organisation. Trim and Upton (2016) supported 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).

Taking culture as a "granted assumption" (Schein, 2010, p. 36) and failing to develop appropriate security culture in an organisation can, therefore, result in significant organisational risk when introducing and practising the BYOD in the organisation. Interviewee responses reveal that Organisation A appears to succeed at keeping its

employees informed in this field, successfully maintaining organisation security culture.

4.11 BYOD education and training

When questioned if Organisation A provides employees with education and training on BYOD, the overwhelming majority of interviewees said “No”, while only Interviewee 4 expressed uncertainty:

“I am not sure if there is anything yet”. (Interviewee 4)

On the other hand, just three interviewees assumed or somewhat confirmed that there was an organised BYOD related training:

“Yes, we do”. (Interviewee 1)

“Yes, but specifically it’s more broad then organisational security awareness training”. (Interviewee 4)

“Yeah, I believe we did get the training”. (Interviewee 8)

Considering that the majority of interviewees feel confident that there is no BYOD related education or training, it needs to be pointed out that this can lead to many BYOD risks in Organisation A, as the literature reviewed in this research stresses that employees play a significant role in the general preservation of organisational security.

Furthermore, Whitman and Mattord (2012) claim that 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. Likewise, Mansfield-Devine (2012) claim that organisations must integrate their staff into security design. Lastly, it can be established that employees’ actions are strongly influenced by the education and training on BYOD; therefore, these same preparations can be recommended for the employees of Organisation A.

4.12 Proposing the final BYOD risk management model

According to the analysis of the interviews, participants have agreed that the model proposed by this researcher and its corresponding elements can effectively address the BYOD-related risks. Hence, it is concluded that the model described in Chapter 2 can be proposed as a final BYOD risk management model (Figure 11). Additionally, this provided an answer to the sub-question number five of this research.

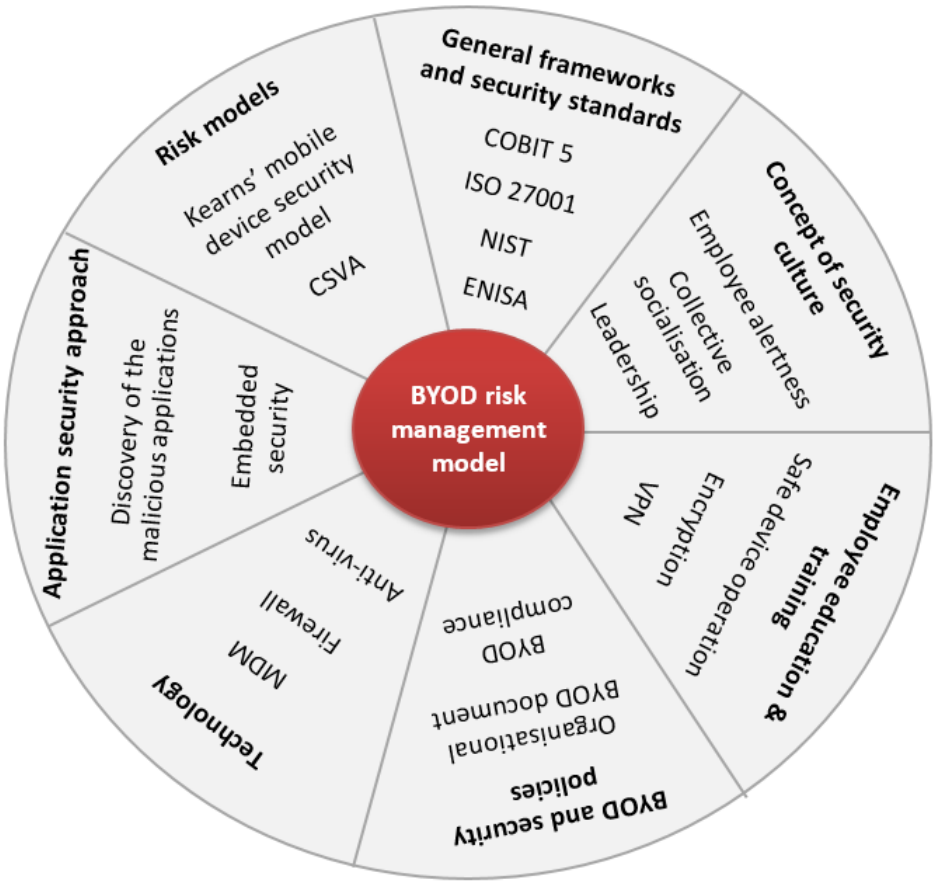


Figure 11. BYOD risk management model. Copyright 2017 by Author.

It has been confirmed empirically 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. 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 should be addressed by combining certain features from previously mentioned MDM technology (e.g. GPS tracking, remote wipe, for example) with the further development of organisational security culture.

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.

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.

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

All these practices and activities are aimed at preventing losses possibly caused by BYOD-related risks, shown in Table 5 under combined risk categories. Furthermore, the empirical testing has confirmed that the phased approach, shown in Figure 12, is also appropriate for addressing BYOD-related risks.

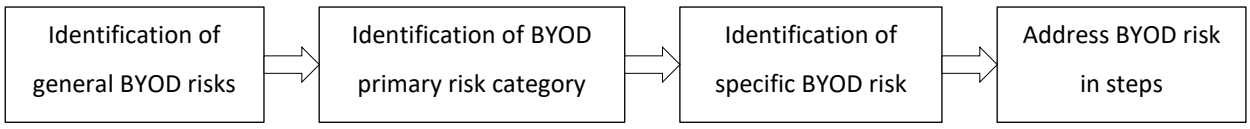


*Figure 12***.** The phased approach to BYOD risk management. Copyright 2017 by Author.

Empirically confirming the validity of the identified BYOD risks and the BYOD risk management model, this chapter also answered the main research question in this research: "*What are the risks of introducing the BYOD in the South African organisation and what is an effective approach to address identified risks?".*

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 methods for managing risks related to BYOD – such as apposite policies, risk and compliance frameworks, education/training on BYOD – they remained confident that Organisation A is doing enough to protect them as employees and the 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 (e.g. Interviewee 10) expressed open concerns and thanked this researcher for helping them be more aware of possible risks related to the introduction of BYOD in their organisation. This confirmed that these types of studies have more than mere academic value, but practical value as well, as achieved during the course of this research.

4.13 Chapter summary

In this chapter, the results of extensive interviews with participants from Organisation A were presented and analysed. In that regard, the interviewee responses have been compared with academic material presented in the literature review.

From information gathered during interviews with participants from Organisation A, it was uncovered that the majority agree that embracing the BYOD phenomenon is important, not only for employees, but for entire organisations as well. On the other hand, other interviewees, while not opposed to this conclusion, were not able to comment. To sum up, many interviewees share the opinion that BYOD is the way forward into the future of the work-place, concurring with the plethora of benefits and risks as portrayed by the literature review.

It can be concluded that interviewee responses are aligned with the findings from the literature review as nearly all identified risks (except two previously mentioned) were confirmed, including the practicality of the BYOD risk management model proposed by this researcher. Therefore, this model is suggested as a plausible solution for addressing the BYOD-related risks in the researched South African organisation, and possibly in other similar organisations as well.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

This chapter closes by reflecting on the objectives and suggesting optimal methods for mitigating BYOD risks. To conclude, this researcher briefly reviews the limitations of the research, suggests future studies and establishes future risk trends as far as the BYOD phenomenon is concerned.

5.1 Meeting objectives

This research set out to investigate the research objectives underlined in Chapter 1:

1. To explore the nature of BYOD phenomenon;
2. To identify why organisations consider BYOD;
3. To recognise risks associated with the introduction of BYOD;
4. To explore nature of these risks; and
5. To suggest an optimal approach for managing these risks.

In general, this researcher accomplished the above-mentioned research objectives by analysing available literature on BYOD (objectives 1. to 5.) and testing these findings by comparing them with responses of interviewees from Organisation A (objectives 2. to 5.).

The first objective, achieved by analysing the available literature on BYOD (Chapter 2), found that the nature of BYOD phenomenon can be traced back to the early 80s when multiple organisations recognised that the ultimate employee not only needs to possess initiative, creativeness and determination but is also able to accomplish tasks across geographical boundaries. The propensity toward the utilisation of privately owned devices was introduced globally in January 2007, when Apple co-founder Steve Jobs revealed the iPhone to the world. Following Apple's footsteps, other mobile manufacturers pushed forward the global mobile computing phenomenon. Over time, the smartphone, including other mobile computing devices such as tablet computers and phablets, gradually found their way into global organisations. The first case of

BYOD in a business environment was officially reported in 2009 by Cisco when they recognised the benefits of the BYOD and permitted employees to access business resources via their personal devices (Harkins, 2013). However, it was not until 2011 that other IT service providers realised the advantages of this phenomenon and set in motion a series of events which brought BYOD to the forefront of the IT industry.

The second objective was met by identifying the considerations of organisations before introducing the BYOD approach, as reported in the relevant literature (Chapter 2) and expressed by the interviewees in this research (Chapter 4). The main considerations revolved around the various benefits of BYOD, such as employee satisfaction, collaboration, productivity and potential financial savings. Besides, another reason why organisations consider the BYOD approach is that it appears to be the norm of the interconnected and technological world in which we live.

The third objective (i.e. the identifying risks associated with the introduction of BYOD in an organisation) was accomplished by analysing both the reviewed literature (Chapter 2) and the empirical data (Chapter 4). The findings confirmed that main risks can be grouped into five categories: i) implementational risks; ii) technological risks; iii) legislation, regulation and privacy risks; iv) human aspect risks; and v) organisational risks.

The fourth objective (i.e. exploring the nature of these risks) was completed by comparing the theoretical data grouped into the five previously mentioned categories as reported in Chapter 2 with the practical data collected during the interviews with participants from Organisation A (Chapter 4). In view of the findings presented above, it can be established that most BYOD risks are technological in nature as these threats appear to represent the largest area of concern, a fact confirmed by the literature review and research participants. This is followed by human aspect risks and legislation, regulation and privacy risks.

The last objective of identifying and suggesting the solution for minimising BYOD-related risks was achieved by, firstly, reviewing the literature on the topic as presented in Chapter 2, followed by testing the literature findings in the empirical setting of this

research as reported in the Chapter 4. The participants' responses were recorded and further compared with findings on the various BYOD risk issues as revealed from the extensive literature review. This comparison of the literature findings and the empirical results showed that besides two technological risks – "jailbreaking" and "contamination of data in cloud storage" identified in the literature review but not definitely confirmed during the interviews – there were no other discrepancies found. In other words, all interviewees have confirmed the validity of the benefits and risks related to BYOD as presented by this researcher.

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 then 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 by this researcher) to help organisations mitigate potential risks related to BYOD in an organisation.

5.2 Contribution of this research

The contribution of this research is twofold:

- Academic, by adding to the body of knowledge on the BYOD phenomenon in general and filling the existing gap on the available BYOD literature in South Africa, more particularly in understanding potential risks when introducing the BYOD initiative into an organisation; and
- Practical, as the research has provided detailed risk considerations, mitigation guidelines and a risk management model for organisations that are currently deciding on the introduction of BYOD or considering improving their current BYOD risk strategy.

Taking into consideration the current evolving BYOD trend in South Africa, this researcher believes that academics, individuals and organisations with an interest in the BYOD phenomenon, more particularly in the area of understanding potential risks when introducing the BYOD in the organisation, will benefit from the findings of this research.

5.3 Limitations of this research

This research focused on discovering which risks related to BYOD the South African organisation faces and how those risks can be mitigated or eliminated. The research was limited to an IT security consulting and service management organisation (labelled as Organisation A), in South Africa. One of the key limitations was the small sample selection of fifteen interviewees, restricting the generalization of this research. However, these limitations did not impact the relevance and validity of the findings and recommendations of this research.

5.4 Recommendations

Next, the researcher provides suggestions for Organisation A and other similar organisations pertaining to risk considerations related to the BYOD phenomenon.

5.5 To the Organisation A and practitioners in other similar organisations

The findings suggest that BYOD brings the promise to enhance employee satisfaction, productivity and work-place flexibility while simultaneously enabling the organisation to become more customer-focused and agile. Moreover, the organisation that embraces our contemporary 'changing times' and introduces the BYOD can gain a strategic advantage by harvesting the benefits that come with having an optimistic and more productive staff. Additionally, these organisations, as 'early adopters' of the BYOD trend, will attract and preserve the best talent, remaining competitive in the South African job market that is known to experience a shortage of skilled workers. Furthermore, it can be established that a properly implemented BYOD strategy can reduce organisational expenses as the direct result of the exclusion of software and hardware purchases if BYOD-related risks are mitigated appropriately. Hence, the introduction of the BYOD can be a worthwhile endeavour for South African organisations, also taking into consideration that BYOD appears to be the future of the work-place as demonstrated by reviewed literature and statements of interviewees from Organisation A.

Moreover, as a word of warning, it was established that allowing employees to use their device of preference in the organisation without proper risk prevention mechanisms can create a plethora of potential risks: data leaks, compromised network, privacy and legal issues, malware and the like. Thus, it is recommended that, in this regard, organisational BYOD strategy is implemented with a right combination of technological (e.g. MDM and additional components) and non-technological solutions (e.g. BYOD policies, risk framework and models) as revealed in this thesis.

In addition, employees should undergo appropriate training, education and attitude (e.g. interviewees 6 and 7) towards the use of BYOD to produce higher levels of knowledge and stronger general awareness in the creation of a security culture. Likewise, the participation of employees in the development of BYOD policies is essential to secure employee buy-in and agreement. Moreover, it is important to mention that local and any organisations doing business in South Africa need to

ensure that their BYOD policies and security are sound, meeting the deadline and avoiding the last-minute panic before the POPI Act is legislated.

Although these recommendations are pertinent to the organisation under research, it is likely that other companies similar in size operating in the same industry will benefit from these recommendations as well.

5.6 For further research

As BYOD is a relatively new phenomenon in South Africa, it was no surprise that this research established that not much work has been done locally in regard to risks related to the BYOD phenomenon. Moreover, taking into consideration limited South African literature on the subject of BYOD risks, further research is highly recommended. Having in mind the limited sample size in this research, this author suggests that further studies are performed using a larger sample from different organisations to increase the generalisability of further studies.

Furthermore, it is recommended that technological risks “jailbreaking” and “contamination of data in cloud storage” that were identified in the literature review, but not definitely confirmed during the interviews with employees from Organisation A, are explored in greater detail to confirm their validity and applicability in a South African context. Moreover, this author also recommends that the subject of non-technological risks (e.g. legislation, regulation and privacy risks) is explored in greater detail as it appears to be an important element for the success of BYOD strategy and in fact, the entire security of an organisation.

REFERENCES

- Abowd, G., Atkeson, C.G., Hong, J., Long, S., Kooper, R., & Pinkerton M. (1997). Cyberguide: A mobile context-aware tour guide, Wireless Networks, 3(5), 421-433.
- Absalom, R. (2012). International Data Privacy Legislation Review: A guide for BYOD policies. Ovum, 1, 1-23.
- Abulad, R. E. (2007). What is Hermeneutics?, Kritike: An Online Journal of Philosophy, 1. Retrieved from http://www.kritike.org/journal/issue_2/abulad_december2007.pdf
- Acronis. (2013). Acronis Survey Shows Nearly 60 Percent of Companies are Vulnerable to BYOD Risks. Retrieved from http://www.acronis.com/en-us/pr/2013/07/17-08-07.html
- 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*, 63(2), 175-202.
- Adler, P.A., & Adler, P. (1987). *Membership Roles in Field Research*. Newbury Park, CA: Sage.
- Ahmad, A. (2013). "Information Security Risk Management", Information Systems Security Consulting lecture on 6 July 2013, University of Melbourne, Parkville.
- Alcatel-Lucent. (2013). Kindsight Security Labs: Malware Report - Q4 2013. Retrieved from http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf
- Amoroso, EG. (2013). From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud. Security & Privacy, IEEE, 1, 23-31.
- Andrade, A. D. (2009). Interpretive Research Aiming at Theory Building: *Adopting and Adapting the Case Study Design. The Qualitative Report*, 14(1), 42-60. Retrieved from http://nsuworks.nova.edu/tqr/vol14/iss1/3/
- Andriessen, E., & Vartainen, M. (2006). Mobile Virtual Work: a New Paradigm?. *Springer Verlag*, Hindenberg.
- Arregui, D. A., Maynard, S. B., & Ahmad, A. (2016). Mitigating BYOD Information Security Risks.
- Ars Technica. (2016). How to block the ultrasonic signals you didn't know were tracking you. Retrieved from https://arstechnica.com/information-technology/2016/11/how-to-block-the-ultrasonic-signals-you-didnt-know-were-tracking-you/
- Astani, M., Ready, K., & Tessema, M. (2013). BYOD Issues and Strategies in Organisations. Issues in Information Systems, 14(2), 195-201.
- Babbie, E., & 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*, 32-33.
- Barker, K.J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime*, 154, 398-410.
- Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), 544-559.

- BBrief. (2017). PoPI – Impact on Risk and Compliancy. Retrieved from https://www.bbrief.co.za/2017/06/05/popi-impact-risk-compliancy/
- BCS. (2013). Bring Your Own Device - The Mobile Computing Challenge, BCS, The Chartered Institute for IT. Retrieved from http://www.bcs.org/upload/pdf/bring-you-own-device-the-mobile-computing-challenge.pdf
- Benbasat, I., Goldstein, D.K., & Mead, M. (1987). The case research strategy in studies of Information Systems. *MIS Quarterly*, (11).3, 69-386.
- Berghaus, S., & Back, A. (2014). Adoption of Mobile Business Solutions and its Impact on Organizational Stakeholders, *27th Bled eConference eEcosystems*, June 1 - 5, 2014; Bled, Slovenia.
- Bertino, E. (2016). Securing mobile applications. Computer, 49(2), 9-9
- Bless, C., & Higson-Smith, C. (1995). *Fundamentals of research methods*. An African perspective. RSA: Juta.
- Boland, R.J., Newman, M., & Pentland, B. T. (2010). Hermeneutical exegesis in information systems design and use, *Information and Organization*, 20, 1-20.
- Bradford Networks. (2012). Ten Steps to Secure BYOD. Whitepaper by Bradford Networks, MA, USA, 2012. pp. 1-4.
- Burns, P., Stanley, A. (2002). Fraud management in the credit card industry. Federal Reserve Bank of Philadelphia.Payment Cards Center Discussion Paper No. 02-05.
- Butler, T. (1998). Towards a hermeneutic method for interpretative research in information systems, *Journal of Information Technology*, 13, 285-300.
- Calder, A. (2013). Is the BYOD Movement Worth the Risks?, Credit Control, 65.
- CheckPoint Software LTD. (2014). The impact of mobile devices on information security: a survey of IT and security professionals. Retrieved from: https://www.checkpoint.com/press/2014/check-points-third-annual-mobile-security-survey-highlights-careless-employees-greatest-mobile-security-threat/
- Chen, H., Li, J., Hoang, T., & Lou, X. (2013). Security challenges of BYOD: a security education, training and awareness perspective. Melbourne, the University of Melbourne., Australia, 1-8.
- Chua, W. F. (1986). *Radical developments in accounting thought*. The Accounting Review, 61(4), 601-632.
- Cisco. (2013). Cisco BYOD Smart Solution. Retrieved from: https://www.cisco.com/c/dam/en_us/solutions/trends/mobility/assessment/pdfs/solution_overviewc22-702775.pdf
- Cisco. (2014). Cisco South African BYOD research highlights that many organisations in South Africa are still vulnerable when it comes to security [Press release]. Retrieved from http://www.cisco.com/web/ZA/press/2014/082514.html
- Citrix. (2012). Workplace of the Future : a global market research report. Retrieved from https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf

- Citrix. (2013). Best practices to make BYOD simple and secure. White Paper. Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf
- Cormack, A. (2013) ENISA Guide to Risk Mitigation for BYOD. Retrieved from https://community.jisc.ac.uk/blogs/regulatory-developments/article/enisa-guide-risk-mitigation-byod
- Creswell, J. W. (1998). *Qualitative Inquiry and research design*: Choosing among five traditions. Thousand Oaks, CA: Sage.
- Clevenger, N. (2011). *Ipad in the Enterprise*, Wiley Publishing Inc., Indianapolis.
- Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS quarterly*, 33(4), 673-687.
- Dawson, K. (2012). Origins of BYOD Suggest a Way Forward. Retrieved from www.businessagility.com/author.asp?section_id=1671&doc_id=237434
- Denzin, N.K., & Lincoln Y.S. (2000). *Handbook of Qualitative Research* (Second Edn.). Thousand Oaks, CA: Sage.
- Dimitriou, T., & Krontiris, I. (2006). Secure in-network processing in sensor networks. Security in Sensor Networks, 275-290.
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73-80.
- Downer, K., & Bhattacharya, M. (2016). BYOD Security : A New Business Challenge. Retrieved from https://www.academia.edu/20071329/BYOD_Security_A_New_Business_Challenge
- Dreyfus, H.L. (1998). Why we do not have to worry about speaking the language of the computer. *Information Technology & People*. 11 (4), 281-289, MCB University Press.
- Eisenstein, E.M. (2008) Identity theft: An exploratory study with implications for marketers. *Journal of Business Research* 61(11), 1160-1172.
- ENISA. (2012). Consumerization of IT: Top Risks and Opportunities - Responding to the Evolving Threat Environment. European Union Agency For Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/consumerization-of-it-top-risks-and-opportunities
- ENISA. (2017). ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends. European Union Agency For Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
- Etro, F. (2011). The economics of cloud computing. *IUP Journal of Managerial Economics*, 9(2), 7–22.
- EY. (2013). Bring your own device, security and risk considerations for your mobile device program. Insights on governance, risk and compliance, 1-12.
- Fade, S. (2004). Using interpretative phenomenological analysis for public health nutrition and dietetic research: a practical guide. *Proceedings of the Nutrition Society*, 63, 647-653.
- Felt, A. P., Finifter, M., Chin, E., Hanna, S., & 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.

- Fiberlink. (2012). Harris Survey Exposes Concerns About Employee Privacy for BYOD: Fiberlink-commissioned Poll Shows Nearly 80% of Business Users Alarmed about Employer Oversight into Location Tracking, Apps and More. Retrieved from http://www.prnewswire.com/news-releases/harris-survey-exposes-concerns-about-employee-privacy-for-byod-171520251.html
- Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26-44.
- Fortinet. (2012). Fortinet Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems. Retrieved from http://investor.fortinet.com/releasedetail.cfm?releaseid=684183
- French, A. M., Guo, C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). CAIS, 35, 10
- Gadamer, H. G. (1976). *The Historicity of Understanding*, in Critical Sociology, Selected Readings, P. Connerton (ed.), Penguin Books Ltd, Harmondsworth, UK, 117–133.
- Garba, A. B., Armarego, J., & Murray, D. (2015a). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences*, *10*(3), 1279–1287.
- Garba, A. B., Armarego, J., & Murray, D. (2015b). A Policy-Based Framework for Managing Information Security and Privacy Risks in BYOD Environments. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Volume 4, Issue 2, March-April 2015.
- Gatewood, B. (2012). The Nuts and Bolts of Making BYOD Work, *Information Management Journal,* 46 (6), 26-30.
- Gerring, J. (2004). What is a case study and what is it good for? *The American Political Science Review*, 98 (2): 341-354. Retrieved from https://fekmekci.files.wordpress.com/2014/11/gerring-case-study.pdf
- Gest, J. (2013). Managing BYOD, *Smart Business Houston*, 7(11), 20.
- Geven, A., Schrammel, J., & Tscheligi, M. (2006). Narrations and storytelling as methodological key elements for studying user experience. Proceedings of Workshop on "User Experience-towards a unified view" at the NordiCHI 2006, *ACM press*, New York. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.2630&rep=rep1&type=pdf
- Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62-70.
- Gizmodo. (2017). OnePlus Admits It Was Snooping on OxygenOS Users, Says It Will Tweak Data Collection Program. Retrieved from https://gizmodo.com/oneplus-admits-it-was-snooping-on-oxygenos-users-says-1819487335
- Gladyng, C. (2013). BYOD: Can it harm your business?: A mobile device based study. University of Derby, UK, 31-34.
- 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 & Control.

- Greenburg, A. (2012). Google Gets Serious About Android Security, Now Auto-Scans App Market for Malware. Forbes. Retrieved from https://www.forbes.com/sites/andygreenberg/2012/02/02/google-gets-serious-about-android-security-now-auto-scans-app-market-for-malware/#76f6fad66a4c
- Guan, L. (2012). Established BYOD management policies needed. Government News, 32(2), 9
- Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Newbury Park, CA: Sage.
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research*, 2(163-194), 105.
- Gummesson, E. (1991). *Qualitative Methods in Management* Research. Sage Publications. Newbury Park, California.
- Gustav, A., & Kabanda, S. (2016). BYOD adoption concerns in the South African financial institution sector. In CONF-IRM (p. 59)
- Hamel, J., S. Dufour, & D. Fortin. (1993). *Case study methods*. London: SAGE.
- Harkins, M. (2013). Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices. Retrieved from www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employeeowned-devices-w-264
- 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. Retrieved from http://www.securityweek.com/evolution-information-security
- Hennink, M., Hutter, I. & Bailey, A. (2011). *Qualitative research methods*, SAGE.
- Herrera, A. V., Ron, M., & Rabadão, C. (2017, June). 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
- Honderich, T. (1995). *The Oxford Companion to Philosophy*, Oxford University Press, Oxford.
- Howie, J. (2012). BYOD Security: Bring your own device – but secure it first!', Windows IT Pro, 37-45. Retrieved from http://windowsitpro.com/site-files/windowsitpro.com/files/uploads/2014/06/WindowsITPro_201207.pdf
- Huang, Y., & Garcia-Molina, H. (2004). Publish/subscribe in a mobile environment. Wireless Networks, 10(6), 643-652.
- Information Security. (2016). BYOD & Mobile Security Spotlight Report, Information Security LinkedIn Group, Retrieved from http://crowdresearchpartners.com/portfolio/byod- mobile-security-report/
- Information Systems Audit and Control Association. (2010).Securing Mobile Devices. Retrieved from http://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx
- Inglesant, P. (2007). Public policy, technology and lived experience: three case studies of technology support of urban transport policies in London. Phd thesis, University of London.

- Iovan, s., & Dinu, M. B. (2014). IMPACT OF THE LOSS AND THEFT OF ELECTRONIC DATA ON COMPANIES. Fiability & Durability/Fiabilitate si Durabilitate, (1).
- Irons, A., & Ophoff, J. (2016). Aspects of digital forensics in South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management*, 11, 273-283.
- ISO (2005). ISO 27005—Security Techniques—Information Security Risk Management. Retrieved from http://www.iso27001security.com/html/27005.html
- IT Online. (2014). Popi and BYOD. Retrieved from http://it-online.co.za/2014/12/03/popi-byod/
- Jarratt, D.J. (1996). A comparison of two alternative interviewing techniques used within an integrated research design: a case study in outshoping using semi-structured and non-directed interviewing techniques, *Marketing Intelligence & Planning*, Vol. 14 No. 6, pp. 6-15.
- Kabanda, S., & Brown, I. (2014). Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries - The Case of Tanzania.
- Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity Theft and Consumer Payment Choice: Does Security Really Matter?. *Journal of Financial Services Research*, 50(1), 121-159.
- Kaneshige, T. (2012). BYOD Stirs Up Legal Problems. Retrieved from http://www.cio.com/article/2396210/byod/byod-stirs-up-legal-problems.html
- Kearns, G.S. (2016). Countering mobile device threats: A mobile device security model. *Journal of. Forensic & Investigative Accounting,* 8(1), 36-48
- Kelliher, F. (2005). Interpretivism and the pursuit of research legitimization: an integrated approach to single case design. *The Electronic Journal of Business Research Methodology*, 3 (2), 23-132.
- Ketel, M., & Shumate, T. (2015). "Bring Your Own Device: Security Technologies," SoutheastCon 2015), pp 1-7.
- Keyes, J. (2013). *Bring your own devices (BYOD) survival guide*. CRC press.
- Khosrow-Pour, M. (Ed.). (2008). *Encyclopedia of information science and technology* (Vol. 1). IGI Global.
- Kim, R. (2011). The iPhone effect: How Apple's phone changed everything, Gigaom, Retrieved from http://gigaom.com/2011/06/29/the-iphone-effect-how-apples-phone-changed-everything
- Kim, G., Jeon, Y., & Kim, J. (2016). Secure mobile device management based on domain separation. In Information and Communication Technology Convergence (ICTC), 2016 International Conference on (pp. 918-920). IEEE
- Klie, L. (2011). SMB hosted CRM market set to triple by 2015. CRM Magazine, 15(12), 16.
- Klein, H. K., & Myers M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 23(1), 67-94.
- KSN. (2016). KSN REPORT: RANSOMWARE IN 2014-2016. Kaspersky Lab, June 2016. Retrieved from https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf
- Kosutic, D. (2015) How to write an easy-to-use BYOD policy compliant with ISO 27001. Retrieved from https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/

- Kumar, R. Siva. (2011). Paper Presentation on Mobile Computing. Retrieved from http://www.scribd.com/doc/48271633/4-mobile-computing
- Kumar, G., & Kumar, K. (2014). Network security – an updated perspective. Systems Science & Control Engineering, 2(1), 325–334. http://doi.org/10.1080/21642583.2014.895969
- Leavitt, N. (2013). Today's Mobile Security Requires a New Approach, Computer, 46, 16-19. DOI=http://dx.doi.org/10.1109/MC.2013.400
- 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*.
- Leedy, P.D. (1997). *Practical Research: Planning and Design (6th Edition)*. Upper Saddle River, New Jersey: Prentice-Hall.
- Li, Q., Wang, C., Wu, J., Li, J., & 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), 1038–1057.
- Livingston, D. (2013). "Introduction & History of Mobile Computing."Slideshare. Linkedin Corporation.
- Lubbe, S. (2003). Development of a case study methodology in the information technology (IT) field in South Africa: a step by step approach. *South African Journal of Information Management*, 5(4).
- Madzima, K., Moyo, M., & Abdullah, H. (2014). Is bring your own device an institutional information security risk for small-scale business organisations? *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. http://doi.org/10.1109/ISSA.2014.6950497
- Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network, *Computer* Fraud & Security, 14-17.
- Mahesh, S., Landry, B. J. L., Sridhar, T., & Walsh, K. R. (2011). Adecision table for the cloud computing decision in small business. *Information Resources Management Journal*, 24(3), 9–25.
- Mangan, J. (2004). 'Combining quantitative and qualitative methodologies in logistic research', *International Journal of Physical Distribution & Logistics Management*. 34(7), 565-578.
- Marais, W. J., & Kruger, C. J. (2005). Implementation of an information system within a bureaucratic environment: an understanding of the human issue. South African journal of Information Management, 7(1), Retrieved from http://www.sajim.co.za/index.php/SAJIM/article/viewFile/254/245
- Markelj, B., & Bernik, I. (2012). Mobile devices and corporate data security. *International Journal of Education and Information Technologies*, 6(1), 97-104. Retrieved from http://www.naun.org/main/NAUN/educationinformation/17-591.pdf
- Marzanah, A. J. (2009). An investigation into methods and concepts of qualitative research in information research. *Computer and information science*, 2(4). Retrieved from http://ccsenet.org/journal/index.php/cis/article/view/3200/3714
- McLarty, M. (2012). BYOD is unstoppable: Smart companies must build apps. Retrieved from

https://gigaom.com/2012/04/08/byod-is-unstoppable-smart-companies-must-build-apps/

- McAfee. (2012). Putting IT Back in Control of BYOD, Osterman Research Inc., USA. Retrieved from http://www.webtorials.com/main/resource/papers/McAfee/paper4/put-it-back-in-control-byod.pdf
- Meeker, M. (2015). Internet Trends 2015 – Code Conference. *Kleiner* Perkins Caufield & Byers (KPCB), 1–196.
- Mercer, V. N. (2001). The double-edged sword: examining perceptions of technology as a process of enablement and construct within an academic organization. Unpublished MA thesis, University of North Carolina, October 2001.
- Miller, K., Voas, J., & Hurlburt, J. (2012). BYOD: Security and Privacy Considerations, *IT Professional*,14(5), 53-55.
- Mont, J. (2012). The Risks and Benefits of Employee-Owned Devices. Compliance and Technology, 48-52.
- Mouton, J. (1996). Understanding social research. RSA: J.L van Schaik.
- Mountain, D., & MacFarlane, A. (2007). Geographic information retrieval in a mobile environment: evaluating the needs of mobile individuals. Journal of Information Science, 33(5), pp. 515-530. doi: 10.1177/0165551506075333
- Morgan, G., & Smircich, L. (1980). The case for qualitative research. The Academy of Management Review, 5(4), 491-500.
- Morse, J. M. (1994). *Designing funded qualitative research*. Sage Publications, Inc.
- Mutwiwa, P. N., Kamau, J. W., & Gikandi, J. (2017). GREEN BYOD-A GREEN COMPUTING APPROACH TO GREENING INSTITUTIONS OF HIGHER LEARNING. *International Journal of Applied Computer Science (IJACS),* 1(1), 13-23.
- My Broadband. (2016). Smartphone penetration in South Africa hits major milestone. Retrieved from https://mybroadband.co.za/news/smartphones/180894-smartphone-penetration-in-south-africa-hits-major-milestone.html
- Myers, M. D. (1994). A disaster for everyone to see: an interpretative analysis of a failed IS project. Accounting, management and information technology, *Elsevier Science*, 4(4): 185-201.
- Navarra, D. D. (2006). The governance architecture of global ICT programmes: a case study of e-government in Jordan London: London School of Economics and Political Science (LSE). Retrieved from https://research.utwente.nl/en/publications/the-governance-architecture-of-global-ict-programmes-a-case-study
- Netstandard. (2013). 13 Best Practices for Developing Your Mobile Device Policy. Retrieved from: http://www.netstandard.com/13-best-practices-for-developing-your-mobile-device-policy/
- Neuman, W. L. (1997). *Social research methods; qualitative and quantitative approaches (3rd Ed)*. USA: Allyn & Bacon.
- Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization - A Theory and Practice Review. Paper presented at the AMCIS, Paper 18. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/EndUserIS/18/

- 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
- Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 5(2) http://doi.org/10.1177/2158244015580372
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: research approaches and assumptions. *Information Systems Research*, 2(1), 1-28.
- Osterman Research. (2012). Putting IT back in control of BYOD. Retrieved from http://resources.idgenterprise.com/original/AST0066579_Accellion_Osterman_Putting_IT_Back_in_Control_of_BYOD.pdf
- Pather, S., & Remenyi, D. (2005). Some of the philosophical issues underpinning research in information systems: from positivism to critical realism. *South African Computer Journal*, 35, 76-83.
- Patton, E., & Appelbaum, S. H. (2003). The case for case studies in management research. *Management Research News*, 26(5), 60–71. http://doi.org/10.1108/01409170310783484
- Patton, M. Q. (1990). *Qualitative evaluation and research methods (2nd ed.)*. Newbury Park, CA: Sage.
- Phifer, L. (2013). Bring your own danger, *Information Security*, pp. 29-35.
- Pillay, A., Diaki, H., Nham, E., Senanayake, S., Tan, G., & Deshpande, S. (2013). Does BYOD increase risks or drive benefits? Melbourne, The University of Melbourne, 1–8.
- Portela, F., Moreira da Veiga, A., & Santos, M. F. (2018). Benefits of Bring Your Own Device in Healthcare. In J. Machado, A. Abelha, M. Santos, & F. Portela (Eds.), *Next-Generation Mobile and Pervasive Healthcare Solutions* (pp. 32-45). Hershey, PA: IGI Global. doi:10.4018/978-1-5225- 2851-7.ch003
- Potts, M. (2012). *The state of Information Security*, 9–11.
- Priest, H., & Roberts, P. (2010). Gathering and making sense of words. In Roberts, P. and Priest, H. (2010) Healthcare research A handbook for students and practitioners, Wiley-Blackwell, UK.
- Prince Samar and Stephen B. Wicker. 2004. On the behavior of communication links of a node in a multi-hop mobile environment. In Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '04). ACM, New York, NY, USA, 145-156. http://dx.doi.org/10.1145/989459.989478
- 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.
- Punch, K. (1998): Introduction to Social Research. Quantitative & qualitative approaches. *Sage publications*, London.
- Ratchford, M. M. (2017). BYOD: A Security Policy Evaluation Model. In Information Technology-New Generations (pp. 215-220). Springer, Cham.
- Reddy, A. S. (2012). Making BYOD Work for Your Organization. Future of Work, 1–16. Retrieved from https://www.slideshare.net/cognizant/making-byod-work-for-your-organization-13450463

- Riege, A. M. (2003). Validity and reliability test in case study research: a literature review with "hands-on" applications for each research phase. *Qualitative Market Review: an International Journal*. 6(2), 75-86. Retrieved from https://www.scribd.com/document/2168226/Validity-and-reliability-tests-in-case-study-research
- Roode, D. (2003). Information Systems Research: A Matter of Choice? *South African Computing Journal* 30, 1-2.
- Rouse, M. (2007). Nomadic computing (Mobile computing).
- Ruighaver A.B., Maynard, S.B., & Chang. (2007). Organisational security culture: Extending the end-user perspective, *Computers and Security*, 26, 56-62.
- Ruighaver, A.B., Maynard, S.B., & Warren, M. (2010). Ethical Decision Making: Improving the Quality of Acceptable Use Policies, *Computers and Security* (29:7), 731-736.
- Sahu, D., Sharma, S., Dubey, V., & Tripathi, A. (2012). Cloud Computing in Mobile Applications. International Journal of Scientific and Research Publications, 2(8), 1-9.
- Santos-Olmo, A., Sánchez, L. E., Caballero, I., Camacho, S., & 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), 30.
- Sasse, M. A., Brostoff, SB., & Weirich D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security, BT Technology Journal, 19(3),122-131.
- Saunders, M., Lewis, P., & Thornhill, A. (2007). Research methods for business students. Essex: Pearson Education Limited.
- Schein, E. H. (2010). Organizational culture and leadership (Vol. 2). John Wiley & Sons.
- 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. Retrieved from http://icsa.cs.up.ac.za/issa/2003/Publications/INFORMATION%20SECURITY%20CULTURE.pdf
- Schneider, D. (2012). The state of network security. *Network Security*, 2012(2), 14–20.
- Schneiders, S.M. (1999). *The Revelatory Text: Interpreting the New Testament as Sacred Scripture*, Liturgical Press, 2.
- Schwandt, T. A. (2000). Three epistemological stances for qualitative inquiry: Interpretivism, hermeneutics, and social constructionism. *Handbook of qualitative research*, 2, 189-213
- Semer L. (2013). Auditing the BYOD Program, Internal Audit, February, 70(1), 23-27.
- Sen, P. K. (2012). Consumerization of Information Technology Drivers , Benefits and Challenges for New Zealand Corporates. School of Information Management, Victoria University of Wellington, 1–57.
- Silvergate S., & Salner, C. (2011). *Smartphones and the Fair Labor Standards Act,* For the Defense
- Singleton Jr, R. A., Straits, B. C., & Straits, M. M. (1993). Approaches to social research. Oxford University Press.
- Singh, S., & Bartolo, K. (2005). Grounded theory and user requirements: A challenge for qualitative research. Australasian Journal of Information Systems, 12(2).

- Smith, J. A., Flowers, P., & Larkin, M. (2009). Interpretative Phenomenological Analysis: theory, method and research. UK: Sage Publishers.
- Smith, J.A., Jarman M., and Osborn, M. (1999) Doing Interpretative phenomenological analysis. In: M. Murray and K. Chamberlain (eds), Qualitative Health Psychology: Theories and Methods. London: Sage, 218-240.
- Sofaer, S. (1999). Qualitative methods: what are they and why use them? *Health services research*, 34, 1101.
- Somers, M. R., & Gibson, G. D. (1994). Reclaiming the Epistemological "Other": Narrative and the Social Constitution of Identity. *Social Theory and the Politics of Identity*, 37–99.
- Song, I. (2013). Driving Business Value with BYOD and Research Contents Developing an Enterprise Mobility Framework, (June). Retrieved from http://enterprise.huawei.com/ilink/cnenterprise/download/HW_280603
- Sørnes, J. O. (2004). Information and Communication Technologies in practice. A study of advanced users in the workplace in Norway and the United States; Unpublished Doctoral thesis, Trondheim.
- Srinivasan, S. (2014). Cloud computing basics. Retrieved from https://play.google.com/store/books/details?id=S2EgBAAAQBAJ&source=ge-web-app
- Stake, R. E. (1995). *The art of case study research*. Sage
- Steven, F. (2013). *Mobile Devices: Securing mobile devices: technology and attitude*, Network Publishing.
- Subramanian, L., Maguire Jr, G. Q., & Stephanow, P. (2011). An architecture to provide cloud based security services for smartphones. In *27th Meeting of the Wireless World Research Forum (WWRF), Düsseldorf, Germany, 18-20 October 2011*. Wireless World Research Forum.
- Symantec. (2016). Internet Security Threat Report, Symantec. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
- Rodríguez, NR., Murazzo, MA., Chavez, S. (2012). Key aspects for the development of applications for Mobile Cloud Computing. *Journal of Computer Science & Technology*, 13(3), 143-148.
- Taniar, D. (Ed.). (2008). *Mobile Computing: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications* (Vol. 1). IGI Global.
- Thacher, D. (2006). The normative case study. AJS 111(6):1631-76. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.533.4413&rep=rep1&type=pdf
- Tech Target. (n.d.). What is cloud sprawl? - Definition from WhatIs.com. Retrieved from http://searchcloudcomputing.techtarget.com/definition/cloud-sprawl
- Tellis, W. (1997). Introduction to case study, The Qualitative Report, 3(2). Retrieved from: http://www.nova.edu/ssss/QR/QR3-2/tellis1.html
- Thomson, G. (2012). Feature: BYOD: enabling the chaos, *Network Security*, 2012(2), 5-8.
- Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7-11.
- Trim, P., & Upton, D. (2016). *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Routledge.

- Trend Micro. (n.d.). Ransomware definition. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/ransomware
- Trochim, W. M., & Donnelly, J. P. (2001). Research methods knowledge base.
- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to Cope with Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination, Information & Management (52:4), pp 506-517.
- Twinomurinzi, H., & Mawela, T. (2014). Employee perceptions of BYOD in South Africa: Employers are turning a blind eye? *Saicsit 2014*, 1–6.
- Tzoumas, C. (2013). The BYOD World. *BusinessWest*, 30, 45.
- Veiga A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture, *Computers & Security*, 29,196-207.
- Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.
- Walsham, G. (1993). *Interpreting information systems in organizations*. John Wiley & Sons, Inc.
- Webopedia.com. (2017). *What is BYOD Bring Your Own Device? Webopedia Definition*. Available at: https://www.webopedia.com/TERM/B/BYOD.html
- Weilenmann, A. (2003). Doing Mobility, Gothenburg studies in Informatics, nr 28, School of Business, Economics and Law, Göteborg University.
- Welman, J.C., & Kruger, S.J. (1999). Research methodology for the business and administrative sciences. South Africa: Thomson.
- Whitman M.E., & Mattord H.J. (2012). *Principles of Information Security, Course Technology*, Boston.
- Willig, C. (2001). Introducing qualitative research in psychology: adventures in theory and method, Buckingham: Open University Press.
- Wood, A. (2012). BYOD: The Pros and Cons for End Users and the Business, *Credit Control*, 33(7/8), 68.
- World Wide Worx (2012). Internet Matters. Retrieved from http://led.co.za/sites/default/files/cabinet/orgnameraw/document/2012/za_internet_matters_final.pdf
- Yeboah-Boateng, E. O. (2013). Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & 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., & Ni, L. (2006). *Smart phone and next generation mobile computing*, Morgan Kaufmann, San Francisco.
- Zhou, H., Wu, C., Jiang, M., Zhou, B., Gao, W., Pan, T., & Huang, M. (2015). Evolving defense mechanism for future network security. *IEEE Communications Magazine*, *53*(4), 45-51.

APPENDIX A: ETHICS APPROVAL

UNIVERSITY OF CAPE TOWN

FACULTY OF COMMERCE

Igniting Knowledge and Opportunity

Ethics Approval Request for the Study entitled:

Signed by:

	Full name and signature	Date
Principal Researcher/Student: IVAN VELJKOVIC	IVAN VELJKOVIC	12.12.2016

This application is approved by:

Supervisor	Adheesh Budree	12/12/2016
Co- Supervisor		

This application has been approved
25 February 2017

Com Ethics_V4

APPENDIX B: CONSENT FORMS

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

13 December 2016

Request to conduct research and interview participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Master's Degree in Information Systems at the University of Cape Town a research study is required.

The researcher, in this case Ivan Veljkovic, has chosen to conduct a case study entitled BYOD - Risk considerations in South African organisation. The objective of the research is to investigate, determine and assess the possible risks introduced by BYOD in a South African organisation. This research has been approved by the Commerce Faculty Ethics in Research Committee.

Your participation in this research is voluntary. All information will be treated in a confidential manner and used exclusively for the purpose of this study. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data collection method will be one-on-one semi-structured interviews with a small group of the staff responsible for various factors related to BYOD, such as implementation, risks and alike. The interviews will be conducted at your company premises and will last between 30-60 minutes. If you are willing to participate in this study, kindly sign the attached form and return to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on 071 603 4396 or email: vljiva001@myuct.ac.za.

Your participation in this study would be greatly appreciated, but is entirely voluntary.

Sincerely,

Name and surname [signature]

Researcher \ M.Com Student, (UCT) - Ivan Veljkovic
Department of Information Systems
University of Cape Town
Email: vljiva001@myuct.ac.za

Supervisor Name and surname [signature]

Research Supervisor - Dr. Adheesh Budree
Department of Information Systems
University of Cape Town
Email: adheesh.budree@uct.ac.za

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

Research Participant Consent Form

I, _____, consent to participate in the research on BYOD - Risk considerations in South African organisation.

I am aware that participation is voluntary and that I may choose to withdraw from this study at any time, should I choose to do so.

_____ _____

Signature Date

APPENDIX C: INTERVIEW QUESTIONS

INTERVIEW QUESTIONS:

BYOD - RISK CONSIDERATIONS IN SOUTH AFRICAN ORGANISATION

Researcher: Ivan Veljkovic, UCT

These interview questions were accompanied by the consent form signed by the participant and researcher.

INTRODUCTORY PART:

1. What is your current title / role in your organisation and how long have you had that role?
2. Please provide a short description of your daily tasks in work-place.

BYOD AWARENESS:

3. Have you ever heard about BYOD (Bring-Your-Own-Device)?
4. Do you use a personal mobile device such as smartphone, tablet computer or laptop in a work-place? If yes, please describe what type of device/s do you use (e.g. laptop, android phone, iPhone, etc.).
5. What do you think about the importance of allowing employees to use their personal mobile devices in the work-place?

BENEFITS OF BYOD:

6. Please provide your opinion on potential benefits of BYOD for both the employees and organisation regarding the following

- Operational benefits (e.g. more flexible working hours, increased workers satisfaction levels and motivation, increased productivity, better organisational image, etc.)
- Financial benefits (e.g. reduced costs, better adoption of cutting edge technology, etc.)
- Organisational benefits (e.g. new partnership possibilities, better efficiency of workers, improved collaboration, etc.)
- Any other potential benefits

RISKS OF BYOD:

7. What are your top BYOD related security concerns?
8. Have you or your organisation ever been exposed to any BYOD or similar security concerns? If yes, please provide more details (e.g. how did it happen, which systems were affected, etc.)
9. Please provide your detailed opinion on potential risks of BYOD for both the employees and organisation, regarding:

- Implementation risks (e.g. protecting data, ensuring security, providing support, etc.);
- Technological risks (e.g. malware, various vulnerabilities, jailbreaking, phishing and social engineering, compromised user account, etc.);
- Legislation, regulation and privacy risks (e.g. ethical and privacy issues, tracking of data, breach of normal working hours, liability due to loss of company data, etc.);
- Human aspects risks (e.g. lack of control over data, stolen or lost device, identity theft, etc.);

- Organisational risks (e.g. inadequate user education, lack of organisational policies, etc.);
- Any other relevant risks.

ADRESSING BYOD RISKS:

10. Is your organisation utilising any methods to prevent risk? If yes, please state solution(s) used to secure, for example, the device, data residing on mobile devices, data in transit, the separation of corporate data from personal data and/or alike.
11. What is your view regarding the appropriateness of the steps that your organisation takes to secure mobile apps within the BYOD initiative?
12. How often are internally developed, outsourced or purchased BYOD apps tested and with what effect?
13. Does your organisation have BYOD or IT security policy? If yes, how effective is that policy?
14. Which are the primary reasons for implementing a BYOD security policy? (e.g. to secure data, regulatory and legal compliance, response to popularity of BYOD in South Africa, etc.)
15. Does your organisation utilise any risk compliance framework (e.g. ISO27005, COBIT 5, etc.) in order to better manage risks related to BYOD?
16. Is there any organisational security-awareness (culture) training that includes information on safe and secure uses of sensitive data on mobile devices? If yes, please describe.
17. Does your organisation provide employees with education and training on BYOD? If yes, please provide more details.
18. Please describe your confidence in your organisation's mobile security controls and their effectiveness in protecting organisational data.
19. What authentication mechanisms your organisation requires for mobile devices that access enterprise data or networks? (e.g. user name and password, on device certificate, pattern, biometrics, etc.)
20. Are organisation-managed mobile devices allowed access to public wireless networks? If yes, under what conditions?

21. Are organisation-managed mobile devices allowed to access social media and social networking sites or use related applications? If yes, under what conditions?
22. Does your organisation use any method of encryption? If yes, how effective it is?
23. What are other steps taken by your organisation to minimise risk other than BYOD related risk?
24. How the implemented risk prevention/mitigation practices influence security culture in your organisation?
25. How the implemented risk prevention/mitigation practices influence your personal productivity?

CONCLUDING QUESTIONS:

26. Do you see more risks related to BYOD than those mentioned in this interview? If yes, please provide more details.
27. Do you see more benefits and opportunities with BYOD than those who have been mentioned in this interview? If yes, please provide more details.
28. Please provide any additional remarks regarding the BYOD risks and their prevention or mitigation?
29. Please feel free to provide any other relevant information or suggestion.