An implementation framework for BYOD in a selected state-owned enterprise

Elliot Mokoena

Student number 890874

emokoena@gmail.com

0769183898

Supervisor: Prof René Pellissier

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2020

(Version 2019-2020)

ABSTRACT

This study will explore the Bring Your Own Device (BYOD) phenomenon in South African State-Owned Enterprise, Transnet. The concept has become significant during the global pandemic lockdown and the resultant slowing of the economy forcing state-owned enterprises to review their cost saving measures. The objective is to identify critical factors influencing BYOD implementation with the purpose of understanding how these factors shape the actions of the information technology portfolio at Transnet. The Perceived e-Readiness Model (PERM) is adopted to identify contextual BYOD adoption factors. There are several studies conducted on the corporate adoption of BYOD, but few have investigated the phenomenon from state-owned enterprise (SOE) perspective in South Africa specifically. The study highlights the importance of technological and organisational readiness in the adoption of BYOD. Due to the complexities in cyber security, the study further highlights the importance of IT security to ensure correct adoption of BYOD as a response to continued work from home response during the Covid-19 pandemic, securing both the user's privacy and confidentiality as well as the organisational goals of productivity.

KEY WORDS

BYOD, mobility, work from home

DECLARATION

I, Elliot Mojalefa Mokoena, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Signature:

Signed at ……

On the …….. day of …… 20…..

DEDICATION

I dedicate this research report to my life partner Ms. Wendy Madlabane who provided all the welfare care during my studies and cared for the running of our lovely home. I also am grateful for the support received in the forming stages of this report from Ms. Bonolo Mothobi, Ms. Zola Mdledle and Ms. Akhona Kotyi, I am eternally indebted to their support.

I also would like to appreciate the lease of life the almighty God gave me after contracting Covid-19 in July 2020, despite the bleak and life threatening period the Lord me spared to continue with my course work and eventually this research report.

ACKNOWLEDGEMENTS

Firstly, I would like to acknowledge the favour and mercy bestowed upon my life to have completed my studies. Surviving Covid-19 pandemic and pressing on with studies was no easy task, none of which was possible without the support of my wife who took care of me and sacrificed a lot to take care of our household.

I also would like to acknowledge the support of my supervisor who gave a lot of advice and really taught me a lot about academic writing. When I was ready to quit, she often made a call and picked me up to press on. Thank you ever so much Professor René Pellissier, your contribution to my studies will forever be cherished.

TABLE OF CONTENTS

Table of Contents

ABSTRACT ii

DECLARATION iii

DEDICATION iv

ACKNOWLEDGEMENTS v

LIST OF TABLES ix

LIST OF FIGURES x

LIST OF ACRONYMS xi

CHAPTER 1. INTRODUCTION 12

1.1 PURPOSE OF THE STUDY 12
1.2 CONTEXT OF THE STUDY 14
1.3 RESEARCH PROBLEM 16
1.4 RESEARCH OBJECTIVES 18
1.4.1 PRIMARY OBJECTIVE 18
1.4.2 SECONDARY OBJECTIVES 18
1.5 DELIMITATIONS OF THE STUDY 18
1.6 DEFINITION OF TERMS 19
1.7 ASSUMPTIONS 19

CHAPTER 2. LITERATURE REVIEW 20

2.1 INTRODUCTION 20
2.2 DEFINITION OF TOPIC OR BACKGROUND DISCUSSION 21
2.3 DRIVERS OF BYOD 22
2.3.1 ONE USER AND MULTIPLE DEVICES 22
2.3.2 PERSONAL AND WORK LIFE OVERLAP 23
2.3.3 ANYTIME AND ANYWHERE MOBILITY 24
2.4 BENEFITS OF BYOD IMPLEMENTATION 25
2.5 BYOD AND EMPLOYEE PRODUCTIVITY 27

2.6 CHALLENGES OF AN BYOD IMPLEMENTATION 28
2.6.1 EMPLOYEE CHALLENGES 28
2.6.2 USER SEGMENTS AND NEEDS 29
2.6.3 ORGANISATIONAL CHALLENGES 30
2.6.4 THE DIGITAL WORK ERA 33
2.6.5 SECURING THE MOBILE DEVICES 34
2.6.6 ADDRESSING THE APPLICATION RISK 35
2.6.7 MANAGING THE ENVIRONMENT 36
2.6.8 A SUPPORTING FRAMEWORK 36
2.7 CONCLUSION OF LITERATURE REVIEW 43
2.7.1 PROPOSITION 1: 43
2.7.2 PROPOSITION 2: 43
2.7.3 PROPOSITION 3: 44
2.7.4 PROPOSITION 4: 44

CHAPTER 3. RESEARCH METHODOLOGY 45

3.1 RESEARCH APPROACH 45
3.2 RESEARCH DESIGN 46
3.3 DATA COLLECTION METHODS 47
3.4 POPULATION AND SAMPLE 47
3.4.1 CASE SITE 47
3.4.2 SAMPLE AND SAMPLING METHOD 48
3.5 THE RESEARCH INSTRUMENT 49
3.6 PROCEDURE FOR DATA COLLECTION 50
3.7 DATA ANALYSIS AND INTERPRETATION 50
3.8 LIMITATIONS OF THE STUDY 51
3.9 VALIDITY AND RELIABILITY 52
3.10 ETHICAL CONSIDERATIONS 52

CHAPTER 4. DISCUSSION OF THE FINDINGS 55

4.1 INTRODUCTION 55
4.2 DISCUSSION PERTAINING TRANSNET DOCUMENTATION 55
4.3 DISCUSSION PERTAINING TO PROPOSITION 1 57
4.4 DISCUSSION PERTAINING TO PROPOSITION 2 59
4.5 DISCUSSION PERTAINING TO PROPOSITION 3 61
4.6 DISCUSSION PERTAINING TO PROPOSITION 4 63

CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS 65

5.1 INTRODUCTION 65
5.2 CONCLUSIONS REGARDING RESEARCH OBJECTIVES 65
5.3 RECOMMENDATION AND CONTRIBUTION 67

REFERENCES **69**

APPENDIX A - Instrument **85**

ORGANISATIONAL 85
MANAGEMENT SUPPORT 86
HUMAN RESOURCES 87
BUSINESS RESOURCES 87
TECHNOLOGICAL READINESS 87
POLICY /GOVERNANCE 88

Appendix B – WITS Ethics Clearance **90**

Appendix C – Transnet Clearance **91**

Appendix D – Participant Form **92**

LIST OF TABLES

Table 1: Comparisons of types of mobility 26

Table 2: Security characteristics of BYOD 31

Table 3: Design levers 34

Table 4: PERM Factors 38

Table 5: Profile of respondents 49

Table 6: Reviewed IT Policies 55

LIST OF FIGURES

Figure 1: Device varieties 23

Figure 2: User segmentation 30

Figure 3: PERM Model 38

Figure 4: Technology Acceptance Model 43

Figure 5: Thematic Analysis phases 51

Figure 6: Proposed Mobility Approaches 57

Figure 7: BYOD Program Awareness 58

Figure 8: Policy provisions for BYOD 58

Figure 9: IT Management support for BYOD 59

Figure 10: Management's commitment rating 60

Figure 11: Training offered or Attended 60

Figure 12: Respondents with MDM configured 62

Figure 13: IT Readiness to support BYOD 62

Figure 14: Users with MDM Configured 63

Figure 15: Availability of mobile device policy 64

Figure 16: Policy support for BYOD 64

LIST OF ACRONYMS

Acronym	Meaning
AI	Artificial Intelligence
BRS	Business Requirements Specification
BYOD	Bring Your Own Device
DoS	Denial of Service
EUCD	End-user Computing Device
ICT	Information, Communications Technology
IP	Internet Protocol
IoT	Internet of Things
IT	Information Technology
ML	Machine Learning
OD	Operating Division
PEER	Perceived External e-Readiness
PERM	Perceived e-Readiness Model
POER	Perceived Organisational e-Readiness
4IR	Fourth Industrial Revolution

CHAPTER 1. INTRODUCTION

1.1 Purpose of the study

The organisation's success in the information age, brought about by the components of 4IR, largely depends on the organisation's ability to empower a mobile workforce (Ophoff & Miller, 2019). Securing access to business applications, data and services remain important regardless of who owns the end-user device. The situation is further aggravated by the entrance of IoT and the cyber-physical systems that provide communication, efficiencies and effectiveness (Klötzer et al., 2017), furthermore with the explosion of connected devices and IoT, the risks associated with BYOD have worsened (Barlette et al., 2020). On top of that, global pandemic lockdown regulations forced organisations to allow a general work from home policy, the extent of which has not been previously experienced (Kramer & Kramer, 2020; Watson, 2020). One of the strategies that can be adopted to enable worker mobility is through the "Bring Your Own Device" (BYOD) concept. The implementation of BYOD should strike a balance between the security risks implications and the inherent benefits associated with BYOD in the workplace. Adopting BYOD will increase access, mobility and productivity, this however can lead to corporate data exposure and loss.

There has been a great shift regarding the use of digital devices in the workspace and beyond. This is as a result of an increase in the usage of employee-owned devices such as mobile devices and tablets (Rosnah & Anang, 2018). This is

referred to as BYOD. Furthermore, the shift into a more digital era, heralded an effective and efficient way of utilising these mobile devices connecting them more for work purposes onto corporate networks. Additionally, employees started using their personal devices for both work and personal purposes (Mitrovic et al., 2014; Rosnah & Anang, 2018). There are various ways that employees do this. For instance, communication through applications such as web browsing, accessing peer-to-peer communications applications, accessing emails, etc. Therefore, this makes work to be easily accessible and viable both from home and at the workstation using the same devices and systems (Rosnah & Anang, 2018).

Employees have indicated they are more efficient if they select a device of their own preference (Ophoff & Miller, 2019). The resultant efficiency has a direct bearing upon productivity due to the choice of device. Due to increasing operational expenses, organisations have also indicated that, to compete in the global economy, they leverage the BYOD phenomenon (Ophoff & Miller, 2019), which saves on upgrade costs, purchasing of devices, device replacement costs, etc. However, by providing permission to employees to access and conduct work using employee-owned devices, intellectual property of the organisation may be exposed to external or unintended parties. These breaches may be conducted innocently and or on purpose (Beckett, 2014; Jahanbakhsh et al., 2020).

The balance can only be attained through a culture change and proper governance regime. Harris and Patten (2014) argue that, in order to integrate business mobility and leverage flexibility and productivity into the organisation strategy, new policies to address and manage people, processes and technology ought to be adopted. Without these policies organisations will only end up with a

myriad of end-user computing devices disguised as BYOD and a plethora of multi-vendor services (Barlette et al., 2020; Cho & Ip, 2018a).

Due to the fast adoption of mobile devices in South Africa (Mzekandaba, 2020; Okwonkwo, 2019; Sanou; & ITU, 2017), this study will therefore investigate what BYOD factors influence productivity and determine the associated risks in regards to the adoption of the BYOD phenomenon at Transnet.

1.2 Context of the study

BYOD is a concept allowing employees to communicate, using their own technology and end-user computing equipment to connect to the corporate IT systems and data for the purposes of conducting work, “anytime, anywhere, from any device” (Cho & Ip, 2018b; Niehaves et al., 2012; Zheng & Ni, 2005). Usage of personal devices for work, such as mobile phones, e-readers, laptops etc., extends the availability of corporate systems to the user anytime, anywhere (Absalom & Drury, 2012). With the growth and proliferation of these devices come the opportunity for organisations to exploit their uses in a corporate setting, offering flexibility, job satisfaction and mobility options otherwise not available (Mahat & Ali, 2018).

Due to the increased access and use of the internet, user intention and likelihood to adopt BYOD have been extensively researched (Lebek et al., 2013), however the factors that positively or negatively influence an organisation’s attitude to adopt, manage and deploy the BYOD as a strategy, remain largely unexplored. There is very little research focusing on BYOD implementation (Brodin et al.,

2015), with some information available on the adoption of BYOD in South African financial institutions (Ophoff & Miller, 2019).

The International Telecommunications Union (ITU) periodically releases a report presenting global trends and developments in Information Communications Technology (ICT) services and tools. The ITU uses a benchmark known as the ICT Development Index (IDI). This benchmark presents the performance of participating countries and highlights areas requiring improvement (ITU, 2021). This benchmark is comprised of quantitative indicators namely ICT Access, ICT Use and ICT Skills. According to the ITU report, South Africa ranked 3rd in Africa and 92nd globally (Mzekandaba, 2020; Sanou; & ITU, 2017), this position in the ranking may have since change due to heightened work from home requirements due to Covid-19 lockdown regulations (Kramer & Kramer, 2020). Interestingly South Africa's ICT access index was above average scoring 5.48 out of 10. The findings indicate that 52% of South African households have access to the internet, while 54% of individuals use the internet. In the main, most of the research is focused on the analysis of capabilities and expectations. Other studies focused on Small, Medium Enterprises (SME) as well as schools, and higher education institutions (Adedolapo, 2015; Sobikwa & Ditsa, 2017) .

Although more recent reports are not available, the South African situation would have changed significantly given the South African Government's hard lockdown rules to pre-empt COVID-19 transmission, forcing larger mobility of the workforce. Due to COVID-19, business and government were required to use an online or virtual platform of communication, thereby increasing the possibility of integrating private and professional environment and increasing the possibility of using

private devices for work (Jahanbakhsh et al., 2020). This situation now presents an opportunity for Government departments, already struggling with financial pressures and budgetary constraints, to continue in this way but to regulate the use of private devices in the public domain (Gov. Gaz., 2020). To better understand the challenges in the BYOD practice in public sector, one ought to appreciate the challenges and opportunities as experienced by the users in the public sector. This research aims to determine the critical factors affecting the BYOD adoption in a public sector setting in South Africa.

1.3 Research problem

The provision of access and security management of all devices on the Transnet network is governed centrally by the Cyber Security Department of the ICT function. Historically, the Group Information Communication Technology (GICT) department of Transnet has spearheaded the control of mobile devices for all of Transnet employees.

The Transnet group IT department provides a total of 25000 users with end-user computing devices (EUCD) for work purposes, this is in response to the business requirement for workforce mobility, as well as remote access to corporate systems (Scarfone et al., 2020). Of these, about 90% have devices that are older than five years. The operational cost of maintaining, supporting and the risks associated with these old devices is escalating. The devices require connectivity that is outdated exposing the information contained in them to cyber security risks.

Transnet is operated federally through seven operating divisions (OD), each OD has an IT department separately which is responsible for the daily ICT operations of the OD (Transnet, 2019). Due to several reasons, ranging from vendor management, contract disputes and lengthy procurement issues, the provision of end-user devices has largely collapsed giving rise to an increase in employee-owned devices in the workplace as existing requirements could not be met by the organisation.

Currently, users have the capability to access the Transnet Network and have access to applications such as Exchange Email and Microsoft SharePoint. Moving forward, users should have access to critical systems such as the SAP modules in the organisation, have access to Board and EXCO Portals (depending on the role that an employee occupies) and be able to exchange information with colleagues via real-time voice and video communication that cover all areas where Transnet has reach.

The research problem that informs this research study is:

> Allowing access for employee-owned mobile devices to Transnet systems poses unique challenges to the organisation. Without formalised access restrictions and policy framework, adoption of the employee mobile device access poses operational risks to Transnet systems.

1.4 Research Objectives

1.4.1 *Primary Objective*

The primary objective of this research project is to provide a framework of risks and benefits for Transnet adopting BYOD for end-user computing in support of employee mobility in an increasingly complex, yet virtual environment.

1.4.2 *Secondary objectives*

Two secondary objectives are proposed in order to achieve the primary objective:

- To investigate the impact of BYOD on Transnet employee productivity, and
- To determine the risks in deploying BYOD at Transnet.

This research will provide the contextual factors to implementors in similar enterprises as Transnet, that may influence adoption of BYOD as a strategy to address provision of IT tools of trade to the workforce in support of business operations in a safe and secure manner.

1.5 Delimitations of the study

This research will be focused on the organisational divisions of Transnet. The study will further limit itself to current IT users as these users will have some lived experience to answer the research questions.

This research study will not cover user preferred methods of budgeting, procurement, procurement methods deployed at Transnet, nor the limitations imposed by procurement standard operating procedures deployed at Transnet.

This research will not cover the support and maintenance required for a successful BYOD adoption.

1.6 Definition of terms

BYOD is a concept of allowing users to connect using own technology and end-user computing equipment to corporate IT systems and data for purposes of conducting work, “anytime, anywhere, from any device” (Cho & Ip, 2018b; Scott et al., 2021; Zheng & Ni, 2005)

IT Consumerisation is defined as an allowance of the use of personal devices to undertake work related tasks in the workplace (Gregory et al., 2018; Niehaves et al., 2012; Pani et al., 2020).

1.7 Assumptions

This study assumes that, due to the growing availability of private network access from home, employees are inclined to want to access work any time, from any device regardless of who provides the device. This fact is due to the large numbers of employees who worked from home during the COVID-19 lockdown as only a maximum of 50% capacity per office block was allowed to work from the office, and about 30% in the factory environments.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

It is becoming evident that the purchasing and maintenance of devices by Transnet for employees is unnecessary, particularly now that BYOD is rife and relevant. BYOD provides relief for many organisations and improves employee productivity (Arpaci, 2015). BYOD's main purpose and its implementation is to ensure that employees are able to work effectively and efficiently to reach the organisation's desired goal or target (Franklin & Ismail, 2015).

There are several benefits associated with BYOD, not only for Transnet, but for the employees as well. Firstly, it may relieve Transnet of the duty of procuring laptops for every employee for work purposes. However, mitigation measures of securing sensitive data might have to be implemented (Pillay, et al., 2013). This would be achieved through Transnet installing certain software on these devices for security purposes and device management.

To reiterate, BYOD is effective and efficient in the sense that employees are able to access work material at their convenience and when required by the company (Toperesu & Van Belle, 2017). This paves the way for faster and effective ways of interactions between employees and fulfilling the work required from them by the company (Franklin & Ismail, 2015). In this way, employees might not even have to present themselves at their respective workstations but purely reach out digitally to undertake whatever duty required from them (Toperesu & Van Belle, 2017). Employees who have devices, in most cases always have their devices

with them. Thus, employees would be able to communicate and work irrespective of their location than the old way of requiring Transnet based devices to be able to pull work through (Mitrovic, Veljkovic, Whyte, & Thompson, 2014).

2.2 Definition of topic or background discussion

IT consumerisation can be defined as an allowance of the use of personal devices to undertake work related tasks in the workplace (Gregory, Kaganer, Henfridsson, & Ruch, 2018; Harris, Ives, & Junglas, 2012). This is sometimes used interchangeably with BYOD, which is defined as concept of allowing users to connect using own technology and end-user computing equipment to corporate IT systems and data for purposes of conducting work, “anytime, anywhere, from any device” (Cho & Ip, 2018b; Niehaves et al., 2012; Zheng & Ni, 2005).

This phenomenon of user technologies being used for work and accessing work networks has tipped the scales for technology adoption. Traditionally, innovations were adopted by the organisation, and later seen coming into private user space (Disterer & Kleiner, 2013) . This was the case with the adoption of personal computers, mainly due to the user technical abilities and the cost factors, to this end this technology innovation was only accessible to large organisations.

With the cost factor and the technical ability of end-user virtually disappeared, accessibility of technologies such as mobile devices is on the increase. This increase is instrumental in driving strategies such BYOD (Dell, 2015).

2.3 Drivers of BYOD

The adoption of BYOD may introduce certain challenges. In order to better understand these challenges, some trends are investigated as below.

In a report commissioned by Deloitte, it is perhaps no surprise that phone penetration in the surveyed developed and developing countries has reached 90% (Wigginton et al., 2017). With such an increase in consumer products, users enjoy more and more applications and tools that they use to manage their everyday lives. Organisations had, in the past, resisted adopting or accepting user-owned devices citing security reasons and the IT readiness to support the users. More and more organisations are adopting less strict approaches and allow user-owned devices to connect for work purposes on corporate networks (Anderson, 2012; Baillette et al., 2018). Anderson (2012) further posits, notwithstanding the reasons for innovation adoption, each organisation should have a strategy for BYOD adoption even if for denying all non-organisational issued device connections to corporate infrastructure.

2.3.1 *One user and multiple devices*

The growing trend is that of a single user having access to more than one mobile device. Users often have a smart device for voice calls and accessing mobile applications, whilst on the other hand users have personal computer or laptops to write and manipulate documents. This has resulted in one user making multiple access points into the corporate networks depending on the use (Harsch, 2019), experiencing the applications and services in multitude of ways. As seen in figure

1, some devices such as phones, smart watches are high in mobility whilst not as robust as desktops which are low in mobility.

Figure 1: Device varieties

Source: Anderson, 2012

2.3.2 *Personal and work life overlap*

The propensity for an average South African worker to bring own device to work was cited at 60%, whilst the average worker in the growth markets was 74.9% (Absalom & Drury, 2012), this number may have since increases owing to lockdown regulations companies relied on work from home approach (Furnell & Shah, 2020), this often leads to the increase in insider threat. The insider threat is can be characterised as employee risk of accidental loss of corporate data and or deliberate malicious activity (Fielding, 2020).

The reasons for this behaviour cited by the report are:

a) The non-availability of organisation issued devices, leaving those employees with own issued devices using them for work purposes, or
b) Employees in markets such as South Africa, Brazil and Malaysia were cited as flexible in blurring the lines between work and personal life. These employees use home internet access to conduct work as and when necessary, from anywhere and from any device available to them

Contrasting the attitudes displayed in developing countries, the main concern in the European countries is that of privacy seeking to keep separate the work from the personal, this has resulted in the introduction of a number of regulations to manage and control privacy and security of users (Privacy Rights and Clearinghouse, 2014).

With the interest of companies as well as countries to keep the economy afloat and active during the Covid-19 pandemic, employees were often required to work from home. IT managers had to quickly make resources available to the workforce to enable businesses to operate in the 'new normal' (Jahanbakhsh, Amini-Rarani, Tahmasebian, 2020).

2.3.3 *Anytime and anywhere mobility*

The capabilities BYOD bring to IT users, especially from single devices are:

a) Anything: device connectedness for own use or for work use beyond email or telephony
b) Anytime: device connectedness for use anytime during work or personal time

c) Anywhere: useable by connecting to wireless local area networks (WLAN) or internet

The optimal balance between providing the required access from anywhere, and anytime remains elusive to many IT departments (CISCO, 2014), blocking progress towards the anytime, anywhere requirements of the business and the users alike. The continued pervasiveness of the connectivity anytime and anywhere, presents an opportunity for organisations to have more connected devices, and deploy mobile applications with 24/7 access.

The BYOD is a response to the demand of organisation to be more productive and accessible to employees beyond the traditional boundaries of time and location, and the ever increasing demand by employees to work from anywhere and anytime (Disterer & Kleiner, 2013; Retnowardhani et al., 2019).

The alternative option to the above is to be able to have clear separation of work and personal life. This proved to be unlikely as could be seen with the security challenges experienced during the Covid-19 lockdown situation (Barlette et al., 2021).

2.4 Benefits of BYOD implementation

To best unpack the benefits of BYOD in an organisation, it is important to investigate other related strategies. This will lead to an understanding of each strategy's inherent benefits, risks and controllability. In the main, the literature presents four strategies available to any organisation, namely: Here is your own device (HYOD), Bring your own device (BYOD), Choose your own device

(CYOD), and, On your own device (OYOD). On the one hand, the requirement is the organisation's desire for employee satisfaction, whilst insisting on control and lowering the risks of enabling mobility in the workforce (Gajar et al., 2013).

Table 1: Comparisons of types of mobility

Strategies	Descriptions	Level of employees' satisfaction	Level of risk	Level of controllability
Here is your own device (HYOD)	Organisation issues the devices	High	High	Very low
Choose your own device (CYOD)	The choice of a device comes from a range of devices on offer by the organisation	Medium	Medium	Low
Bring your own device (BYOD)	Devices are privately owned and issued, often with some financial support from the organisation	Low	Low	Medium
On your own device (OYOD)	Devices are privately owned and issued, often with no financial support from the organisation	Very low	Very low	High

Source: Gajar et. al (2013)

For organisations and employees alike, the literature previously indicated benefits of BYOD. On one hand employees, BYOD presents a convenient and flexible connectivity choice (French et al., 2014; Lebek et al., 2013). On the other for organisations BYOD has proven to save costs, increase employee morale and productivity (French et al., 2014). Literature seems to have drawn a correlation between employee and organisation benefits of BYOD, and it is therefore difficult to argue that one may reap a benefit whilst the other does not.

2.5 BYOD and employee productivity

One of the effects of BYOD on an organisation, is perhaps increase in productivity, as employees have a 24/7 access to business applications. In a study conducted by Frost and Sullivan (2016), the researchers argue that the ability to communicate colleagues, partners and customers all the time from anywhere is the most notable improvement by organisations in the mobile age (Frost & Sullivan, 2016). This leads to the concepts of efficiency and productivity: Efficiency is "*the number of labor hours required to accomplish a given task, when compared with the standard in that industry or setting*." Productivity on the other hand is "*the ratio of the output of goods and services to the labor hours devoted to the production of that output*" (Mankins, 2017, p. 3).

Remarkably, organisations have, for decades, sought to be efficient by removing wastage in the production lines, this however falls short when the organisation seeks to spur innovation and reignite profitability as it also needs to remove barriers to tools and services required to complete work. (Mankins, 2017)

Technology-literate employees will benefit the most from mobile devices, as mobile devices remove access barriers to corporate information increasing turnaround times as employees can now access the information for longer work hours (Pillay et al., 2013). Speaking of shortening sales cycles, thereby increasing sales, Ortbach, Brockmann, and Stieglitz, (2014) posit that access to inventory levels, ability to update and access customer profile, pricing and capability to conduct transitions in real-time is important.

2.6 Challenges of an BYOD implementation

Albeit BYOD is an intriguing and beneficial factor within organisations it can also create a big challenge for IT (Osterman Research, 2012). There are many risk factors associated with BYOD. It is likely that personal devices might be vulnerable to data breach and software malware as it is the employee's personal device and might therefore fiddle with content that might pose a threat to an organisation’s classified data. Mitrovic et al., (2014) argues as well that BYOD is not immune to the aforementioned challenges such as malware and data breach. Below are the challenges associated with BYOD.

2.6.1 *Employee challenges*

BYOD adoption often stems from the demand employees make on the organisation for device flexibility. The challenge is compounded by rate of change in the consumer device space. This is further compounded by the variety of devices to choose from. Even further the connection types available to connecting to corporate networks (Anderson, 2012).

Each device may require different steps to connect to the corporate networks to be onboarded. Security protocols may vary depending on the location and the device the employee is connecting from. This needs to be carefully managed, organisations need to achieve some level of simplicity for connecting to the corporate network no matter where the employee connects from, nor from which device the wish to connect (Anderson, 2012; CISCO, 2014).

2.6.2 *User segments and needs*

In a BYOD implementation, it is important to undertake user segmentation analysis. This will avoid pitfalls of bundling all users as homogenous. It will also assist in planning adequate support requirements based on user profile.

Organisations are inherently different. Figure 2 depicts user segmentation based on support requirements. Organisations with low levels of IT support are likely to implement the BYOD with ease. Organisations with high mobile workforce that require high levels of IT support may prove difficult to implement BYOD without an increase in support costs (Toperesu & Van Belle, 2017).

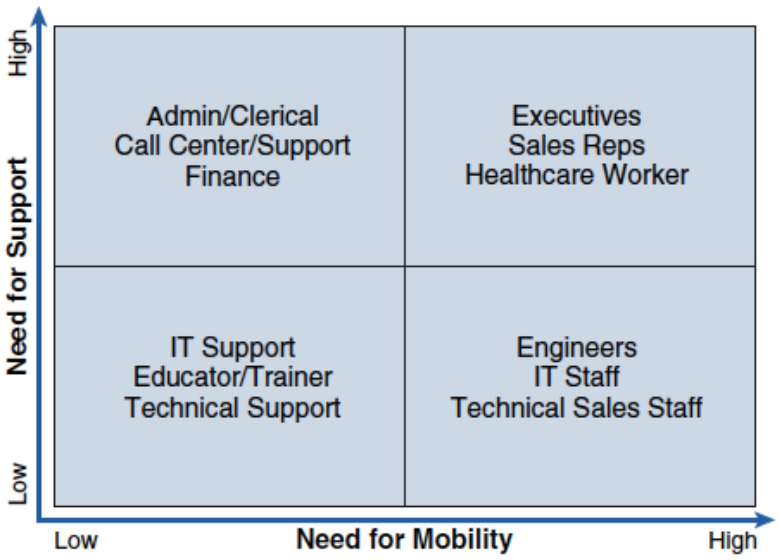


Figure 2: User segmentation

Source: (Toperesu & Van Belle, 2017)

2.6.3 *Organisational Challenges*

The major challenge in IT organisations remains the boundary of security that is now challenged by the boundary extension presented by employee-owned devices. Traditionally IT department held total control of corporate network connected devices (Osterman Research, 2012).

This was a more manageable support situation as the range and type of devices to be allowed was decided solely by the organisation. This expansion of the scope however in itself does not introduce new risks on their own, but rather the extend of the current risks (EY, 2013). The risk landscape can thus be broken into three areas, namely securing the mobile devices, addressing the application risk, and lastly, managing the environment. In the BYOD enabled environment, employees have access to their own services and applications as the devices can be used

for work purposes or personal use (Kabanda & Brown, 2014), this may lead to IT security support issues due to unknown applications and services (Fani et al., 2016). Employees should always be made aware of their part in securing organisational data (Madzima et al., 2014). In the implementation of BYOD, the organisation need to address several characteristics about BYOD security, table 2 lists the key issues identified in literature that need to be complied with.

Table 2: Security characteristics of BYOD

Characteristic	**Data Extract**
Risk identification	BYOD is an institutionalised security risk which requires thorough assessment (Lawrence & Moyo, 2006)
	There are inherent risks to confidential information of the organisation in the use of BYOD (Garba et al., 2015)
Security requirements	"Legal and liability issues should be considered and stated in the BYOD policy" (Yang, Vlas, Yang, & Vlas, 2013, p. 412).
Context of the organisation	From a perspective of internal IT, employee owned devices can present dynamic security risks (Allam et al., 2014)

	“Organizations require secure, accurate and reliable information because they use or depend on IT to develop, manage, and communicate substantial information resources and knowledgeable facts” (Garba et al., 2015, p. 39)
Device Analysis	“Devices should be registered for participation in the BYOD program, officially approved for use, and provisioned with required security settings” (Zahadat, Blessner, Blackburn, & Olson, 2015, p. 86)
Employee role	“Users should be educated as they perform their daily activities, with frequent policy reminders that are non-intrusive and relevant to their current task” (Charbonneau, 2011)
IT Administration	“Organizations BYOD should realize the impact BYOD can have on technical support”
	“It is crucial for organizations to employ a proper security model for mobile devices as security challenges will increases in organizations” (Eslahi, Naseri, Hashim, Tahir, & Saad, 2015, p. 189)
BYOD Policy	“Policies are a good starting points for gaining control on an enterprise as they provide guidelines for BYOD adoption” (Madzima, Moyo, & Abdullah, 2014, p. 6)

	"The policy should provide clarity on how devices will be used and how IT can meet those needs"
Compliance	"A BYOD policy is likely to improve compliance by educating employees the risks associated with their devices" (Madzima, Moyo, & Abdullah, 2014, p. 6)
	Policy violation must be accompanied by swift punishment to deter would be violators (Johnston & Warkentin, 2015)
	"Companies must re-evaluate BYOD compliance" (French et al., 2014, p. 194)

Source: Author's work

2.6.4 *The digital work era*

The digital work era is a new phenomenon, which brings forward great mobility and flexibility in the workspace (Hanelt et al., 2015; Köffer, 2015). Organisations have overtime being constantly looking for ways to improve productivity, and enable digital workspace (Köffer, 2015), perhaps more so due to the COVID-19 pandemic.

Organisations spent a lot of money and resources in traveling, employees are required to cover vast territories spending a lot of time in travel (Bharadwaj et al., 2016; Haffke et al., 2016). Digital work is a probable option offering great flexibility, enabling continued collaboration without the boundaries of location and time (Colbert et al., 2016).

New infrastructure need to be put in place to facilitate this new workspace, Dery, Sebastian, Van Der Meulen, and Meulen, (2017) conceptualise three levers that drive the design of this new IT and infrastructure. The design levers are listed in table below.

Table 3: Design levers

	Systems	Social	Space
IT Infrastructure	• Unified communications • Mobile enabled devices	• Corporate Social Media	• Hot desking • Open plan offices
Aim	Borderless, always on collaboration	Quicker collaboration and creation of ideation space	Create new interpersonal workspaces and encourage collaboration

Source: (Dery et al., 2017)

2.6.5 *Securing the mobile devices*

When it comes to mobile devices, a well-formed adoption program should concern itself with the user types, and a clearly defined set of support segments. The driver for adoption should be a well-articulated plan driven largely by the user experience (Gajar et al., 2013; Ophoff & Miller, 2019). Some threats to mobile

devices are similar to personal computers, however mobile devices require additionally specific intervention targeted to mobile devices (Gajar et al., 2013; Kearns, 2015), a list of some of the threats is:

- IT Virus infections
- Data leakage threats
- Modification or destruction of data files
- Peer-to-peer messaging
- Impersonation
- Message contamination
- Jail-breaking
- Denial of Service (DoS) attacks

2.6.6 *Addressing the application risk*

The main accelerator in the integration of mobile devices in people's lives is the applications. From mapping applications, social media networking, to productivity tools, applications have become pervasive in the workplace as they make available conveniently the information required to carry out daily tasks (Kearns, 2015). However without proper controls of the applications loaded on the mobile devices, malware and viruses can hide themselves in malformed, untested applications (Hoffmann et al., 2016), more dangerous malwares can even destroy data sitting on corporate server (Kearns, 2015).

A level of awareness of current malwares, identity theft, phishing attacks and viruses should be top of mind for BYOD adoptions, this should be supported by

training on how to mitigate against risk arising from malwares and viruses (Garba et al., 2015)

2.6.7 *Managing the environment*

A critical task in the management of IT assets is the upkeep of the assets inventory. Mobile device turnover and evolution is normally two years versus the five to six years for traditional enterprise computers. This leads to a laborious task of keeping up with the maintenance, support, inventory management, patches and updates required for IT assets. This may not be a direct risk but it is a good mitigation against malwares (BSI, 2018; Gajar et al., 2013).

Challenges related to mobile device may also stem from the type of operating system in use. For instance blackberry was considered more secure as it offered organisation total control of the environment whilst android phones do not and therefore referred to as not so secure (Kearns, 2015). Platform vulnerabilities have been widely researched and the organisation may need to ensure deployment of Mobile Device Management (MDM) technologies to better manage the environment.

2.6.8 *A supporting framework*

Often adoption programmes concern themselves with technology, neglecting people and processes that will drive operational goals. Non-technical controls such as training, policies and user awareness are key in the implementation of BYOD (Adedolapo, 2015; Fani et al., 2016). In a study by Gustav and Kabanda

(2016) in the context of South African financial institution indicates that environmental variables are to be considered before a BYOD adoption.

This study positions itself in the context of the PERM (Perceived e-Readiness Model) framework (Molla & Licker, Paul, 2005). This model has been used several developing countries when investigating factors affecting BYOD adoption. This is appropriate for Transnet which is in South Africa, as South Africa is considered a developing country. Two contextual constructs are identified in the model when examining adoption,

a) Perceived External e-Readiness (POER),
b) Perceived Organisational E-Readiness which comprise a number of successive factors (PERM factors).

The POER construct investigates:

i. perception of the organisation, its understanding, organisational projection of technology and the potential risks and benefits (innovation imperatives);
ii. the manager's commitment (managerial imperative); and the
iii. organisational components e.g. infrastructure, processes and resources (organisational imperative). Factors of POER are listed in figure 3.

The organisation's assessment of external factors defines the PEER factors include (Molla & Licker, Paul, 2005).

i. preparedness of the government to promote, regulate and facilitate technology adoption,

ii. the organisation and its partners readiness to adopt technology, and lastly

iii. availability of support organisations for successful implementations. Factors of PEER are listed in figure 3.

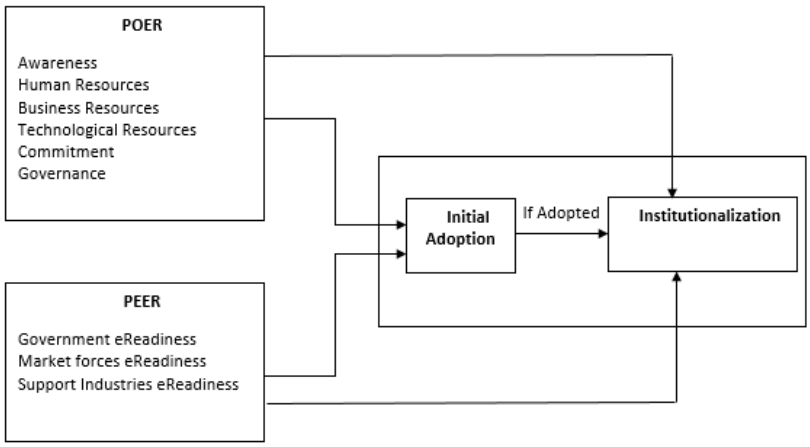


Figure 3: PERM Model

Source: (Molla & Licker, Paul, 2005)

The table below summarises the factors identified as drivers for BYOD as exploited by various authors.

Table 4: PERM Factors

PERM Factors		BYOD Factors	Description	Data Extract
Organisation - POER	Technology Readiness	Privacy	Creating trust as regards the employees and the organisation on usage of mobile devices in the organisation	"Placing a hold on mobile data may be more difficult than it is for traditional systems – and much more difficult when it is located on devices that are under the control and ownership of individual employees" - Osterman Research (2012, 7)
		Security	The capability of the organisation to respond to inherent risks arising from adoption of BYOD	"Existing controls such as firewalls, intrusion detection systems, and proxy servers are also effective for mobile security but are not sufficient and may not address employee misuse, new malware, theft, and compromise resulting from lax security." - Kearns (2015)
		Infrastructure	Available resources and ICT infrastructure to support BYOD adoption in the organisation	"On the other hand, technical support for BYOD proved challenging as a high number of requests needed to be serviced and support staff needed training in this area. As reported by the participants, setting up the IT infrastructure for BYOD

				can be costly for the organization" - Ophoff & Miller (2019)
	Governance	Policies	Established principles and guidelines to employees on the usage of employee-owned devices for work	"It was seen that policies (mainly security-related) and information security training were an important part of the organization's BYOD strategy and helped to address the device and data risks." - Ophoff & Miller (2019)
	Business Resources	Costs	Capital resources/expenditure in relation to BYOD adoption	"They stated that, inasmuch as they would have preferred to provide standardized equipment for their employees, they simply do not have the capital for such a project" - Adedolapo (2015)
	Awareness	Education/Training	Employee training in handling BYOD	"Formal controls can include policies while informal controls can include education and training, and technical controls could be mobile device management (MDM), Citrix or encryption software" - Ahmad (2013)

	Human Resources	Expertise - ICT	Ability of the organisation in relation to ICT matters and the skills required	"SMEs complained about the shortage of ICT expertise in South Africa. They perceive that this affects the adoption of BYOD within SMEs due to the limited amount of ICT expertise to manage dependent environmental infrastructure, which BYOD depends on" - Adedolapo (2015)
	Commitment	Senior Management Support	Commitment and Support from top management in support of BYOD adoption	"Agency managers must think through their policy on work-related and personal applications, because all device applications may have an impact on network security." - Fiorenza (2013)
Environmental - PEER	Market Forces	Business Partners, Suppliers & Customers	The influence obtained from the ecosystem in driving BYOD adoption in the organisation	"the means and mode of communicating with customers and client is shifting from the traditional use of fax, emails and telephone calls to the use of social media and instant messaging" - Adedolapo (2015)
	Supporting Industries	Supporting Industries	Availability of BYOD support from other organisations in the management of BYOD	"The environmental context includes the industry context, competitors, presence or absence of technology service providers, macroeconomic

				context, and regulatory environment. Competition may stimulate the adoption of innovation" - Ophoff & Miller (2019)

Source: Author's work

The introduction of the Technology Acceptance Model (TAM) was initially introduced by (Davis et al., 1989) as demonstrated in figure 4. This model has been used before in the prediction of the technology acceptance by potential users. Two basic factors are used with this model, namely the perceived usefulness (PU) and perceived ease of use (PEOU). Perceived usefulness is based on the users perception about how technology will be of assistance to them in completing theirs tasks. This is the belief or perception by the user that technology will enhance their performance in carrying out their tasks

The PEOU is about how the users perceives the effort required to complete their tasks aided by technology, this is about the use of technology being easy. In the context of this study the PU and PEOU are important factors in the technology acceptance by employees in the process of the mobility preference (Deepshikha Aggarwal, 2018). This is underpinned by the believe that users will choose a technology that they perceive to be useful to them in carrying out their tasks.

In deciding which technology to use to enhance mobility in the workplace, it is also important to look into what the organisation perceives to be useful technologies in the workplace.

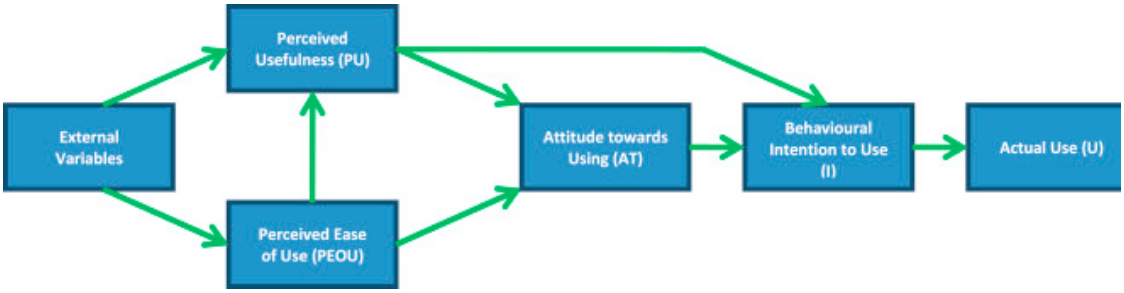


Figure 4: Technology Acceptance Model

Source: (Davis et al.,1989, p. 985)

2.7 Conclusion of Literature Review

The literature review has demonstrated the body of work conducted in the BYOD space. It has further demonstrated benefits and risks associated with the BYOD adoption. The propositions raised from this review will assist in the determination of the critical factors for a successful adoption of BYOD in the organisation.

2.7.1 *Proposition 1:*

A well formulated adoption of BYOD can yield positive benefits for Transnet

2.7.2 *Proposition 2:*

An increase in the access of corporate information and tools increase employee productivity

2.7.3 *Proposition 3:*

Employees fit for BYOD needs to be matched against their support requirements to reduce frustrations, increasing chances of real tangible productivity.

2.7.4 *Proposition 4:*

A malformed environment can lead to BYOD adoption failures, introducing risk to the organisation

CHAPTER 3. RESEARCH METHODOLOGY

This section describes the methodology that was followed to address the propositions that arose from the literature review and that have been put forward as possible solutions to the research objectives.

3.1 Research approach

The approach used in this study is explorative and qualitative and made use of the Case Study Methodology (CSM), in particular. Due to the complex setting of issues being explored, the selected methodology is deemed appropriate as it allows for the in-depth exploration of issues in real-life setting and is therefore applicable in this study (Crowe et al., 2011). To understand the subjects' actions, views, opinions and thoughts about the BYOD, the interpretivist approach was selected as appropriate as described by (Aberdeen, 2013). To explore the research problem and objectives (see section 1.4 in chapter 1), the IT policy documents, the business requirements specifications and the various IT strategy documents were scanned. This was followed up with a semi-structured questionnaire to obtain specific opinions in regard to the research objectives outlined in chapter 1.

The Southern Africa countries encompasses small and medium private businesses, resource based activities and state owned enterprises (SOE)(Balbuena, 2014), similarly the South African government has at least 131 state-owned companies (SOC). SOCs play a vital role in the direct service delivery to citizens as they operate as the state commercial vehicles in delivering

basic services such as water, sanitation health services etc.(Africa, 2020; Balbuena, 2014). In the logistics and freight business, the government established Transnet (SOC). This study will focus on the provision of mobility tools at Transnet as Transnet operates nationally and into international borders, the company is large enough to provide an adequate basis for requirements in public sector companies.

3.2 Research design

The research design proposed involved conducting a literature review on the BYOD phenomenon, followed by collection of data from Transnet internal documents and by way of an online questionnaire. This approach is useful in exploring the participant's lifeworld. This study purposively selected employees from Transnet in all the operating divisions. The participants were selected based on their current roles in the IT organisation, possible knowledge on current initiatives in the organisation and based on their current IT use.

The study is organised in the following way: Discussing the benefits of implementing BYOD, determining the risks and concerns associated with the implementation and understanding how BYOD influence employee productivity. The above-mentioned are based on the literature reviewed, propositions tested via data collected by questionnaire and the results and finding is reported in this study.

3.3 Data collection methods

The data was collected by way of an online questionnaire to the selected participants and from TRANSNET documents and artefacts such as policies and procedures as outlined in chapter 4. The questionnaire was by a way of a combination of closed-ended and open-ended questions, thus allowing for in-depth extraction of information from the participants and is suited for this study. The questions are aimed at answering this study's primary and secondary objectives.

3.4 Population and sample

To select the participants, this study used a non-probability (purposive) sampling. This is so in order to ensure that the participants are either directly involved in the technology implementation or are key decision makers in IT delivery in the organisation as this will assist in answering the interview questions on BYOD implementation.

3.4.1 *Case Site*

The case will be conducted in Transnet, a state-owned company (SOC). Transnet SOC Ltd which is a huge South African rail, port and pipeline organisation, headquartered in the Carlton Centre in Johannesburg. It was framed as a restricted organization on 1 April 1990. The shareholding of the company is with the Department of Public Enterprises (DPE), of the South African government.

The organisation was formed by rebuilding into specialty units the activities of South African Railways and Harbours and other existing tasks and items.

Transnet is the custodian of ports, rail and pipelines, Transnet has a responsibility to ensure the optimal development of the national freight system. The Company is thus charged with enabling and contributing to an internationally competitive freight system for South Africa. Specifically, Transnet must ensure sustainability and value-adding ports, rail and pipelines, and that the national freight system is able to satisfy economically viable customer demand at internationally competitive levels.

The organisational divisions of Transnet include:

- Transnet National Ports Authority – Chief Administrator for South Africa's Ports
- Transnet Pipelines - Chief Administrator of South Africa's fuel pipelines
- Transnet Engineering - rolling stock assembling and maintenance
- Transnet Property – Property Management of immovable assets
- Transnet Freight Rail – Freight and logistics business
- Transnet Port Terminals – Container terminal operations

3.4.2 *Sample and sampling method*

A sample of six organisational divisions was used, and a total of 20 participants were approached. The participants were purposively selected based on their experience and knowledge of the BYOD. Farrugia (2019) posits that, while the

sample size may be small, in the qualitative study the small sample size will allow for exploration of the richness and detail of the data been collected.

The participants of this study consisted of employees already using own devices to access work and IT decision makers in Transnet. The list of the targeted participants is contained in table 4.

Table 5: Profile of respondents

Description of respondent type	Number to be sampled
General Manager	6
Senior Manager	6
BYOD users	8
TOTAL number of respondents	20

3.5 The research instrument

The research instrument is adapted from the PERM Framework (Molla & Licker, Paul, 2005). To enable the researcher to observe, ask and record responses to the research question the instrument is comprised of a combination of closed and open-ended questions. The themes identified in section 2 form the basis of the instrument design. The instrument contains three sections namely, environmental, organisational and closing section (see Appendix A).

Questions in the organisational section were formulated to engage the participants in their understanding of the BYOD program within the organisation to establish levels of awareness from the view of the participant. The

management support and human resources sections contained questions that would explore what management interventions are in place, the capacity of the employees to fully engage in BYOD and what can be done to enhance the current status quo. The business resources, technological readiness and policy/governance sections explored the organisational readiness to undertake BYOD.

3.6 Procedure for data collection

The targeted respondents were approached directly. A pilot to determine the timing and the clarity of the questions was undertaken before approaching the participants to ensure quality and good time management. Together with the request for participation in this study, respondents were sent the approval and ethics letter, the respondents were further advised that they may opt out of the study at any time.

3.7 Data analysis and interpretation

This study employed a thematic analysis to analyse the semi-structured interview transcripts. The entire data set were put through a rigorous process to identify, report and analyse themes emerging from the data (Braun & Clarke, 2006). Data was then coded inductively without associating any meaning to the data whilst important data was coded. Through a deductive approach meaning was then assigned to the themes identified in section 2. This study employed the Braun and Clarke (2006) approach to conduct the thematic analysis as shown in figure 5.

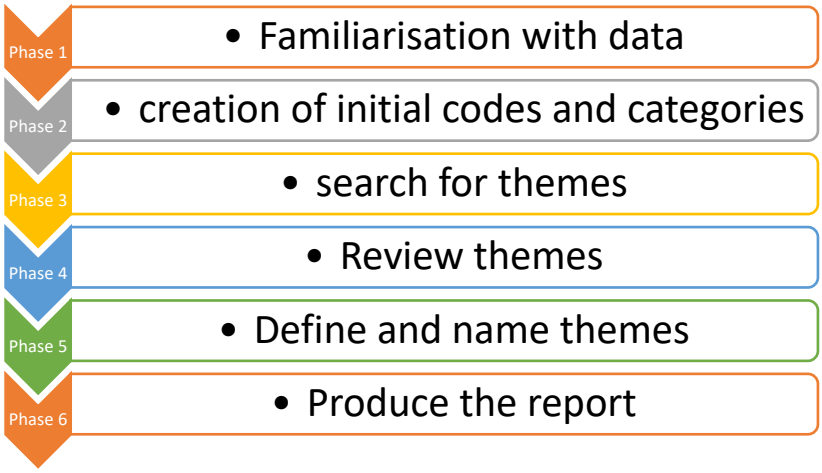


Figure 5: Thematic Analysis phases

Source: Braun and Clarke (2006, p. 87)

3.8 Limitations of the study

The study was conducted during the COVID-19 lockdown restrictions providing a good opportunity to conduct such a study. However, the interviews needed to be conducted electronically which did not provide for follow up discussions.

Albeit Transnet is one of the large state-owned companies in South Africa, the findings of this study might not be generalised to other state-owned companies. This study, however, provides a good foundation for future studies on implementation of BYOD. Due to the time constraints for the master's degree program, this study adopted a cross-sectional timeframe, as data was collected at one point in time. Future studies may consider longitudinal timeframe, collecting data over longer periods of time. This approach may assist in conducting deeper understanding on the contextual factors in the implementation of BYOD.

3.9 Validity and reliability

Since both validity and reliability are aimed at ensuring credibility of the qualitative research (Golafshani, 2003), this study considered both validity and reliability together. To extrapolate the results to similar contexts and situations, the credibility of the results is a fundamental requirement, it is therefore imperative for the qualitative researcher to observe validity and reliability (Patton, 2015).

Bashir, Afzal, and Azeem (2008) describe validity and reliability in qualitative studies as trustworthiness. Four strategies for assessing trustworthiness are identified by (Moser & Korstjens, 2018), as transferability, credibility, confirmability, reliability and reflexivity. To ensure that this study meets the requirement for trustworthiness these methods will be employed:

a) Triangulation of theoretical perspectives – this will address bias,
b) Triangulation of data methods – this will reduce distortion from researcher or single source, and
c) Detail description of the interpretation, collection and analysis methods – this will increase levels of repeatability.

3.10 Ethical considerations

In all instances the study remained constrained academically and professionally in gathering all the relevant information needed to conclude this study.

Given the fact that data collected was through secondary sources, the main ethical consideration here has been acknowledgement and citation of the

published sources used in the study. The researcher tried to avoid all forms of research misconduct, fabrication, falsification or plagiarism, including misrepresentation of facts and misinformation. Ethically, this project adhered to the Wits Business School ethical guidelines.

Careful consideration for issues of ethics is observed, furthermore it is important for the researcher to always “abides by the principle of informed consent” (Scott and Morrison, 2006:88) and observe the research ethics (McMillan and Schumacher, 2006). Prior to embarking on the collection of data, the researcher obtained approval from the Wits Business School ethics committee to continue with this study.

When collecting data, it was expressed to each participant that the participation in this study is voluntary and that they may opt out at any.

Once the committee had verified the study’s ethical credibility and approval was granted the data collection commenced to complete investigation. The letter of approval will be annexed as Appendix B.

The researcher approached Transnet SOC Ltd for ethical clearance and approval to undertake the study in Transnet was obtained prior to collecting any data from the targeted organisational divisions. The approval letter will be annexed to this study, once granted by Transnet SOC as Appendix C.

The study targeted and collected data from all organisational divisions of Transnet, “careful attention was paid to the various levels of power within the organisation” (Scott and Morrison, 2006:88).

CHAPTER 4. DISCUSSION OF THE FINDINGS

4.1 Introduction

This section presents the findings of the study. By using thematic analysis, I will analyse the data that was collected. Due to time limitation and the Covid-19 related challenges, out of the 20 respondents approached only 10 were ultimately available and thus only the data from these will be used.

4.2 Discussion pertaining Transnet documentation

Below in table 5 is the analysis of the documents forming the governance framework for mobile device users at Transnet. The collection focused only on the currently approved and under review documentation.

Table 6: Reviewed IT Policies

#	Document Name	Status	BYOD Mentions	Except
1.	Mobility Policy	Active Policy	0	None
2.	Mobility Policy	Draft review	1	"The use of your own device must adhere to the Transnet ICT Policies, namely the Information Security Policy, Transnet Bring Your Own Device (BYOD) Directive, Transnet Acceptable Use Policy, Transnet's Records Management Policy,

				Transnet's Cloud Policy, Transnet's User Management Standard."
3.	Transnet Information Security Policy	Active Policy	0	None
4.	Transnet Cloud Policy	Active Policy	0	None

It is worth noting that although the above policy set may not address the governance of employee-owned devices, there is a specific project underway to address the provision of IT tools of trade and aims to also enable BYOD in the organisation.

The study came across a strategy review document jointly written by human resources and IT management to address specific challenges in the provision of IT tools to a wider end-user community in the organisation. The problem in this strategy is articulated as:

"*Can we reduce cost by revising the Transnet Enterprise Mobility Policy and/or approach?"*

The strategy document in response to the above challenge proposes at least three responses as articulated in the figure 6.

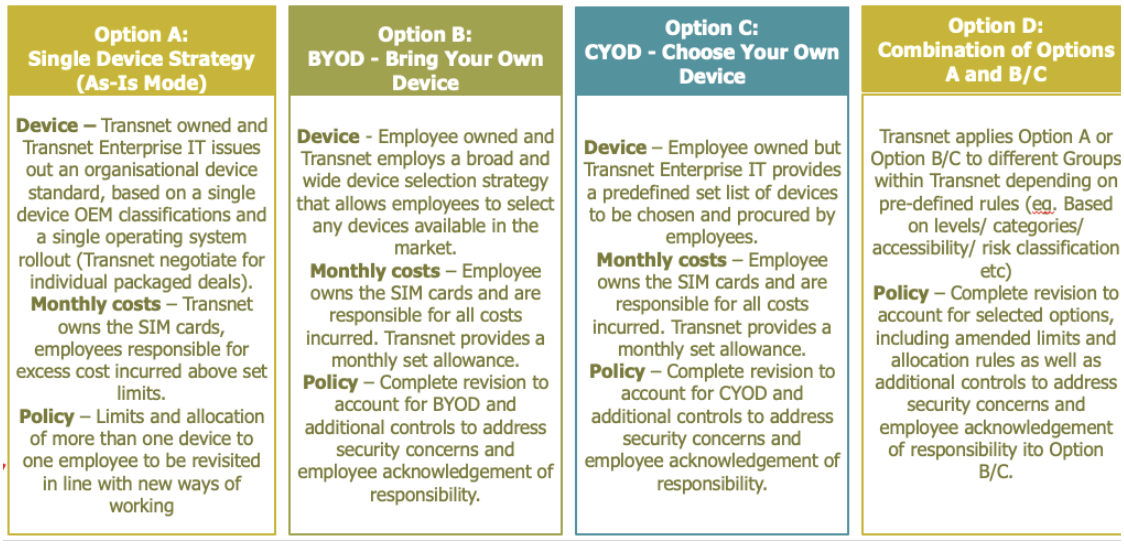


Figure 6: Proposed Mobility Approaches

Source: (Transnet, 2020)

As can be seen in the above discussion, the organisation governance framework shows gaps in addressing and adopting BYOD program, however as it will be demonstrated in the below findings users are already accessing the corporate systems via own devices. Commendable though is that there are initiatives underway to address the gap.

4.3 Discussion pertaining to Proposition 1

The adoption of BYOD can be described as the act of utilising employee personal devices for work related tasks. This act may emanate or not from company practices and expectations, or from the employees themselves. In the case of this study, results show that the current deployment of BYOD in the organisation is both by the act of employees and the organisation, leading to different experience in the organisation. This was the case as one responded remarked:

"It is slow as policy still needs to be drafted and users are running it"

Encouraging is that many users seem to be aware of the BYOD program in the organisation as can be seen in figure 7. Employee awareness of the BYOD elements and their perception, and or their understanding of these elements can be referred to as awareness (Molla & Licker, Paul, 2005).

Figure 7: BYOD Program Awareness

As per figure 8, current policy framework formulation is at an advance position as most respondents answered affirmative when asked if they are aware of any policy provisions for BYOD within the organisation.

Figure 8: Policy provisions for BYOD

Given the responses by the responded on their awareness of the BYOD initiatives in the organisation, and the availability of the policy provisions for the same. My

conclusion is that the benefits of BYOD adoption to the organisation are attainable and achievable, this can be seen in the respondent's remark to the question of productivity and said:

"Flexible working environment and access to work and increased productivity"

4.4 Discussion pertaining to Proposition 2

To get the benefits ascribed to BYOD adoption, management support and commitment in the BYOD program is important as the resource allocations are management discretion, this commitment includes and is not limited to vision and strategy (Molla & Licker, Paul, 2005). There seems to be a perception amongst respondents that the management is not entirely supporting BYOD adoption. When asked if the IT management supports BYOD, 68% of the respondents answered no as per figure 9.

Figure 9: IT Management support for BYOD

The respondents further provided their rating as to the commitment of management towards the BYOD program, and as per figure 10, expressed that management may not necessarily be against the BYOD program.

Figure 10: Management's commitment rating

To encourage adoption of any initiative, training is paramount as it encourages responsible use and ensures quality of experience. When asked if any training has been provided for BYOD by the organisation or attended any training before on BYOD, an overwhelming 100% of the respondents said they never attended any BYOD training nor offered any by the organisation, see figure 11 for results.

Figure 11: Training offered or Attended

Due to the lack of clear strategy and vision for BYOD and the supporting business resources such as training and funding, the organisation may not be realising the benefits of BYOD adoption and therefore may not objectively measure the levels of productivity resulting from the program. If the status quo remains the risks of data breach and loss may increase, as remarked by one of the respondents:

"BYOD is an IT environment for tools of trade provisioning and can bring about security threats and should therefore be sponsored by ICT"

4.5 Discussion pertaining to Proposition 3

Ability for self-service by employees can reduce technical difficulties that may lead to slow adoption of the BYOD program. So a good adoption should not concern itself with the ease of the use and the security of the solution (Prashant Kumar Gajar, n.d.), when asked whether the respondent configured the mobile device management on their device when connecting to the environment, 63% said no whilst 38% said yes as can be seen on figure 12. When asked how easy it was to configure the mobile device management, an average of 3.71 rating was achieved on a scale of 1-5, 1 being difficult and 5 being easy

Figure 12: Respondents with MDM configured

The respondents where then asked what they think of IT support in support of the BYOD program, see figure 13. 25% of the respondents said that the readiness of IT to support BYOD was highly encouraging, 38% said it was discouraging and 38% said the IT readiness was medium.

Figure 13: IT Readiness to support BYOD

While the fit for BYOD may be matched with the user or employee needs, these needs are constantly changing. Of greater importance is the agility of support and training offered to users. The organisation must strive to make the service easy to use whilst preserving security of its assets and data.

4.6 Discussion pertaining to Proposition 4

The successful implementation of a BYOD program largely requires a conducive environment to operate from. This environment will include but not limited to a policy framework that support the program, business resources such as finance, training, IT support etc. that will ensure adoption and continued improvement of the program (Adedolapo, 2015; Fani et al., 2016).

When asked if a mobile device management (MDM) has been configured on their mobile devices, over 60% of the respondents answered negatively indicating a potential breach in the access of corporate data, see figure 14.

Figure 14: Users with MDM Configured

Respondents where then asked if a policy exists in the organisation governing the use of mobile devices in the environment, 100% of the respondents answered yes to the question, see figure 15

Figure 15: Availability of mobile device policy

When asked whether the mobile device management policy covers for the use of personal devices, the answer was 50% for yes, and 50% for no, see figure 16

Figure 16: Policy support for BYOD

The data suggests that although the policy may exist in the organisation, the understanding and application by users may not be consistent leaving the organisation in the risk of non-compliance. Furthermore, a significant number of users may have configured and obtained unauthorised access to corporate assets as not MDM has been configured on their device ensuring both security and regulatory compliance for such access.

CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS

5.1 Introduction

Presented in chapter 1 was the aim of this study, investigating the framework for BYOD by state owned enterprise in South Africa. Presented in chapter 2 was related works in BYOD. Covered in chapter 3 was the research methodology, in chapter 4 the findings were discussed. The current chapter summarizes the findings with an intention to review to what extent the research question has been addressed.

5.2 Conclusions regarding research objectives

The primary objective of this research project was to provide a framework of risks and benefits for Transnet adopting BYOD for end-user computing in support of employee mobility in an increasingly complex, yet virtual environment. Of interest was whether by increasing employee mobility you can improve their productivity whilst de-risking the organisation and its data assets.

Findings indicate that the contextual factors such as organisational and environmental factors influence the adoption of BYOD. This means that for the successful adoption of BYOD in the organisation, there needs to be environmental and organisational readiness. Discussed in terms of opportunities and threats were organisational factors such as management support, business resources, awareness and technological readiness.

Identified in this study was the human resources and business resources as opportunities, identified challenges are awareness, lack of management support, lax formal governance and technological readiness in support of the BYOD program. The study has further identified “informal governance” and “environmental readiness” that has legitimised BYOD in the organisation by the requirements imposed on the workforce by Covid-19 to work from home.

It is without any doubt that due to trends such as IoT, Artificial Intelligence (AI) and Machine Learning (ML), the explosion of Internet Protocol (IP) enabled mobile devices is soaring without an end in sight. This shift in the use of IT resources has increased the surface area for attacks and put pressure on IT resource management. The ability to provide secure mobile solution to the organisation has proven to be complex, and therefore relying on perimeter security, control of employee devices, policy enforcement tactics are not adequate to address the current data insecurity challenges the IT organisation now face.

With the Covid-19 lockdown and restrictions, BYOD as a response is the correct response to enable the organisation to continue its business imperatives. However, IT managers need to enhance the security of BYOD to support the privacy, confidentiality and sovereignty of the corporate data that may be accessed by the employees remotely and in their personal devices. In any event the organisation despite the ownership of the device used to access the data sets is ultimately responsible for its data security. With the use of MDM, the organisation can balance the security of its data assets as well as preserve

privacy of the employee data on the employee device providing the balance required for the adoption of BYOD in the organisation.

By highlighting the contextual factors influencing BYOD, this study has assisted in bringing into focus the areas that management need to focus on for an effective adoption of BYOD program. Mobility enablement by adopting BYOD can improve productivity as seen in the work from home phenomenon that was adopted during the Covid-19 lockdown, however the findings of this study suggest that without a well-planned and coordinated governance framework the organisation may be exposed to risk of data loss, privacy and confidentiality.

5.3 Recommendation and Contribution

By undertaking a study into the factors influencing the adoption of BYOD this study has contributed to literature, in particular to the areas of environmental and organisational readiness. This study highlighted the contextual environmental and organisational factors that precedes the adoption of BYOD in the organisation.

Employed in this study were multiple theoretical perspectives such as the use of PERM and TAM thus making a theoretical contribution. The weakness and bias arising from single-theory study was reduced and credibility of results enhanced.

Applicability of PERM in the South African organisational context was applied. The applicability was high as the theory assisted in highlighting original themes that would later be linked to the organisational characteristics of the SOE in South Africa.

Findings of this study will assist the IT managers looking to adopt BYOD in their respective organisation. Findings indicate a governance weakness in dealing with security with the BYOD program. Transnet like any other business may suffer irreparable damage arising from a security attack. Due to the important contribution to the South African economy, Transnet need to sharpen its focus in the security training and awareness campaign of its workforce and partners.

Lack of policy framework and implementation of policy regulating the BYOD program was highlighted in the study. Findings revealed inconsistent use of mobile device management, lack of awareness of the policy and illegitimate access to organisational assets. Due to the similarity of the other state-owned IT organisation regulatory and governance frameworks, findings of this study can be used in support of the BYOD programs in the respective organisation. Against these findings it is critical that the organisation put a focus into:

- Regulating the access to organisation's business systems
- Implement the Mobile Device Management to manage devices
- Provide training and awareness about responsible use of BYOD

REFERENCES

Aberdeen, T. (2013). Case study research: Design and methods (4th Ed.). *The Canadian Journal of Action Research*, *14*(1), 69–71. https://doi.org/10.33524/cjar.v14i1.73

Absalom, R., & Drury, A. (2012). BYOD: An emerging market trend in more ways than one. *Employee Attitudes to Work/Life Balance Drive BYOD Behavior, Logicalis White Paper, OVUM*, 1–12. http://www.ovum.com/research/byod-an-emerging-market-trend-in-more-ways-than-one/

Adedolapo, A.-A. (2015). *Bring Your Own Device (BYOD) Adoption in South African SMEs* (Issue November). University of Cape Town.

Africa, G. of S. (2020). *State-Owned Enterprises (SOEs) | South African Government*. Government of South Africa. https://www.gov.za/about-government/contact-directory/soe-s

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*, 56–65. https://doi.org/10.1016/j.cose.2014.01.005

Anderson, N. (2012). Cisco Bring Your Own Device. *Cisco*, *10*(7), 1–24.

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own

device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management*, *43*, 76–84. https://doi.org/10.1016/j.ijinfomgt.2018.07.007

Balbuena, S. S. (2014). State-owned Enterprises in Southern Africa : A Stocktaking of Reforms and Challenges. *OECD Corporate Governance Working Papers*, *13*, 1–90. http://search.ebscohost.com.ezproxy.liv.ac.uk/login.aspx?direct=true&db=edsoec&AN=edsoec.5jzb5zntk5r8.en&site=eds-live&scope=site

Barlette, Y., Jaouen, A., & Baillette, P. (2020). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information Management*, 102212. https://doi.org/10.1016/j.ijinfomgt.2020.102212

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information Management*, *56*(April 2020), 102212. https://doi.org/10.1016/j.ijinfomgt.2020.102212

Bashir, M., Afzal, M. T., & Azeem, M. (2008). Reliability and Validity of Qualitative and Operational Research Paradigm. *Pakistan Journal of Statistics and Operation Research*, *4*(1), 35. https://doi.org/10.18187/pjsor.v4i1.59

Beckett, P. (2014). BYOD - Popular and problematic. *Network Security*, *2014*(9),

7–9. https://doi.org/10.1016/S1353-4858(14)70090-X

Bharadwaj, A., Sawy, O. A. El, Pavlou, P. A., & Venkatraman, N. (2016). Digital Business Strategy: Toward a Next Generation of Insights. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brodin, M., Rose, J., & Åhlfeldt, R.-M. (2015). Management issues for Bring Your Own Device. In V. M. Kostantinos Lambrinoudakis Marinos Themistocleous (Ed.), *European, Mediterranean & Middle Eastern Conference on Information Systems 2015 (EMCIS2015), 1-2 June, Athens, Greece*. European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS). http://his.diva-portal.org/smash/get/diva2:817936/FULLTEXT01.pdf

BSI. (2018). *Information and Cyber Challenges in the Public Sector Survey 2018 Contents Executive summary*.

Charbonneau, S. (2011). The role of user-driven security in data loss prevention. *Computer Fraud and Security*, *2011*(11), 5–8. https://doi.org/10.1016/S1361-3723(11)70112-9

Cho, V., & Ip, W. H. (2018a). A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659–673. https://doi.org/10.1080/17517575.2017.1404132

Cho, V., & Ip, W. H. (2018b). A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659–673. https://doi.org/10.1080/17517575.2017.1404132

CISCO. (2014). *Device Freedom Without Compromising the IT Network*.

Colbert, A., Yee, N., & George, G. (2016). *The digital workforce and the workplace of the future*. Academy of Management Briarcliff Manor, NY.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*, 100. https://doi.org/10.1186/1471-2288-11-100

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology : A Comparison of Two Theoretical Models Authors (s): Fred D . Davis , Richard P . Bagozzi and Paul R . Warshaw Published by : INFORMS Stable URL : http://www.jstor.org/stable/2632151 REFERENCES Linked references a. *Management Science*, *35*(8), 982–1003.

Deepshikha Aggarwal. (2018). Using the Technology Acceptance Model to

Understand the Use of Bring Your Own Device (BYOD) to Classroom. *Journal on Today's Ideas - Tomorrow's Technologies*, *6*(2), 83–91. https://doi.org/10.15415/jotitt.2018.62007

Dell. (2015). *Mobility Meets Reality*. 34.

Dery, K., Sebastian, I. M., Van Der Meulen, N., & Meulen, N. van der. (2017). Succeeding in the Digital Economy Requires New Ways of Working1. *MIS Quarterly Executive*, *16*(135), 135–152. http://www.misqe.org/ojs2/index.php/misqe/article/viewFile/767/460

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, *9*, 43–53. https://doi.org/10.1016/j.protcy.2013.12.005

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., & Saad, E. H. M. (2015). BYOD: Current state and security challenges. *ISCAIE 2014 - 2014 IEEE Symposium on Computer Applications and Industrial Electronics*, 189–192. https://doi.org/10.1109/ISCAIE.2014.7010235

EY. (2013). *Security and risk considerations for your*. *September*.

Fani, N., Von Solms, R., & Gerber, M. (2016). A framework towards governing "Bring Your Own Device in SMMEs." *2016 Information Security for South Africa - Proceedings of the 2016 ISSA Conference*, 1–8. https://doi.org/10.1109/ISSA.2016.7802922

Farrugia, B. (2019). WASP (write a scientific paper): Sampling in qualitative research. *Early Human Development*, *133*, 69–71. https://doi.org/10.1016/j.earlhumdev.2019.03.016

Fielding, J. (2020). The people problem: how cyber security's weakest link can become a formidable asset. *Computer Fraud and Security*, *2020*(1), 6–9. https://doi.org/10.1016/S1361-3723(20)30006-3

French, A. M., Guo, C. J., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, *35*(December), 191–197. https://doi.org/10.17705/1cais.03510

Frost & Sullivan. (2016). *The Smartphone Productivity Effect : Quantifying the Productivity Gains of Smartphones in the Enterprise*. 1–19. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/the-smartphone-productivity-effect/20170727/WP_Smartphone_Productivity_AUG16FS_2.pdf?CampaignCode=https-www-samsung-com-us-business-short-form-the-smartphone-productivity-effect-thank-you-f

Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud and Security*, *2020*(8), 6–12. https://doi.org/10.1016/S1361-3723(20)30084-1

Gajar, P. K., Ghosh, A., & Rai, S. (2013). Available Online at www.jgrcs.info BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING. *Journal of Global Research in Computer Science RESEARCH PAPER Available Online at Www.Jgrcs.Info BRING*, *4*(4), 62–70.

Garba, A. B., Armarego, J., & Murray, D. (2015). A policy-based framework for managing information security and privacy risks in BYOD environments. *International Journal of Emerging Trends & Technology in Computer Science*, *4*(2), 189–198. https://pdfs.semanticscholar.org/2046/b937854ba4826d63e769378a95dfbfa447f4.pdf

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, *8*(4). https://nsuworks.nova.edu/tqr/vol8/iss4/6

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). It consumerization and the transformation of it governance. *MIS Quarterly: Management Information Systems*, *42*(4), 1225–1253. https://doi.org/10.25300/MISQ/2018/13703

Haffke, I., Kalgovas, B., & Benlian, A. (2016). The Role of the CIO and the CDO in an Organization's Digital Transformation. *ICIS 2016 Proceedings*. https://aisel.aisnet.org/icis2016/ISStrategy/Presentations/3

Hanelt, A., Piccinini, E., Gregory, R. W., Hildebrandt, B., & Lutz, M. (2015). Digital Transformation of Primarily Physical Industries – Exploring the Impact of Digital Trends on Business Models of Automobile Manufacturers. *12th International Conference on Wirtschaftsinformatik*, *April 2016*, 1313–1327.

Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive*, *11*, 99–112.

Harris, M., & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, *22*. https://doi.org/10.1108/IMCS-03-2013-0019

Harsch, J. (2019). *Key to BYOD isn't multiple devices, but single user experience | Network World*. Network World. https://www.networkworld.com/article/2161558/key-to-byod-isn-t-multiple-devices--but-single-user-experience.html

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. In *Cyberpsychology* (Vol. 10, Issue 4). Masaryk University. https://doi.org/10.5817/CP2016-4-7

ITU. (2021). *The ICT Development Index (IDI): conceptual framework and methodology*. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx

Jahanbakhsh, M., Amini-Rarani, M., Tahmasebian, S., & Shahbazi, M. (2020). Policymaking for Applying the Approach of Bring Your Own Device in COVID-19 Pandemic: A Perspective. *Health Information Management*, *17*(2), 87–89. https://doi.org/10.22122/him.v17i2.4121

Johnston, A. C., & Warkentin, M. (2015). *AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK : L EVERAGING THREATS TO THE HUMAN ASSET THROUGH SANCTIONING RHETORIC*. *39*(1), 113–134.

Kabanda, S., & Brown, I. (2014). Bring-Your-Own-Device (BYOD) practices in SMEs in developing countries - The case of Tanzania. *Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014*, *July 2016*.

Kearns, G. (2015). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, *8*(1), 157–167. http://www.nacva.com/jfia

Klötzer, C., Weißenborn, J., & Pflaum, A. (2017). The Evolution of Cyber-Physical Systems as a Driving Force Behind Digital Transformation. *2017 IEEE 19th Conference on Business Informatics (CBI)*, *02*, 5–14. https://doi.org/10.1109/CBI.2017.8

Köffer, S. (2015). Designing the digital workplace of the future – what scholars recommend to practitioners. *ICIS 2015 Proceedings*.

https://aisel.aisnet.org/icis2015/proceedings/PracticeResearch/4

Kramer, A., & Kramer, K. Z. (2020). The potential impact of the Covid-19 pandemic on occupational status, work from home, and occupational mobility. In *Journal of Vocational Behavior* (Vol. 119, p. 103442). Academic Press Inc. https://doi.org/10.1016/j.jvb.2020.103442

Lawrence, L., & Moyo, G. (2006). *Education and social transformation: An Eastern Cape study*. University of Fort Hare Press.

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. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, *3*(August), 2191–2198.

Madzima, K., Moyo, M., & Abdullah, H. (2014, November 7). 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*. https://doi.org/10.1109/ISSA.2014.6950497

Mahat, N., & Ali, N. (2018). Empowering Employees through BYOD: Benefits and Challenges in Malaysian Public Sector. *International Journal of Engineering and Technology(UAE)*, *7*, 643–649. https://doi.org/10.14419/ijet.v7i4.35.23077

Mankins, M. (2017). Great Companies Obsess Over Productivity, Not Efficiency. *Harvard Business Review*, 2–6. https://hbr.org/2017/03/great-companies-obsess-over-productivity-not-efficiency

Mitrovic, Z., Development, M., Veljkovic, I., Whyte, G., & Thompson, K. (2014). *Introducing BYOD in an organisation : the risk and customer services viewpoints*. *November*.

Molla, A., & Licker, Paul, S. (2005). ECommerce adoption in developing countries: A model and instrument. *Information and Management*, *42*(6), 877–899. https://doi.org/10.1016/j.im.2004.09.002

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9–18.

Mzekandaba, S. (2020). *SA's smartphone penetration surpasses 90% | ITWeb*. https://www.itweb.co.za/content/xA9PO7NZRad7o4J8

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization – A Theory and Practice Review. *AMCIS 2012 Proceedings*. https://aisel.aisnet.org/amcis2012/proceedings/EndUserIS/18

Okwonkwo, C. (2019). *An investigation on the adoption and diffusion of mobile applications in Africa CW Okonkwo Promoter : July*.

Ophoff, J., & Miller, S. (2019). Business Priorities Driving BYOD Adoption: A Case Study of a South African Financial Services Organization. *Issues in Informing Science and Information Technology*, *16*(3123), 165–196. https://doi.org/10.28945/4303

Ortbach, K., Brockmann, T., & Stieglitz, S. (2014). DRIVERS FOR THE ADOPTION OF MOBILE DEVICE MANAGEMENT IN ORGANIZATIONS. *ECIS 2014 Proceedings*. https://aisel.aisnet.org/ecis2014/proceedings/track16/10

Osterman Research. (2012). *Putting IT back in control of BYOD*. *June*, 1–10.

Pani, A. K., Choudhary, P. K., Routray, S., & Pani, M. R. (2020). Effects of MDM Adoption on Employee in the Context of Consumerization of IT. *IFIP Advances in Information and Communication Technology*, *618*, 59–69. https://doi.org/10.1007/978-3-030-64861-9_6

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. https://books.google.co.za/books?hl=en&lr=&id=ovAkBQAAQBAJ&oi=fnd&pg=PP1&dq=Patton,+M.+(2015)+Qualitative+Research+and+Evaluation+Methods.+4th+Edition,+Sage+Publications,+Thousand+Oaks&ots=ZRWV3qBFC-&sig=vpykjOApdm3ckYXklobnMTRZ5sw#v=onepage&q=Patton%2CM

Pillay, a, Nham, E., Tan, G., & Diaki, H. (2013). Does BYOD increase risks or drive benefits? *Dtl.Unimelb.Edu.Au*, *2013*, 1–8.

Prashant Kumar Gajar, 2*Arnab Ghosh and 3Shashikant Rai. (n.d.). *BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES*. Open Access Journals. Retrieved September 8, 2020, from http://www.rroij.com/open-access/bring-your-own-device-byod-security-risks-and-mitigating-strategies-62-70.php?aid=38224

Privacy Rights and Clearinghouse. (2014). *BYOD . . . at Your Own Risk*. Privacy Rights Clearinghouse. https://privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk

Retnowardhani, A., Diputra, R. H., & Triana, Y. S. (2019). Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(2), 753–762. https://doi.org/10.12928/TELKOMNIKA.v17i2.10165

Rosnah, A. A., & Anang, Y. (2018). A proposal of system for device capability assessment in bring your own device (BYOD) environment of computer assisted personal interviewing. *Communications in Science and Technology*, *3*(2), 71–76. https://doi.org/10.21924/cst.3.2.2018.91

Government Gazette, 657 Government Gazette 12 (2020).

Sanou;, B., & ITU. (2017). *Measuring the Information Soceity Report 2017* (Vol. 1).

Scarfone, K., Greene, J., & Souppaya, M. (2020). *Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions*. https://csrc.nist.gov/publications/detail/itl-bulletin/2020/03/security-for-enterprise-telework-remote-access-and-byod/final

Scott, B., Mason, R., & Szewczyk, P. (2021). A snapshot analysis of publicly available BYOD policies. *ACM International Conference Proceeding Series*, 1–6. https://doi.org/10.1145/3437378.3437394

Scott, D., & Morrison, M. (2006). *Key ideas in educational research*. Continuum. https://books.google.co.za/books?id=VsGvAwAAQBAJ&dq=Scott,+D.+and+Morrison,+M.+(2005).+Key+ideas+in+educational+research.&lr=&source=gbs_navlinks_s

Sobikwa, D., & Ditsa, G. (2017). The Usage of Gauteng Online Schools Systems for Basic Education in Soweto. *Journal of IT and Economic Development*, *8*(81), 1–24. https://search.proquest.com/docview/1935242485/fulltextPDF/CA231BEBD3A9464FPQ/1?accountid=188233

Toperesu, B. A., & Van Belle, J. P. (2017). Organisational capabilities required for enabling employee mobility through bring-your-own-device concept.

Business Systems Research, *8*(1), 17–29. https://doi.org/10.1515/bsrj-2017-0002

Transnet. (2019). *Transnet Divisions*. https://www.transnet.net/Divisions/Pages/DivisionsHome.aspx

Watson, B. (2020). Coronavirus and homeworking in the UK labour market - Office for National Statistics. *Office for National Statistics*, 1–15. https://webarchive.nationalarchives.gov.uk/20200401201938/https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/coronavirusandhomeworkingintheuklabourmarket/2019%0Ahttps://www.ons.gov.uk/employmentandlabourmarke

Wigginton, C., Curran, M., & Brodeur, C. (2017). Deloitte: Global mobile consumer trends. *Deloitte*, 2–20. https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/gx-global-mobile-consumer-trends.html

Yang, T. A., Vlas, R., Yang, A., & Vlas, C. (2013). Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior. *Proceedings - SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013*, 411–416. https://doi.org/10.1109/SocialCom.2013.64

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security

engineering: A framework and its analysis. *Computers and Security*, *55*, 81–99. https://doi.org/10.1016/j.cose.2015.06.011

Zheng, P., & Ni, L. (2005). *Smart Phone and Next Generation Mobile Computing (Morgan Kaufmann Series in Networking (Paperback))*. http://dl.acm.org/citation.cfm?id=1200923

APPENDIX A - Instrument

BYOD Research Instrument

ORGANISATIONAL

What organisational factors would you say influenced Transnet to adopt BYOD? (Factors could berelated to privacy, security, infrastructure, policies, cost, training /education, ICT expertise, top management support etc.).

1. Do you know about the BYOD programme in Transnet?
2. Are you aware of the Transnet provisions (policy, strategy) as regards the use of your mobile device for work-related activities
3. Are you aware of any training in your organisational division in relation to using your personal device for work purposes (i.e. training in cyber-security)
4. Are there any benefits you can ascribe to the ability to use own device for work
5. Do you think this may result in threats to Transnet?
6. What is your preferred method of collaboration and communication with other employees, or direct reports and/or peers?
7. Would you say the use of mobile devices for work purposes has brought about any changes to the work environment?
8. What changes?
9. Does you work require you to undertake any work after official work hours (e.g. responding to emails after work)?

10. In your view what is the adoption model for BYOD in Transnet? Is it led by the organisation or users?

Management Support

11. Does IT management provide support for the adoption of the BYOD?
12. How does management provide support when it comes to BYOD?
13. - Could be related to business resources (finance), human resources, technological readiness, governance (BYOD policy). Finance: when your device gets damaged who pays? Reimbursement for data and call charges. Human resources: The right IT staff.
14. Have you attended any training in regard to BYOD?
15. Was this offered by Transnet?
16. Does Transnet have clear objectives and a clear image of how BYOD can help in achieving organisational goals?
17. Comparing the implementation of BYOD with other IT programmes, what is your rating for BYOD adoption in Transnet?
18. In your view what is the management commitment to the adoption of BYOD in Transnet?

Human Resources

19. In your view, does Transnet have the capability (skills and know-how) to implement and maintain BYOD?
20. Who should be the sponsor for BYOD? Why?
21. Do you know who determines the roadmap for the implementation of BYOD in the organisation, training, policy?
22. What or who informs these activities?
23. In your view, is this the right person to undertake this role?
24. In your view, is the level of BYOD adoption in Transnet related to the availability of human resources? Why?
25. Has there been any policy updates to regulate and manage BYOD use in your organisation? Which policy?

Business Resources

26. Is there a specific budget available to finance BYOD?
27. In your view, what role and influence should the non-technical business resources have in the implementation of BYOD in the organisation?
28. Has there been any non-technical resource allocated to BYOD adoption?
29. How have business resources influenced the adoption of BYOD in the organisation? (budget, trust, collaboration, communication, policy etc.)

Technological Readiness

30. Are you provided with internet/network-capable computer for work?
31. Have you configured an MDM (mobile device management) solution on your device?
32. How easy was it to connect your mobile device to the organisational systems?
33. In your view, how encouraging or not is the technological readiness of IT towards supporting BYOD?

Policy /Governance

34. Does Transnet have an IT policy governing mobile devices in the environment?
35. does the policy allow or prohibit BYOD?
36. Does Transnet have a policy for BYOD?
37. Is there consequences for not complying with the BYOD policy?
38. Does Transnet have any business or organisational process that encourages or leverages the use of the BYOD (e.g. sales, field work)?
39. Has there been any data breaches as a result of BYOD?
40. What do you suggest should be done to prevent them from recurring?
41. Has the policy been updated recently to manage the risks of BYOD?
42. In your view, do current policy frameworks encourage the adoption of BYOD? How?
43. In your view, do current policies enable a new way of work? How?

SECTION 4: CONCLUSION

Are there any questions you would like to ask? Thank you very much for your time.

Appendix B – WITS Ethics Clearance

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

SCHOOL OF GRADUATE SCHOOL OF BUSINESS ADMINISTRATION ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: WBS/BA890874/764**

PROJECT TITLE	Critical success factors for the implementation of BYOD: A case study for Transnet
INVESTIGATOR	Mr Elliot Mokoena
SCHOOL/DEPARTMENT OF INVESTIGATOR	MM (Digital Business)
DATE CONSIDERED	16 November 2020
DECISION OF THE COMMITTEE	Approved unconditionally
RISK LEVEL	MINIMAL RISK
EXPIRY DATE	30 JUNE 2021

ISSUE DATE OF CERTIFICATE 25 November 2020 **CHAIRPERSON** __ _____
(Dr MDJ Matshabaphala)

Matshabaphala

cc: Supervisor: Doctor Pellissier

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ _____/_____/_____
Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

Appendix C – Transnet Clearance

19 January 2021
138 Plover Street
Pinehaven Country Estate
Pinehaven
1739

elliot.mokoena@transnet.net

Dear Mr Elliot Mokoena

Re: Request for permission to conduct research at Transnet SOC Ltd

Your email of request for permission to conduct research at Transnet on "BYOD in a selected state-owned enterprise" is acknowledged.

We duly note the conditions of the study for strict academic purposes, the results of the study will be submitted to Transnet, and the research will be confidential and that anonymity for both respondents and the organisation is guaranteed. Should you or the University of Witwatersrand want to publish the study in any other manner than the final assignment, Transnet will be approached for permission to do so.

Based on the above conditions, your request to conduct the research study in Transnet is granted. We are looking forward to the outcomes and recommendations of your study and the positive contributions towards the marketing strategy of Transnet.

Yours sincerely,

LRadebe

Ms Lerato Radebe
General Manager: People Management
Date: 19/01/2021

Appendix D – Participant Form

Dear Participant;

Hope this message finds you well.

I am a student at Wits University, pursuing a qualification in Masters in Digital Business.

The title of my research is "**An implementation framework for BYOD in a selected state-owned enterprise** " and the target is fifteen (15) ICT practitioners in Transnet.

Primary Objective:
The primary objective of this research project is to provide a framework of risks and benefits for the adoption of BYOD for end-user computing at Transnet in support of employee mobility in an increasingly complex, yet virtual, environment.

Secondary objectives
Two secondary objectives are proposed in order to achieve the primary objective:

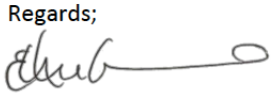
1. To explore the impact of BYOD on Transnet employee productivity
2. To explore the risks inherent in deploying BYOD at Transnet

I estimate the time required will be 45 minutes to conclude the online questionnaire. The link is https://forms.office.com/Pages/ResponsePage.aspx?id=lpmjoRP5FkClijYcYN7FgDuyRCy1Z95PhvXPfhPlOwRUQjNWRUFHRkRLWkw2OFpMQk9NWURaS1EyQS4u

Find attached hereto the ethical clearance from Wits University Ethics Committee and from the Transnet HR Department, as well as sample questions/instrument to be used during the semi-structured interviews.

Due to Covid-19, physical consent will not be sought, your completion of this online questionnaire will be used as your consent to the study as per the attached consent letter.

Regards;



Elliot Mokoena
Std# 890874
Wits Business School