Security awareness and training policy guidelines to minimise the risks of BYOD in a South African SME

ME Kholoanyane

orcid.org/0000-0002-8240-2454

Dissertation accepted in partial fulfilment of the requirements for the degree *Master of Science in Computer Science* at the North-West University

Supervisor: Prof DB Jordaan

Graduation: May 2020

Student number: 28066103

Acknowledgements

To my amazing supervisor, Prof JB Jordaan, thanks for your constant feedback, critical comments and brilliant suggestions, they made a huge impact on my work. Without your guidance, accurate feedback and insights, I would not have been able to produce this report. Thank you to everyone who contribute to this study. To the field experts, thank you for taking your time to partake in the interviews, sharing your knowledge and feedback. To the SMEs employees who were willing to share their insights and experience, without the useful insights derived from the interviews and surveys, I would not have been able to complete this research. Lastly, to my family and friends, thank you for your support.

Abstract

Concepts like Bring Your Own Device (BYOD) are not new to organisations. Information technology within organisations is getting more diverse. In line with the latest technology trends and forecasts, mobile device ownership is growing at an exponential rate, with users becoming more and more tech-savvy. This has a huge effect in the workplace, where employees now choose to use their own devices (known as bring your own device/BYOD) instead of company phones and laptops. For most organisations, BYOD is arguably very positive, and its benefits and challenges are well documented in the literature. However, like any other technology trend, BYOD has a dark side. From the South African Small and Medium Enterprises (SMEs) context, there is a concern, especially where BYOD is used to address the lack of technological resources in an organisation. The purpose of this research is to investigate the training and security awareness aspect of BYOD. The research will provide comprehensive literature regarding the challenges of BYOD and security awareness and training, highlight the most important elements that need to be included in the BYOD awareness and training policy to minimise the security risks. The aim is to help SMEs in South Africa, by providing a policy guideline and putting together awareness and training policy for organisations in this sector.

An in-depth literature review was carried out to evaluate the extent of coverage for this topic and motivation for the research. To uncover the security awareness, policy elements and challenges, interviews and surveys were conducted to identify relevant questions for online questionnaires. From the academic side, recent literature has started to examine different aspects of BYOD, including awareness. Although there is very limited coverage on this topic for SMEs and, therefore, arguably not effective for measuring the effectiveness of the policy elements, this study took a highly exploratory design, seeking to fill these gaps by exploring how a training and awareness policy can be utilised to educate and create awareness of BYOD security risks and subsequently minimise the risks in SMEs. The findings of the interviews and questionnaires were cross-referenced with the literature to identify the most relevant awareness and training elements that can be used as a guideline to tackle challenges of BYOD awareness and training policies.

Key Words: Small and Medium Enterprises (SMEs), Bring Your Own Device (BYOD), Security awareness and training policy, Information Technology (IT)

Table of Contents

List of figures

List of Tables

Chapter 1 - Introduction

1.1 Introduction

The field of mobile computing is becoming predominant due to the increasing number of smartphone users (Johnson & Maltz, 1996). However, for organisations, mobile devices have long become an integral part of business activities. As a result, organisations are faced with pressure to allow employees to use their personal mobile devices like smartphones and laptops for work purposes. This trend is called Bring Your Own Device (BYOD) (Ellis *et al.*, 2012). Additionally, with the use of mobile devices, employees can stay connected to the internet and work from anywhere.

The risks of mobile devices are also becoming a concern for most organisations (Eschelbeck & Schwartzberg, 2013). Data breaches have become very common and cost organisations a lot of money. According to a report published by Ponemon (2018b), organisations in South Africa have the highest probability of experiencing a data breach, at 43%, with a total average cost of $2.90 million. This is something to be seriously worried about. According to Thomson (2012), BYOD and the use of mobile devices in the workplace contribute to the growing IT security risks and threats.

A study conducted by Accenture (2018) in South Africa shows that IT security is a top priority for every organisation. BYOD poses new security challenges for the organisation, like prime issues of data security. This stands out as a major problem because BYOD takes control away from the organisation and gives it to the user (Ellis *et al.*, 2012). The challenges of data security, malware and compliance are the results of lack of awareness and knowledge from the employees' side because, as the mantra goes, "if you know better, you do better" (Harris *et al.*, 2013; Thomson & von Solms, 1998). Peltier (2005) argues that, with awareness and training policies, organisations might be able to change the way people think and, ultimately, the way they act. Subsequently, this might help to minimise the risks of data breaches.

D'Arcy *et al.* (2009) emphasise that user awareness and training on security risks and threats have a direct impact on organisational security risks. They say the lack of emphasis on user awareness and training is likely to create a discrepancy between managers' awareness and training of security policies and users' awareness of the same policies.

According to Leavitt (2013), new security challenges require a new approach. Many studies (Chen *et al.*, 2013; Thomson & von Solms, 1998) indicate that BYOD risks require new security strategies, which include coming up with security awareness and training policies for users, which will also help to create awareness of the risks and threats of BYOD. In their study, McCoy and Fowler (2004) and Peltier (2005) agree that new security strategies are needed where employees are more involved and informed of the risks and threats of BYOD and the awareness and training policies are more relevant to the changing world. Harris *et al.* (2013) reports that new security challenges demand a well-informed end user, who will be able to make the right decision to protect the organisation's data and this can be achieved by having effective awareness and training policies.

1.2 Background

In South Africa, Small Medium Enterprises (SMEs) are known as a key contributor to economic development. With South African youth and government currently facing a huge problem of unemployment and poverty, a study conducted indicates that SMEs have a positive impact in society and contribute to South African economy through jobs creation (Seed-Academy, 2017). SMEs in south Africa, not only contribute to job creation but also create opportunities for the unskilled workforce, contributing to skill development in general (Neneh, 2014).

According to (SME-South-Africa, 2019) some of the perennial challenges that SMEs in South Africa face is access to funding, business support and skill development. Recent studies also point out that most SMEs are forced to look for opportunities for alternative funding (Sage, 2017). More than fifty percent of SME owners indicated that they started their business either from sourcing funds from family members or friends, only a few receive funding from government, while receiving funding from financial institution is also a challenge for most SMEs. The reasons for being refused funding include insufficient operating history, inadequate cash flow and limited collateral, to support what financing is supposed to do for business and implementing a system that can help generate more money. This is in support of current literature on small businesses which states that most SMEs are self-funded (Neneh, 2014).

Due to lack of jobs and employment opportunities, South African government acknowledges the significant role that SMEs play in the economic development and

job creation and often assist by creating government initiatives that addresses finance related issues in SMES and ease of access to information, to encourage entrepreneurship and assist SMEs to be successful. Over and above the funding challenges that SMEs face, the success rate of SMEs in South Africa is one of the lowest when compared to other countries (Nene & van Zyl, 2012; Neneh, 2014). The challenge is moving from the infant stage to the maturity stage where the business is established and generating revenue. It is reported that most new SMEs don't make it past 5 year mark and this can be due to many reasons such as qualities possessed by the businesses and the manner in which they are managed (Neneh, 2011).

As part of identifying opportunities, majority of SMEs owners say they use their smartphones in their businesses (Adclick, 2019). Most companies are constantly seeking ways to improve how they conduct business by adopting new technological trends and BYOD sounds like a bargain (Rose, 2013). Organisations that have implemented BYOD, with the hope to reduce the cost of hardware and maintenance, are facing serious security risks and threats (Bell, 2013). Previous studies show that IT security teams face challenges of implementing strategies that prevent data breaches caused by lost and stolen devices, malware and phishing from mobile devices due to lack of awareness and training for BYOD users (Shumate & Ketel, 2014; Khanna, 2014).

For successful adoption of BYOD, it is important for organisations to have strategical plans, follow best practices and invest in their employees in terms of training and awareness, in order to inform employees of the risks and threats of BYOD. This puts the organisation in a better position to describe the necessary actions and requirements for users to receive contextualised security training that relates to the scopes of their duties and responsibilities. For an IT team, these policies will serve as guidance when creating programmes and user instructions on how to adhere to the policies so as to maximise the benefits of BYOD and minimise security threats (Absalom, 2012; Armando *et al.*, 2013; Bennett & Tucker, 2012).

With BYOD, organisations do not manage the mobile devices; BYOD users do. BYOD users are responsible for ensuring that they do not expose their devices to malicious attacks which may result in data breaches and putting in place the right security measures for the safety of the device and the corporate data on the device itself (Ellis

et al., 2012). This shows the need to put enough effort into the user awareness and training plans in the implementation of this concept (Downer & Bhattacharya, 2015). It is crucial for an organisation to create training and awareness policies to educate the BYOD users and inform them of its risks and threats, in order to ensure user readiness and understanding of security best practices (Harris *et al.*, 2013).

According to research conducted by Shumate and Ketel (2014), the business decision to adopt the BYOD strategies is mainly driven by pressure from employees and hardware cost savings. However, the gap between the cost-saving through BYOD strategies is not proportionally linked to the costs that will be incurred if the adoption is unsuccessful due to data breaches.

According to Leclercq-Vandelannoitte (2015), the success of BYOD depends heavily on three things: the technology, the organisations and the user. Technology refers to having the right security architecture in place for threat intelligence, prevention, and protection. Organisation refers to the organisation's value of asset and its readiness in terms of policies and enforcing compliance. The term user refers to an employee's rights and responsibilities as an individual, which creates a collective co-dependency to make BYOD adoptions a success. Because new vulnerabilities, risks, and hacks arise on a regular basis, new technological developments require continuous updating of security awareness and training policies.

1.3 Research rationale and relevance

The motivation for investigating this problem can be separated into theoretical and practical relevance.

1.3.1 Theoretical relevance

Detailed research can be found on the use of BYOD in organisations (Mitrovic *et al.*, 2014). These are often investigative studies that discuss the benefits, advantages, disadvantages, and the risks of BYOD (Singh, 2012a). However, not much literature can be found on the training and awareness policies for BYOD, and the few existing studies focus mainly on countries and organisations which are not comparable to South Africa and SMEs. The lack of research in BYOD training and awareness in SMEs is to be expected, keeping in mind that BYOD is mostly formally adopted by big organisations and therefore lots of research focus has been around large corporates. There is also a gap in the academic literature on how BYOD training and awareness

can be used to address the security risks of BYOD in the SMEs (Harris *et al.*, 2013). Studies that have been conducted around this topic mostly focus on the available technologies that can be used to combat the risks of BYOD, but do not discuss the human element and how awareness training can minimise the risks (Peng *et al.*, 2013).

On a similar note, research regarding the policy guidelines of BYOD awareness training is also limited to different industries and the sensitivity and confidentiality of data (Akin-Adetoro & Kabanda, 2015a; Dingwayo & Kabanda, 2017b). In contrast to big organisations, SMEs have a distinctively different business environment and model and therefore; different requirements to which BYOD training and awareness policy should be tailored (Njiva, 2015). Hence this study seeks to fill these gaps by exploring how awareness training policy guidelines can be utilised to help SMEs create awareness training policies and subsequently minimise the BYOD security risks.

1.3.2 Practical relevance

According to Harris and Patten (2014), if done correctly, BYOD could be the best thing for SMEs. BYOD could save them the cost of procuring and managing company-owned devices. This type of enterprise, more than others, should be leveraging BYOD more effectively and efficiently (Kabanda & Brown, 2014b). Previous research shows that complexity is one of the biggest challenges for most organisations (Harris *et al.*, 2012). For SMEs, managing BYOD is much more complex since most of them do not have IT security and risk teams or leaders, which amplifies the difficulty of managing the security risks. Although the CIOs of SMEs have diverse security technologies to choose from in order to protect their organisations from the BYOD risks, most of these technologies are way too expensive and difficult to deploy or manage. This study has a practical nature since its recommendations should be implementable in SMEs so as to improve their use of BYOD through educating employees about the possible security risks thereof. In the long-term, awareness training minimises security risks like data breaches and malware.

1.4 Problem statement

Organisations face challenges on training and awareness policies for BYOD, informing the employees about the risks and threats of BYOD and helping them understand and adhere to security practices in the best possible way. The problem is that while

organisations have implemented BYOD and developed IT teams to retain access control and protect corporate data through technologies, most organisations tend to overlook or pay little attention to the security awareness and training for BYOD users, assuming that the user is well informed about the risks and threats of BYOD. In most cases, BYOD users bypass many security protocols because they are unaware of the risks and threats of not doing the right things, and to them BYOD is just another “cool” trend (Twinomurinzi & Mawela, 2014).

Research shows that organisations that have implemented BYOD are struggling with user awareness and training in terms of the security aspects of BYOD (Yang *et al.*, 2013). This is due to a lack of security awareness and training for employees (Hovav & Putri, 2016). The problem is amplified by lack of development of meaningful security awareness and training programmes that explain areas of caution, and identify appropriate security policies and procedures that need to be followed, as well as discuss any sanctions that might be imposed due to lack of compliance (Crossler *et al.*, 2014; Furnell *et al.*, 2002; D'Arcy *et al.*, 2009). Although it seems that organisations have the right security measures in place to prevent any data loss, they still face challenges with developing policies that are focused on security awareness and training to inform users and make them aware of the actions they can take to keep information safe and use the appropriate channels to report suspected incidents or violations. Most organisations claim that employees often lose interest and quickly develop a negative mind-set towards security (Weeger & Gewald, 2014; Hovav & Putri, 2016).

The development and details of BYOD training and awareness policies should be aligned to its purpose. There is a need to establish what is, or ought to be, and the purpose of the policies, such that BYOD serves the interests of those who must benefit from it. Different organisations and stakeholders may have different viewpoints of what should be included in this policy document, or what counts and what should not count, as relevant knowledge. For this reason, it is very difficult for organisations to come up with training and awareness policies that address security issues when expectations are not known.

The problem that this study aims to address is that there is a lack of guidance for organisations to develop BYOD training and awareness policies that truly address and

help them to inform and educate the users of the security threats of BYOD. There is a greater need for organisations to know what to include in the policies and be abreast with the processes and steps to follow to improve these policies.

The research question is:

How can SMEs reduce security risks in their organisations using training and awareness policies?

The research question is further broken down into four sub-questions, which are listed below**:**

1. What risks are SMEs facing in their organisation?
2. What human-factor related risks are contributing to BYOD security risks?
3. What measures are currently being implemented and to what extent are they effective?
4. What are the key elements used to formulate a solid training and awareness policy for SMEs?

1.5 Objectives of the study

The following objectives were formulated for the study:

1.5.1 Primary objectives

The main objective of this research is to develop guidelines for security awareness and training policy to minimise the security risks of BYOD strategies. To achieve the primary objective, the following theoretical and empirical objectives are formulated for the study:

1.5.2 Secondary objectives

In accordance with the primary objectives, the following theoretical objectives have been formulated:

1.5.2.1 Theoretical objectives

The following theoretical objectives are derived:

1.1. Demonstrate an understanding of BYOD training and awareness elements within the organisation.

1.2. Identify the challenges of developing BYOD training and security policies.

1.5.2.2 Empirical objectives

The following empirical objectives are derived:

1. Investigate policies that organisations currently have by collecting and analysing the document data from these organisations.
2. Investigate the perspectives of stakeholders, using interpretive research, as well as understand the needs of the stakeholders in terms of BYOD training and awareness policies and the process of designing these policies. The stakeholders will at least include industry IT security experts and employees, who are the BYOD end users.
3. Develop guidelines representing the needs of all identified stakeholders. The guidelines should be grounded in the literature review, reflect the organisation's current policies and interview data analysis.
4. Evaluate the effectiveness of the guidelines

1.6 Significance of the study

Research shows that by 2020, 90% of global enterprises would have implemented business processes that depend heavily on mobile devices (Gartner, 2018).This shows the expected growth of BYOD adoptions. The latest survey conducted by Tech Pro in 2014 says that from 2009, there has been an immense growth in the number of companies adopting this concept. Figure 1-1 below, shows that 60% of the organisations that participated in the survey said they have adopted the BYOD concept in their organisations, while 26% said they were planning to roll out the concept.

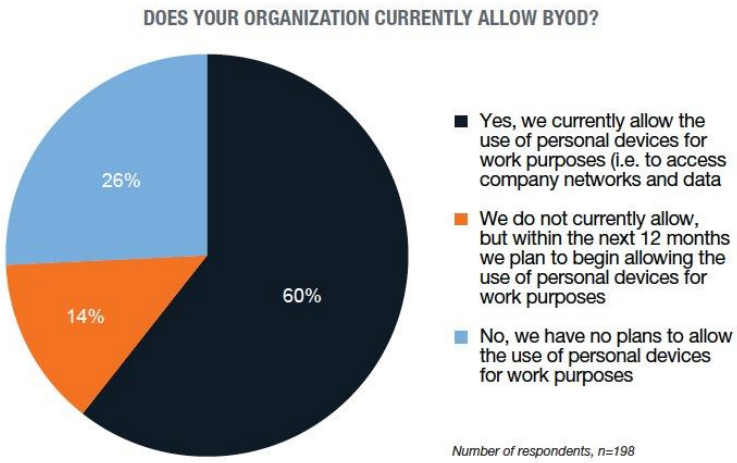


Figure 1-1: BYOD Adoption

Study shows that employee awareness and training about the importance of security is very crucial for the mission of any IT organisation (McCoy & Fowler, 2004). The challenges of data breaches, malware, compliance, and data loss are the results of a lack of knowledge by the employees (Harris *et al.*, 2013; Thomson & von Solms, 1998). Through education and awareness programmes, organisations might be able to change the way people think and ultimately the way they act. This might subsequently mitigates security risks (Peltier, 2005).

Developing awareness and training policies for BYOD to minimise the security risks and threats might be a step in the right direction for organisations. Security awareness ensures that users are familiar with potential threat mechanisms, while training teaches them the strategies they must employ to prevent or respond to these threats (Kruger & Kearney, 2006; McCoy & Fowler, 2004). In their report, Intel (2011) agrees that it is important to have an awareness and training policy. This policy is designed to help the IT staff to guide employees toward understanding and adhering to best security practices that are relevant to their job responsibilities. It is believed that by ensuring employees' understanding of the risks and building accountability for these concepts will enhance information security through behaviour modification. According to Furnell *et al.* (2002), awareness of information security risks is a necessary requirement for any organisation utilising BYOD. In their study, Spears and Barki (2010) argue that an appropriate level of awareness and training may serve as a prerequisite for adequate security protection.

The study will be immensely important for organisations adopting BYOD by providing evidence-based information. The information will include awareness and training policy guidelines for organisations to inform employees of the risk and threats of BYOD. Furthermore, other organisations can use the findings of this research as a foundation for developing awareness and training policies to inform employees of the risk of BYOD and minimise its risks and threats.

The aim of this study is to explore the potential risks of BYOD in SMEs and to propose guidelines to develop awareness and training policies to ensure the effectiveness of this training. This contribution of this research study will be two-fold, that is; it has practical and academic relevance, as it seeks to:

- Provide basic guidelines to develop awareness and training policies, which in return can be used to inform the employees of the risk and challenges of BYOD can then be used to minimise the risks, OR
- Improve knowledge regarding the training and awareness policies of BYOD. In addition, the findings of this study will contribute to the literature in this particular area of BYOD security risks in South African SMEs and maybe be used as a foundation for future studies.

1.7 Thesis outline

The report is organised in the following manner:

Chapter 1: Introduction and Background

Introduces the problem statement, the research questions, the research motivation and the objectives of this research.

Chapter 2: Literature Review

Explores the challenges of security awareness and training policies, defines, and analyses the key elements of BYOD awareness and training policies.

Chapter 3: Research Methodology

Describes the research philosophy, research design and the methods used to conduct the research.

Chapter 4: Results

Presents the findings of the interviews and questionnaires.

Chapter 5: Discussions

Analyses the findings of the study in relation to the literature review, how the findings were analysed, interpreted and discussed.

Chapter 6: Summary and Recommendations

Summarises and concludes the study with regards to the theoretical and empirical objectives and provides recommendations emanating from the study, as well as some proposals for future research.

Chapter 2 - Literature Review

2.1 Introduction

An acronym SME stands for Small and Medium-Sized Enterprise. Often SMEs are acknowledged as one of the important sectors for economic growth and are engines for job creation (Kongolo, 2010). It is estimated that more than 90% of formal entities in South Africa are SMEs, which means they contribute significantly to economic development and employment creation (Abor & Quartey, 2010). With the current economic issues in South Africa, SMEs are an important contributor to economic growth, as they employ most of the national workforce, according to SEDA (2017).

Among some of the known challenges for SMEs in South Africa is lack of management, skilled employees, regulatory compliance and appropriate technology. This makes the timing of this research even more appropriate, especially now when SMEs are expected to drive economic development and job creation, and technology is predicted to be the driver and enabler of business. According to the Department of Trade and Industry (2018), SMEs can be classified into two categories; small and medium enterprises, as differentiated by the number of employees and turnover.

In the SME sector, decisions are made differently in comparison to the large corporate world or central government. The security policies are a foreign concept to most SMEs, especially towards security and technology, including the BYOD (Adedolapo, 2016a).

Before considering the BYOD security training awareness concerns for SMEs, it is necessary to create an understanding of the overall BYOD security concerns that SMEs are facing. The following sections provide in-depth discussions of the BYOD security concerns and provide a background of its human element and evolution from the traditional desktops to mobile devices. This background is crucial to forming an understanding as to why training and awareness are important for BYOD adoption. Lastly, BYOD security training and awareness of current practices and examples of how they are currently implemented within other organisations and SMEs are provided.

2.2 Background

Recent studies on BYOD in South Africa by Dingwayo and Kabanda (2017) and Twinomurinzi and Mawela (2014) show that most large organisations have already

adopted BYOD and small and medium-sized enterprises (SMEs) are increasingly following suit (Adedolapo, 2016; Akin-Adetoro & Kabanda, 2015), mainly because of the known benefits of BYOD. BYOD has different meanings for big organisations and SMEs. The benefits might be the same but for SMEs, BYOD means employees use their own devices to help the organisations to achieve their missions and visions. Given the lack of funds to invest in the infrastructure and technology, the use of employees' personal mobile devices to carry out work activities is important for the survival of the organisation, regardless of whether the mobile networking channels are safe or not (Adedolapo, 2016; Kabanda & Brown, 2014). Akin-Adetoro and Kabanda (2015) emphasise that for big organisations and developed countries, moving from the traditional IT of desktops to mobile devices was pushed by the employees through the influx of mobile devices but for SMEs, it is the other way around. BYOD is a technology solution for SMEs. Other researchers add that increased access to mobile devices is beneficial for SMEs because employees can use new technologies to increase productivity at a lower or no cost to SMEs (Lydon, 2014; Sumaili *et al.*, 2018). This helps the SMEs to save on the cost of purchasing the devices and addresses the issue of lack of investment and budget for in-house technology.

The sensitivity of information stored by SMEs

Cybersecurity is a big issue for small and medium-sized companies. The number of threats continues to worsen. According to Kurpjuhn (2015), SMEs are now using, generating and storing enormous amounts of data, which makes them a far higher target for potential gains from a successful hack or security breach than they were five years ago. Like other organisations, SMEs deal with sensitive and confidential data that might destroy the future of an organisation, if not protected (Grljevic *et al.*, 2011). The type of data includes:

- Internal information
- Customer information
- Confidential sales and business strategy information

Figure 2 below displays the structure of this section, starting with Cyber Security in South Africa, followed by identification of the BYOD security challenges faced by

SMEs. The next subsection discusses BYOD training and awareness practices, followed by BYOD training and awareness policy key elements. Lastly, the need for BYOD policy guidelines will be justified.

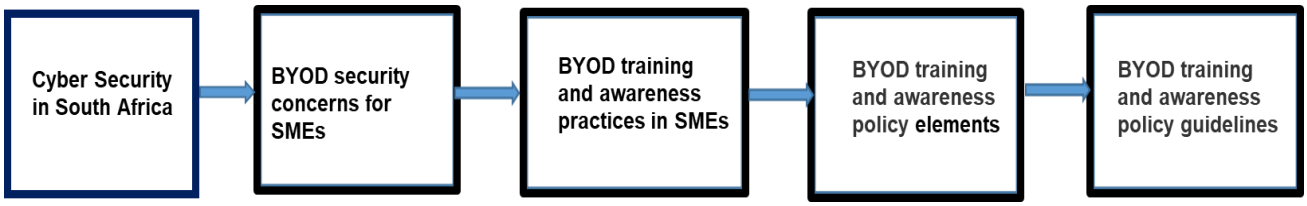


Figure 2-1 The Literature Review Structure

2.3 Cyber Security in South Africa

According to Ponemon (2018b), in 2017 South Africa experienced what was called its "worst data breach" when a file of approximately 30 million citizens' private data was leaked on the internet. This recent study conducted on cybercrime also shows that the average size of breached records has increased to 6.31% and the average cost of a data breach is R36.5 million in South Africa (Ponemon, 2018b). In response to the cybercrimes and global shift towards purposeful handling of personal information, the South African Government, through Department of State Security, enacted the National Cybersecurity Policy Framework (NCPF) in 2015, following the Protection of Personal Information (POPI) Act of 2013. The latter, which primarily governs how people's personal information is collected, retained, used, distributed and deleted, was expected to take effect in 2019 (Bruyn, 2014). The act states that one's information and privacy should be protected at all times. All corporations operating in South Africa need to comply with these regulations and this seems to be a challenge, even for SMEs. The effects of POPI still need to be explored in detail (Botha *et al.*, 2015 & Niekerk, 2017). A study conducted by Kabanda and Brown (2014a) reports that although the implications of POPI on BYOD are not yet known, one still needs to understand how BYOD can safely be adopted while being compliant with the regulations. According to research, not more than 34% of SME organisations seem prepared, 16% of are POPI non-compliant and 56% are not aware of the POPI laws (Swartz & Da Veiga, 2016). This non-compliance can leave the organisation in danger of breaching its employees' data privacy rights and, therefore, open to lawsuits (Absalom, 2012). In their findings, Kabanda and Brown (2014a) also mention the need

for awareness and training on the policies and laws such as POPI and how they affect BYOD. This is another aspect that still needs to be explored.

Cybersecurity is a daunting task for SMEs, which are largely too burdened with skills, budget and other resources constraints to afford solutions that could help protect their information assets, save them time, money and business reputation (Brodin, 2017). Rivera *et al.* (2013) add that, with the growing list of security threats due to BYOD migration, organisations need to assess the efficiency of their training and awareness initiatives. Big organisations normally have governance policies and frameworks to manage the mobile device challenges, but SMEs do not seem to have standard procedures to manage the challenges (Niekerk, 2017).

2.4 BYOD security risks in SMEs

Recent studies about cyber risks show that SMEs are a target for cybercrime (Stewart, 2013) and the user remains the weakest link for security risk (Karr, 2015). In her research, Renaud (2016) mentions that due to their weak defence, SMEs are increasingly being targeted by cyber-criminals. The BYOD security risks are just as harmful for small and medium-sized enterprises (SMEs) as they are for big organisations. In general, SMEs deal with the same levels of risk as larger organisations, but often have considerably fewer resources and lower budgets (Kurpjuhn, 2015). According to Adedolapo (2016b), BYOD adoption is adding on to the existing security risks such as data leakage, malware attack, and network intrusion. Such risks, as recent studies show, are mainly due to lack of organisational control over employees' mobile devices (Scarfo, 2012; Beckett, 2014; Ghosh *et al.*, 2013; Singh, 2012b). It is believed that employees are not always careful with device usage, and this can do a lot of damage to the organisations (Beckett, 2014). Research on this topic also points out that the majority of data breaches (9 out of 10) originate from malicious and cybercrime attacks. Other dangerous threats are; phishing, accessing unsafe websites, downloading software from suspicious websites, using unprotected WI-FI and weak passwords, consequently contributing to the risks of BYOD (Koh *et al.*, 2014; Byol *et al.*, 2014; Ghosh *et al.*, 2013). One of the important elements that should be studied in detail is the human aspect. The human element plays a critical role in BYOD security scenarios and seems like the weakest link (Frumento *et al.*, 2017; Jasek & Sarga, 2014). In their study Bann *et al.* (2015);

Jasek and Sarga (2014) argue that while malware attacks and phishing comprise the most significant challenges for BYOD, the human element is also a major drawback. Pillay *et al.* (2013) concluded their study by saying that in order to continuously reap the BYOD benefits, its risks have to be carefully identified, assessed, monitored and controlled by specifically addressing the importance of the human factor. With this in mind, the human elements identified above as part of the security risks of BYOD, in relation to current South African research, are discussed next.

2.4.1 Data breach

In his research, Romer (2014) mentions that mobile devices brought security vulnerabilities in the workplace, as attackers act very fast in order to exploit design flaws or architectural weaknesses of these gadgets. With BYOD, organisations not only face loss of control over the device but also employee negligence, which can also affect network availability, resulting in data loss (Beckett, 2014). Unauthorised access and installation of malicious applications on employees' devices can cause data leakages(Ali *et al.*, 2015). Things like confidential work emails and files, client information and data on mobile applications can be compromised thus causing huge harm to the business. Due to the costs of data breaches, some major organisations have decided not to change their security protocols and, instead, adopt BYOD because they do not want to risk increased exposure to cyber threats and data breaches (Shim *et al.*, 2013). Astani *et al.* (2013) say the BYOD practice is very complex as it can expose sensitive organisation data to wrong hands. Storing data on mobile devices with fewer controls can even lead to data breaches, as BYOD requires good security programmes at the core foundation of the organisations (Astani *et al*., 2013). According to Kumar and Singh (2015), the latest technologies like WI-FI networks, third-party patches and BYOD have added to the magnitude and frequency of security threats and loopholes that lead to data breaches. In their study Liginlal *et al.* (2009) allude to the human error element of security risks and add that this element is often overlooked as a cause of data breaches incidents.

2.4.2 A lost or stolen device

Garba *et al.* (2015) say the mobile device itself can be stolen or lost. There is a high potential for devices carrying private information to get lost or stolen (Smith & Forman,

2014) therefore giving away a lot of information stored on the device, which can be used against the organisation. Ghosh *et al.* (2013) argue that BYOD poses a great challenge to the security of the mobile device, along with the information on it as the gadget can very easily get lost or stolen due to its extra portability. Miller *et al.* (2012) also agree that bad things can happen to sensitive information that walks out the doors on a daily basis, especially if the device is lost or stolen. In his study, Rose (2013) says losing a device that has thousands of files with confidential information puts the company in a vulnerable position. Tokuyoshi (2013) advocates the practice of having the right measures in place to secure the data, in case such incidents happen. In his study, Ketel and Shumate (2015) and Shumate and Ketel (2014) emphasise the importance of instituting security procedures and best practices to mitigate the inherent security concerns. Other researchers who have covered the response strategies for stolen or lost devices say it is important to have strategies like remote wiping tools to clean out the corporate data on the stolen devices (Dedeche *et al.,* 2013). This solution can be used by the organisation as a countermeasure when the employee loses the device (Chen *et al.*, 2013), but it is a more reactive approach. Creating awareness and training users about the procedures and best practices of security risks can be used to motivate the user to commit to BYOD policies and practices, argue Harris *et al.* (2013).

2.4.3 Stolen identity

If the security concerns of BYOD are not addressed in the workplace, the same mobile devices will be used for cybercrimes to initiate data theft (Stewart, 2013). Identify fraud has been a risk to most companies. In an event where the device is compromised, the usernames and passwords may be easily retrievable on the device. Ademujimi (2013) mentions that cybercrime and data fraud are threats to business, due to the increase in identity fraud, given that most people's accounts get hacked and important corporate information is obtained and used against the company. In his study, Reid (2013) argues that BYOD adoption actually exposes the organisation to unauthorised access to sensitive corporate data and this increases cybersecurity threats. Even if encryption were to be used, the BYOD strategy would still be vulnerable because encryption does not prevent information loss when an employee is reckless (Reid, 2013). Browsing unsafe websites, downloading suspicious software, opening and clicking suspicious

links, using unprotected public Wi-Fi and weak passwords are among the biggest security threats. In particular, research points out that employees are highly vulnerable to phishing. Below, the above-stated risky activities are discussed in detail.

2.4.4 Visiting unsafe websites

Adopting the BYOD concept technically means that organisations allow their employees to store sensitive corporate data on their mobile devices. . Users can also make it easier for internet predators to collect their information by visiting unsafe or malicious websites (Kadena & Kovacs, 2017). Allowing employees to access corporate emails, applications and shared resources from their devices, with no access restrictions to browsing unsafe website, may also invite more security risks for the organisation. It is important for employees to protect their stored data from attackers trying to gain access to their accounts (Ayoade, 2016; de las Cuevas *et al.*, 2015). Predators often use the unsafe websites to collect the users' personal information like passwords, for fraudulent activities when they reveal them (Miller *et al.*, 2012). According to research, organisations expect the employees to use common sense and look for signs for legitimacy, assuming that all the employees are "smart" enough. It is users who are well aware and educated about the security risks who will spend a moment to confirm the URL and properties of a website, but this does not mean that all the users do the same. They could do it if they were well informed. Uninformed users do not pay attention to URL, HTTPS or the lock icon (de las Cuevas *et al.*, 2015).

2.4.5 Using unsecured networks

To some extent, the users' attitudes toward security risks are also worrying (Lennon, 2012). Styles (2013) argues that in most cases, end-users often have a view that security risk is 'someone else's responsibility" not theirs and this is witnessed when they use unsafe networks. Accessing unsafe networks puts an organisation's security at risk and It is this kind of mentality and behaviours that cause an increase in the human-aspect related security risks (Dang *et al.*, 2013). This can result in factors such as loss of business data and corruption of the corporate network. According to Chang *et al.* (2014), security issues can be found at all layers of the device, including the network. Koh e*t al. (2014)* state the importance of having security technologies to

prevent the breach of corporate data from outside. In their study, Koh *et al.* (2014) also stress the importance of investing in technologies that would control user access to the network and validate the employees before they can access the network. Ketel and Shumate (2015) talk about technology solutions like Mobile Device Management and Network Access Control (NAC) to prevent intruders from accessing the corporate network with stolen devices. In their study, Ketel and Shumate (2015) argue that the issue of deciding on which device must have access to which network, companies need to look at possible solutions like NAC, which also provides a mechanism to control the network access from outside. Due to financial limitations, not all the SMEs can afford to implement these products. Because the employees are in control of their mobile devices, SMEs need to explore other means to ensure that data is secure and protected. French *et al (2014)* say organisations must work on how to decide on which network a given device is allowed to log onto. According to Miller *et, al.* (2012) proper planning and decisions should be taken within the organisation to make sure that employees only get access to the information and systems they need to perform their day to day duties and nothing more.

2.4.6 Public Wi-Fi

Another potential threat arises when employees use their mobile devices to access company data from public Wi-Fi. Bell (2013) states that most organisations believe that their existing security is robust enough to protect their network when the employees bring their devices and attach them to the organisation's network. Wi-Fi attackers set up false Wi-Fi access points with deceptive names that make them look legitimate and that way, they gain access to all the information sent between the devices. The attackers aim to get user IDs, passwords and other private information that can later be used for fraudulent activities. Seigneur *et al.* (2013) agree that accessing the corporate data or network from the public Wi-Fi is risky for the company because the mobile device and the location might not be trustworthy, therefore posing data leakage threats to corporate data. With public Wi-Fi available everywhere, most restaurants, coffee shops, hotels, and airports now have free Wi-Fi. This makes our lives a lot easier. In his research, Straw (n.d.) says public Wi-Fi has a list of potential threats like malicious access points, hijacking and sniffing that can intrude the corporate network. Wi-Fi connections are not always dangerous, but some are not

secure. This poses a risk for the data stored on mobile devices. As Mobile devices are always connected, they pick up Wi-Fi access points very easily. Users need to use Wi-Fi with great caution, as not all Wi-Fi networks are secure. Automatic connectivity is one of the features that comes with smartphones and allows seamless connectivity from one Wi-Fi hotspot to another. This is an amazing feature for convenience, but it can also expose devices to unsecured networks that one may not want to use. This feature is similar to Bluetooth connectivity and it poses a huge security threat. Keeping the Wi-Fi feature off allows users to connect to only to secure websites.

Transmitting data over unsecured Wi-Fi opens doors for data modification and theft (Byol *et al.*, 2014; Koh *et al.*, 2014). According to research, most users believe that their data is safe when they use Wi-Fi and do not take the responsibility to ensure that it is safe (Shim *et al.*, 2013). They also think the responsibility to ensure that the Wi-Fi is secure lies with the service provider. It is quite easy to run into a trap of connecting to a fake Wi-Fi access point. Such ignorance is dangerous because unsecured Wi-Fi can be quite dangerous for the organisation (French *et al.*, 2014b). Logging on unsafe Wi-Fi due to lack of due diligence can impose one's device to a number of risks. The attackers gain access to all the information sent to and from the device. This data can be corporate data, media files, presentations, images, intellectual property and emails, including login credentials and passwords. This might cost the organisation millions of Rands and brand reputation.

2.4.7 Opening emails that spread malware

Without a doubt, malware has become a serious threat used by attackers to exploit vulnerabilities (Damopoulos *et al.*, 2014). Kendall and McMillan (2007) define malware as software that is explicitly designed to perform evil and should never be allowed to run on a device used to send emails or perform other work or personal activities. Malware often happens in the form of phishing. Phishing is one of the malicious strategies for cybercriminals because it takes advantage of the weaknesses of the organisation's security. It is quite easy to get a person to click on an emailed link that looks legit than to hack through the system (Bann *et al.*, 2015). Phishing is when the attackers send emails that look like they come from reputable sources or companies known to the user in order to trick users into clicking on the link or opening an attachment (Bann *et al.*, 2015). These kinds of activities often lead to stolen identities,

whereby user credentials will later be used to access organisations' intellectual property or sensitive corporate data.

In her research, Singh (2012b) states that each company that is thinking of implementing BYOD must keep in mind the significant mobile security issues. Some of the applications and software installed on employees' mobile devices might be a danger to the organisations data, just like malware, and it steals data from the devices without the knowledge of the employee (Singh, 2012b). This puts the company in danger of data breaches and leakages. Singh (2012b) concludes that companies must look into these security threats and ensure that there is a solution in place to deal with such before even migrating to BYOD. In addition, Singh (2012b) recommends solutions like Mobile Device Manager (MDM) that can be used to block some suspicious applications.

Human error impacts on organisations' ability to control and secure sensitive corporate data. In his research, Styles (2013) asks a very pertinent question: “Why is it that most computer users feel an overwhelming urge to open suspicious email, access a URL sent to them by an unknown ‘friend’, open the attachment that they were not expecting but which appealed to their curiosity, or to click on a pop-up message telling them to “Update your anti-virus software now!” when they open a web page?”

2.4.8 Using weak passwords

Using a weak password as a type of authentication is also a concern for BYOD risks. Morrow (2012) says the password is an easy mechanism to use as security for mobile devices, but the company needs to put this measure in place before distributing it to the devices of the employees. While people do not normally use a strong password on their smartphones, the password is the only simple and fundamental practice to protect sensitive company data on mobile devices (Vignesh & Asha, 2015). This can also be useful in the event when employee loses the phone with corporate data. Such data can be left on the phone or company applications that run on the mobile device. This poses a huge risk to the organisation if the employee loses the phone (Astani *et al.*, 2013; Singh, 2012). In their study, Singh *et al.* (2014) emphasise that data leakage can be the result of the use of weak passwords or none at all. SMEs must encourage their employees to use strong passwords on the

devices. Astani *et al.*, (2013) argue that enforcing this practice is difficult because, with the BYOD concept, the devices are owned by the employees and not provided by the company, so it is not easy to emphasise how crucial these small things are.

Figure 2-2 categorises and summarises the BYOD security risks, as identified in the pertinent literature related to BYOD security risks in SMEs.

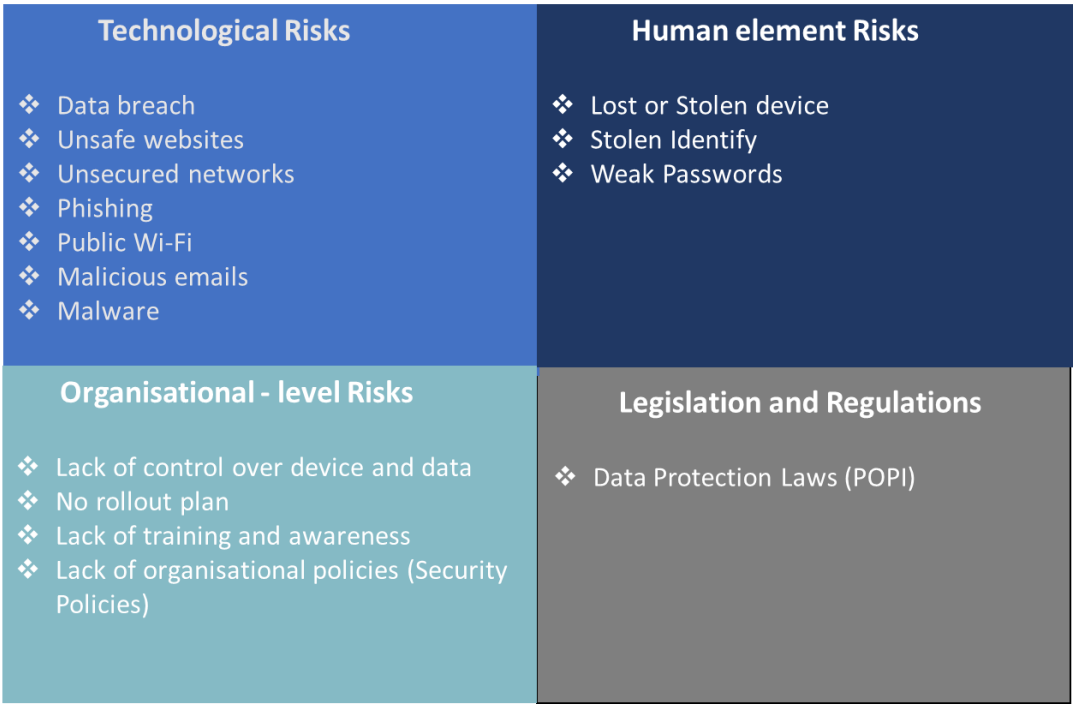


Figure 2-2: A summary of BYOD security challenges
(Downer & Bhattacharya, 2015)

2.5 BYOD training and awareness

Abawajy (2014) and Furnell *et al.* (2002) define awareness as a state of knowing or being mindful about a certain concept. Awareness represents consciousness and understanding of security issues and ways of addressing them (Wilson & Hash, 2003). Thomson (2012) says organisations need to consider other aspects of security, along with the required controls before introducing BYOD in an organisation. Thomson and von Solms (1998) add that for successful BYOD implementation, organisational support and awareness training are required for the entire organisation. Recent studies in security emphasise the significance of human error as a cause of most security risks. Most privacy breaches are results of human error (Liginlal *et al.*, 2009).

It seems as if employees do not understand the importance of corporate data and the significance of keeping their devices safe. Miller *et al.* (2012) advise that ethical values that promote the understanding of data rights and privileges must become part of the educational curriculum to ensure that employees understand the importance of keeping the data they are entrusted with safe. Current research also points out that user actions are the reason why many security attacks are successful, but on the other hand, the most significant part of the current academic literature on this topic seems to ignore the psychological aspects of computer security. Organisations rely heavily on technology to secure their network infrastructure while ignoring the key issue of human vulnerabilities which exist in every organisation. This shows why organisations need to invest in the awareness and training programmes to educate their employees about the security best practices, including identifying unsafe websites, phishing emails, malware and how to protect their login credentials (Katsikas, 2000; Chen *et al.*, 2013; D'Arcy *et al.*, 2009). This will, in return, ensure that the employees do not compromise critical business information because of ignorance (McCoy & Fowler, 2004).

Styles (2013) states that while the security risks are arguably high for SMEs, security is not a key priority for them due to affordability, and this results in a significant lack of security mechanisms, subsequently increasing the risk for this target group. As the attackers continue to expand their threats, accompanying BYOD with an efficient security culture and security-conscious employees will play a key role in protecting organisations (Mitrovic *et al.*, 2014). A study conducted by Putri and Hovav (2014) also shows that security awareness programmes increase an employee´s response efficacy to security risks. According to Sumaili *et al.* (2018), there is a need for SMEs to adopt the culture of training to enable employees to effectively use mobile devices. While most cybercrimes investigations of the data breaches do not mention how the data was leaked, analyses by security risk experts point to phishing emails. Employees are often the weakest link, especially when they do not know how to avoid such incidents (Hovav & Putri, 2016).

As a result of the above, security awareness is becoming an important issue for any organisation adopting BYOD. Security awareness training efforts are designed to change behaviour or reinforce good security practices. It is believed that learning

gradually changes in stages; it starts with awareness, builds to training, and evolves into education (Wilson & Hash, 2003). As the employees become mobile and use more devices over connected networks and access, security-conscious employees have become more important as their risks continue to surge without a slowdown (Harris *et al.*, 2013; Kruger & Kearney, 2006). Non-technical controls like policies and user awareness training are important when creating a supportive framework for BYOD (Rivera *et al.*, 2013). Organisations need to understand their employees better if they are ever going to be in a position to dramatically reduce human-aspect security incidents. It is crucial for organisations to provide awareness and training on BOYD risks as well as highlight the best practices and guidance on how to respond, in case of emergency, to ensure that users are well informed (Thomson & von Solms, 1998).

Educating users on activities like using strong passwords and how to report malicious emails is critical (Peltier, 2005). In their study, Harris *et al.* (2013) highlight the need for mobile device training and awareness, and caution that organisations that only focus on technology and ignore the human element, in particular, the awareness and training of employees, overlook a critical layer of protection. Technologies can offer technical security control, but not a complete solution, as they can never be 100% secure, but so are humans, so the utmost best is to use a combined approach of both human and technical approach (Harris, *et al*., 2013). As it is becoming more difficult to combat the attackers, organisations need to develop inclusive security control, consisting of both technological and humans for an effective solution (Chen *et al.*, 2013).

Abawajy (2014) states that technology and applications are more protected these days and, as a result, attackers have shifted their attention to the human element to break into the organisation's systems. Attackers capitalise on the personnel and the significance of the human factor and fighting cybercrimes cannot be understated, adds Abawajy (2014). For organisations to defend the cyber-attacks designed to exploit human factors, security awareness with an objective to reduce security risks that occur due to human-related vulnerabilities is paramount (Knapp & Ferrante, 2012). McCrohan *et al.* (2010) agree that security awareness training intervention

can have a positive impact on user security behaviour and positive awareness can be more impactful in affirming security behaviours.

2.5.1 Current BYOD training and awareness practices in SMEs

Few studies on this topic suggest that, amongst other things, lack of attention to IT security could be a major issue for SMEs. The other challenges include financial constraints and lack of training and awareness for employees. For the same reasons, SMEs tend to neglect the risk assessment and awareness of security risks, which is also indicative of the organisations' perceptions of BYOD.

Other researchers, notably D'Arcy *et al.* (2009) and Caldwell *et al.* (2012), suggest employee security risk behaviour assessment as part of awareness and training, which they regard as another approach to identify and positively influence user security decisions to counter the threats. Examples of awareness training include, amongst others, security briefings, formal training, regular reminders, ethical codes of conduct as well as the promulgation of organisational policy describing the appropriate use of system resources (D'Arcy *et al.*, 2009; Caldwell *et al.*, 2012). According to Markelj & Bernik (2012), there are technology approaches such as encryption, anti-malware software, firewalls and mobile device management that can be used to guard against security risks like corporate network and mobile devices, but for threats that involve employees, security awareness and training are mandatory. The current security training and awareness practices for employees lack mobile device security (Markelj & Bernik, 2012). Other researchers also highlight the important point that even though training and awareness challenges of BYOD are well documented in policies and guidelines, mobile device security is still largely dependent on the user's motivation and ability to comply. Big organisations believe in investing in advanced technology to protect the corporate networks and forget about the human factor, which is the weakest link targeted by hackers (Romer, 2014). This is not even the case with SMEs, as funding is a big issue and security is not a priority for this type of organisation.

Most research that is pertinent to this topic also points out that employees prioritise work more than security and, in most cases, do not comply with the security

guidelines and procedures (Albrechtsen, 2007). It is believed that this is due to lack of motivation and understanding of security, which are the key factors for training and awareness programmes. Musarurwa *et al.*, (2017) believe that culture also plays an important role in security training and awareness. Romer (2014) adds that due to the short attention span of employees, security and awareness training should be kept as short and simple as possible to ensure that employees are not overwhelmed and bored. Abawajy (2014) also agrees that keeping employees motivated and engaged is just as important for a successful training and awareness programme. Currently, most organisations offer this training in different ways and web-based methods are the most widely used. Although it is still not clear if these methods are effective, researchers argue that there are other methods, like instructor-led training and workshops, which are more effective than web-based training in terms of information retention and practicality (Walsh & Homan, 2012)

Chen *et al.* (2013) encourages combining all methods for better results, effectiveness and to reinforce the message, while Walsh & Homan (2012) argue about relaying the information and retaining it. According to them, some of these methodologies are great for one aspect, but not so great for the other. Albrechtsen and Hovden (2010) state that group training and awareness programmes, where employees are highly involved in discussions, are more effective for short term awareness, whereas information and knowledge shared in workshops remains for longer but is not as effective as instructor-led and web-based training. The latter two strategies seem to result in shorter knowledge retention spans of at least 3 months after the training (Walsh & Homan, 2012).

2.5.2 BYOD training and awareness policy elements

After the literature review, the following were identified as critical elements of BYOD training and awareness policies.

2.5.2.1 BYOD onboarding

Most of the researchers on BYOD believe that it is important to introduce the users to the concept, security and policy guidelines as part of BYOD training and awareness (Chen *et al.*, 2013). This also gives an organisation a chance to set the right expectations with the users and clear any misconceptions, if any. The onboarding

process, if done well, is highly useful for highlighting the risks that BYOD could bring to the organisation. This is the part of the training where the management and IT departments also get an opportunity to highlight the supported devices, operating system, applications and network access. Most BYOD security risks occur due to employee negligence (French *et al.,* 2014a), so it is important to ensure that there is an onboarding process in place to highlight to the users the security risks of BYOD and the consequences of the risks associated with shifting the security responsibility to the employees. This is a crucial part of BYOD security education, training and awareness programmes.

2.5.2.2 User responsibility

User responsibility, in terms of training and awareness, refers to addressing the more technical responsibilities required from the user, and these include logging onto corporate, hotel and public network to receiving software, security and application updates, and passwords. In contrast to the traditional IT system, BYOD adoption leaves the device reasonability in the user's hands. Gessner *et al.* (2013) explain the difference between the two systems by pointing out that in the traditional IT system, where the company provides the hardware, it was easy for a company to make any changes or upgrades on the operating system and force the employees to adhere to the company policies. However, it is a different case with BYOD because the employees own the devices. Rose (2013) says when an organisation adopts BYOD, the IT security competences change drastically because the company does not provide the hardware; hence, it is important to address IT support issues related to BYOD. There are also incompatibility issues that need to be addressed because employees use different phones and OS platforms, which might create support issues like software and hardware mismatch, making it even harder for the IT support to support the system (Rose, 2013). Because of these mentioned issues, the mobile device security standards are diverse and therefore the user security risks are also diverse, yet SMEs have shortages of skilled IT security personnel to support all the different platforms. As a result, users should assume responsibility for their devices and understand the risks of using their own devices for work purposes (Chen *et al.*, 2013). In this case, ensuring that the users are armed with all the knowledge, through

training and awareness of the security risks associated with BYOD, is important for an organisation as this facilitates the shift in responsibilities.

2.5.2.3 Data ownership policy

In his study, Reid (2013) argues that BYOD adoption actually exposes the organisation to unauthorised access to sensitive corporate data and increases cybersecurity threats. It is important that users are informed and educated about the expectations and control of corporate data on their devices. For some users, BYOD adoption means having access to corporate emails and storing work-related documents on mobile devices (Markelj & Bernik, 2012). Training around data ownership policy should be included in the awareness and training programmes, with clear distinctions and expectations between personal and corporate emails and data (Morrow, 2012). Ademujimi (2013) mentions that cybercrime and data fraud are big threats to SMEs due to the increase in identity fraud and most people's accounts get hacked and cybercriminals obtain important corporate information, which they then use against the organisations. If data loss risks of BYOD are not addressed in the training and awareness policies, the same mobile devices will be used for cybercrimes to initiate data theft (Harris *et al.*, 2013).

2.5.2.4 Device policies

Research points out that another potential risk of BYOD occurs when employees use mobile devices to access company data from public Wi-Fi (Bell, 2013, Garba *et al.* (2015). Bell (2013) states that most organisations believe that their existing security is robust enough to protect their network when the employees bring their devices and attach them to the organisation's network. Garba *et al.* (2015) also add that accessing corporate data or network from the public Wi-Fi is risky for the company because the mobile device and the location might not be trustworthy, and this poses a risk of corporate data leaks. While people do not understand the significance of passwords on their smartphones, the password is the only simple and fundamental practice to protect sensitive company data on mobile devices. Passwords are also useful in the event when employees lose their phones, as they secure the device and guard against data theft, which is a huge risk to the organisation (Astani *et al.*, 2013; Singh *et al.*, 2014). Users are not always aware of the policies that govern BYOD, so issues like

Wi-Fi, passwords, network, lost or stolen devices need to be highlighted in the training and awareness policy (Morrow, 2012). It is important for the organisation to set up and document security policies that highlight the security expectations. This policy needs to be included as part of BYOD training as this will ensure that the users fully understand the security risks associated with negligence (Putri & Hovav, 2014). Romer (2014) states that there are a lot of challenges around putting a policy together for BYOD. The major challenge is that the company does not own the device and, if anything happens to it, what legal actions will the company be allowed to take? These policies will guide the actions and highlight the consequences to the employees (Romer, 2014; Shumate & Ketel, 2014).

Figure 2-3 summarises the above critical elements as identified in the literature review.

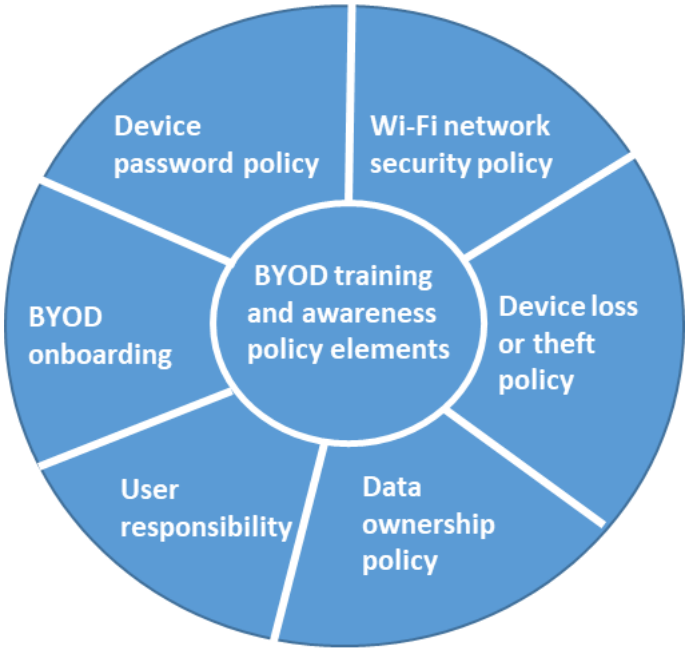


Figure 2-3: A summary of BYOD training and awareness policy critical elements

(Mitrovic *et al.*, 2014)

2.6 The need for BYOD training and awareness policy guidelines

By now, SMEs should be aware of BYOD security risks and consequences and the need to create awareness and educating the employees about the BYOD security risks (Morrow, 2012). From the available literature on this topic, it is clear that security awareness and training is a must-have for BYOD adopters (Keyes, 2016). However, there are no well-documented guidelines on what needs to be included or excluded,

must-haves and not so important elements for training and awareness. In their research, Chen *et al.* (2013) highlight the importance of exploring different approaches to training and awareness. Chen et al. (2013) advise trainers to focus on employees, highlight the security risks and consequences that are mostly fuelled by user actions and behaviours, and the security policies that affect the employees. Thomson and von Solms (1998) agree that policy is critical to the success of BYOD and it should put more emphasis on security policies affecting employees.

2.7 Conclusion

In conclusion, is it clear that many BYOD security risks are related to employee negligence and this justifies the need for training and awareness policies to ensure that employees are well educated and informed about the security risks related to BYOD. Gladyng (2013) states that there are a lot of challenges around putting a policy together for BYOD. It is also important for management to ensure that the organisation has a clear policy that is assessed and updated regularly.

It is important to also highlight device access and limits as, once BYOD is allowed, employees will go all out to find ways to ensure they bypass the security measures that are in place to access network using their personal devices. This might not be for selfish reasons but to enhance productivity and flexibility when away from the office. As a result, it may, in turn, harm the organisation and expose it to some hitherto unknown security risks.

If mobile devices are used for business purposes, they form part of the business, so it is important to ensure that all of them conform to the organisation’s security policy. However, it is not easy to impose corporate rules on personal devices. BYOD training and security policies must clearly describe security policy and the roles and responsibilities of maintaining mobile devices and ensuring that company policies and procedures adhere to the industry standards of data protection.

Bell (2013) explains that organisations must revise their old security and data policies and come up with new ones to accommodate the new changes that come with BYOD adoption. For organisations that have training and awareness policies, most still do not cater for the new dawn of BYOD. Security policies need to change regularly to address the current security threats and risks of BYOD (Chang *et al.*, 2014). Even if

an organisation can spend time to develop and communicate the BYOD security policies, guidelines and education, without user involvement and motivation, this would be another futile exercise. User involvement is a requirement for successful BYOD training and awareness policy.

Having the right technology in place is great for the mobile device owners and management, but the related human-factor risk will require proper training and awareness that cover all possible risks and best practices. Considering the fact that the same mobile devices used for work are also for personal use, it is important to consider privacy laws and involve employees so that they do not feel that their privacy is being invaded.

2.8 Summary

This chapter presented and reviewed literature that is pertinent to this study. Some of the literature that was reviewed was international in outlook and not specific to SMEs. This can be attributed to limited research on the topic in South Africa. This chapter begins with a discussion on the topic of cybersecurity in South Africa, gives a background of BYOD security risks in SMEs and training and awareness policies best practices to minimise BYOD security risks. BYOD human-element related security risks and challenges affecting training and awareness policies in organisations were also discussed.

The reviewed literature shows that SMEs are facing lot of challenges and security risks relating to BYOD and that training and awareness policies can play a very crucial part in addressing these challenges. In-depth literature review on how training and awareness policies can be used effectively to minimise the BYOD security risks, and on guidelines to develop these policies, was conducted. Although there are some studies which were conducted in South Africa, they were focused on big and international organisations. The findings of these studies may not necessarily apply to SMEs, thus, proving that there is a knowledge gap on this topic. This study attempted to address this knowledge gap.

The following chapter will discuss the research methodology adopted for this study, as guided by the literature review.

Chapter 3 - Methodology

3.1 Introduction

There are various methodologies that can be used to conduct research and guarantee unwavering quality of the study results. This chapter outlines the research methodology that was adopted for this study and provides context as to why the chosen approach is the most suitable. The aim of the study is to develop guidelines for security awareness and training policy to minimise the risks and threats of BYOD. For this specific study, the following research question was asked:

What are the guidelines to develop awareness and training policies to ensure that employees are well informed about the risks and threats of BYOD (Chen *et al.*, 2013)?

Recent studies on this topic point out that providing training and awareness for employees is important to the creation of an underlying foundation for BYOD (Rivera *et al.*, 2013). With this information in mind, this study seeks to empirically investigate the human-element of BYOD security issues and understand the policies organisations currently have. This will be done by collecting and analysing information around BOYD training and awareness from organisations and identifying the stakeholders' needs in terms of BYOD training and awareness and the underlying issues and requirements that need to be included in the policies.

Furthermore, this section will cover the research philosophy, approach, and ethics, followed by the analysis and discussion. For this study, the research methodology structure will be based on Saunders *et al.* (2007).

3.2 Research Philosophy

According to Bajpai (2011), research philosophy consists of beliefs about different ways in which data about a specific phenomenon can be collected, analysed and interpreted. Kuhns & Martorana (1982) describes a research philosophy as "…the set of common beliefs and agreement shared between a community of scientists about how a problem should be understood and addressed."

Terre Blanche *et al. (*2006) and Guba (1990) posit that the research philosophy can be characterised through the following dimensions:

- Ontology – our philosophy about reality,

- Epistemology – the theory of getting the reality and the knowledge,
- Methodology – how we get the data.

According to Hallebone and Priest (2009), epistemology deals with the nature of knowledge about social reality; it is more concerned about the source and limitations of knowledge and ways of acquiring it, the nature of the relationship between what can be known to be true and the knower, which is opposite to ontology. Ontology refers to what exists in the social world and is known to be a reality that reflects facts and the nature of that social reality (Blaikie, 2009).

There are two main aspects of ontology, which are objectivism and subjectivism. Objectivism holds a position that attests that social phenomena are built on grounds that actions of social actors and what they mean exist independently (Saunders *et al.*, 2007). It is an ontological position that speaks to a view that social entities exist in reality external to social actors related to them (Bryman, 2012). On the other hand, subjectivism holds a different view that social phenomena are formed as a result of the perceptions and the after-effects of the actions of the social actors concerned with their existence (Saunders *et al.*, 2007; Bryman, 2012). For this study, the researcher adopted a subjectivism ontological view, which suggests that the reality about the challenges of developing BYOD training and awareness exists. The knowledge and understanding of BYOD training and awareness challenges are shaped through the participants of the study, based on their social context and experience with BYOD adoption. The participants are the employees of SME organisations which have adopted BYOD. This is quite important in the context of BYOD, according to Waterfill & Dilworth (2014). BYOD training and awareness must include the people, process and technological effects of BYOD integration.

Epistemology refers to human attempts to gain knowledge about social reality. It is associated with the nature of knowledge of social reality and ways of knowing and learning about it (Saunders *et al.*, 2007). Bell *et al.* (2017) and Bryman (2012) postulate that an epistemology relates to the question of what is, or should be regarded as, acceptable knowledge in a specific field. There are four main aspects of epistemology and the two primary ones are positivist and interpretivist. Positivist research is used more when filling the gap. It is sometimes called quantitative research because often the output is quantitative data and is based on statistics as the researcher finds

relationships statistically. To a large extent, it is very objective, hence the term "objectivist", as it involves hypothesis testing to obtain the "objective" truth. It is also used as a means of predicting future trends. Critical realism is a subtype of positivism that incorporates some value assumptions on the part of the research. Researchers primarily rely on quantitative data to do this and theory is deductive.

On the other hand, interpretivist methods are inductive and associated with qualitative research. It is used mainly to obtain an understanding of the word from an individual perspective. Interpretivist research looks at reality from a different perspective and believes there is no single reality hence; we have to understand different cultures and people. The output of interpretivist research is often qualitative data.

For this research paper, the researcher adopted the interpretivist research method as illustrated in Figure 3-1, with the end goal of creating new and deeper understanding through multiple interpretations of the situation under investigation (Burrell & Morgan, 2019).

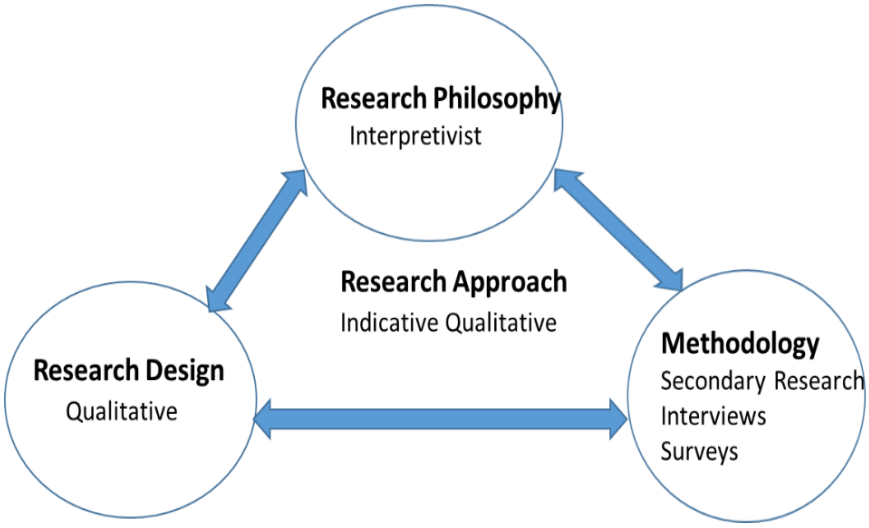


Figure 3-1: An overview of the adopted research approach and methodology

The researcher opted for this method because, according to Saunders *et al.* (2007), this method is suitable for this study since BYOD adoption situations are complex and unique. Interpretivism sees the world as complex, believes that different views do exist and that there is not only one right view (Saunders *et al.*, 2007). This resembles the complexity of the BYOD phenomenon, where different actors are more likely to

experience reality in different ways. Hence the researcher believes that the right view depends purely on one's perspective.

3.3 Research approach and design

According to the available literature on this topic, there are limited empirical studies in terms of the BYOD adoptions in the context of SMEs, which makes this study exploratory. This study is deemed exploratory because it aims to gain insights about the BYOD training and awareness challenges in SMEs. The study topic is very mainstreamed, but it is not fully explored.

According to Alvesson and Sklödberg (2008), research can be approached in three different ways namely: inductive, deductive or abductive. The inductive approach is mostly used when there is not enough theory on a particular topic or field of study. It starts with observing the situation before gradually moving towards the theoretical ideas and suggestions (Hallebone & Priest, 2009). The deductive approach starts with theoretical assumptions and move towards empirical evidence obtained through research and literature review. It is mostly used when there is already an established theory relating to the topic. The abductive approach works similar to the inductive approach, as it also starts with empirical evidence but does not eliminate the theoretical pre-conceptions. For this study, the inductive approach was followed, as inductive research aims at developing a theory by moving from specific observations to broad generalisations.

3.4 Research methodology

There are two approaches to conducting empirical research: qualitative research and quantitative research methods (Creswell, 2014). Each type of research has different objectives and methods, and both are important for gaining different kinds of knowledge.

Quantitative research explains phenomena by collecting numerical data that are analysed using mathematically based methods (in particular statistics). Qualitative research seeks to answer questions about why and how people behave in the way that they do. It provides in-depth information about human behaviour and makes use of qualitative data, such as surveys, interviews, documents, and participant observation, to understand and explain the social circumstance.

Qualitative research occurs in a natural setting (Bogdan & Biklen, 2007; Marshall & Rossman, 2006). In qualitative research, the researcher interacts with participants by observing and/or questioning. The study begins, not with hypotheses to be proved or disproved, but with a flexible plan to explore a phenomenon. Inductive reasoning is used to draw conclusions after all the data has been collected (Bogdan & Biklen, 2007; Taylor *et al.*, 2016). Qualitative research has four purposes: to explore, explain, describe or predict, (Marshall & Rossman, 1995). This type of research is expressed in words. It is used to understand concepts, thoughts or human experiences and how they construct meanings in their contextual settings, thereby revealing people's perceptions, values, beliefs, rules and interpretive schemes. It also enables the researcher to gather in-depth insights on topics that are not well understood, while quantitative methods are focused on numbers and are great for deductive approaches, as well as describing and measuring levels of occurrences on the basis of numbers and calculations (Saunders *et al.*, 2007).

According to Saunders *et al.* (2007), the appropriate research design for exploratory and inductive research is followed by extensive literature reviews and qualitative research through conducting in-depth interviews and questionnaires. For this study, the researcher adopted qualitative research methods. This methodology is applicable in this research as an extensive literature review on BYOD training and awareness challenges was conducted. This descriptive research method does not only provide definitions, but also interprets the different frameworks which allow this form of research to be effective in obtaining high results (Galliers & Land, 1987). In order to ensure that, the most relevant BYOD awareness and training policies were analysed by the researcher. Looking for commonalities, the researcher asked IT and Security personnel questions around the most critical and key points that should be covered in training and awareness for BYOD. Security experts who specialise in IT security and BYOD assisted the researcher with the BYOD security challenges and training and awareness findings, which served as a foundation for determining what training and awareness elements of the policy were most relevant to facilitate and cover for effective BYOD security training and awareness.

3.5 Data Collection technique

For this study, data were collected in two phases. Firstly, the main data collection technique was the interviews, followed by surveys. Interviews are described as a form of a conversation between the researcher and the participant for the purpose of obtaining clarity on the problem under investigation. In-depth interviews can be used together with other techniques like observations and can also be used as the main source of data in research.

According to Marshall and Rossman (1995), data collection methods for qualitative research can be divided into two main parts, which are primary and supplemental data collection techniques. For this study, the primary techniques include the following:

- Participation – this involves first-hand involvement in the activities of the participants chosen for the study.
- In-depth interviewing – this is a conversation between the researcher and the participant and ranges from completely structured to open-ended.

Marshall and Rossman (1995) define an interview technique as a method of data collection that may be described as an interaction involving two participants, an interviewer and an interviewee, with the purpose of eliciting valid (credible) and reliable (dependable) information.

As the second phase of the data collection, the researcher conducted surveys with selected participants to gather qualitative information about BYOD security challenges and awareness and training policy, following the interviews with the BYOD security experts and employees.

This study is targeted at SMEs operating in different industries within the borders of South Africa. The primary source of data sources was from the IT/Security managers and BYOD users to gain more knowledge about BYOD, from the SME context, the challenges and the relevant elements in the experts' opinions. This was achieved by conducting surveys and in-depth interviews with experts in the field, such as heads of security and IT security managers. Interviews with experts are the most appropriate tool, considering the nature of the complexity of this topic and because experts are useful sources of in-depth and high-quality data (Lapan *et al.*, 2012; Morse, 1994).

These interviews were semi-structured to ensure consistency, but also provided room for follow-up questions which were necessary to gain more knowledge about any complex components with which the researcher was not familiar. The interview questions were slightly adjusted depending on the interviewees' expertise and perspectives.

Surveys were used in addition to interviews because there was a need for another data source to complement the lack in the literature review. For this topic, it was important to get practical knowledge which would give the researcher much better insights than just the theoretical body.

Since the aim of the study is to develop a guideline, it is important for the researcher to gain relevant information through interactive sessions, such as in-depth conversations and interviews with experts. The interviews were used to test whether organisations had guidelines or not. In additions, these interactive sessions were used to explore the reasons why organisations had or did not have any BYOD guidelines. Where the guidelines existed, the aim was to explore how they were developed, as well as ask for more context around them. The interviews immensely helped the researcher in that regard.

The questionnaire, in contrast, covered the BYOD risks that users need to know about and tested if they were aware of those risks. The responses to these questions helped the researcher to understand the risks and rank the important elements to be covered in the guidelines. Both data collection methods cover a different area of this study.

In addition, the goal of the interviews was to extract information from security experts about the effectiveness of BYOD awareness and training elements for SMEs. It was important to gather information about awareness and training challenges and the effectiveness of the policies in practice from security personnel within the SMEs, since they have a better understanding of BYOD use and challenges in their respective organisations. The interviews were recorded and later analysed through thematic coding. From the data collected in the literature review, two questionnaires were created with the goal to structure and prioritise BYOD training and awareness elements derived from the literature review. During the survey, the participants were also asked if they were willing to partake in the interviews. It was explained to the

participants that the responses to the questionnaires and interview questions would be included in the research findings.

3.6 Sampling strategy

For this study, the researcher, the researcher applied a purposeful sampling technique, also known as subjective sampling. According to Merriam (1998) this sampling happens when the researcher uses his/her own judgment to select the research participants who know more and can provide more about the topic at hand. Patton (2002) also explains the purposeful sampling technique as a non-random method of selecting participants for the study.

The sample for this study is made up of 15 SMEs, from different industries such as media, fintech, insurance, transportation and distribution, marketing, IT services and tech, tourism, and hospitality, employing between 15 – 50 employees. Both the end-user and IT/security personnel who participated in this study are an integral part of this study as they are directly affected by BYOD in their organisations. It made much sense to include them in the study as well as interview IT security experts as they are also quite knowledgeable of the security risks of BYOD and the significance of ensuring that the right tools and measures are put in place to protect the organisational assets. Due to their involvement and experience in SMEs, developing and implementing the BYOD training and awareness policies. It was practical to use them as participants and sample for this study.

The tables below profile SME IT managers/IT security professionals and employees who participated and were interviewed for this study.

The purposive sampling technique is used quite extensively when selecting participants for qualitative research, because it helps the researcher to uncover the most significant data about the problem being investigated. The chosen participants were shown to be experts in the field and were approached through social media and business networks. To ensure the correct sampling size was used, the researcher followed Saunders *et al.'s* (2007) sampling guidelines for size. According to Saunders *et al.* (2007), for semi-structured interviews, the sampling can vary between 5 to 25 participants.

The data collection process started in May 2019, with emails and messages sent to different SME security experts, asking them to participate in the study. The researcher

sent interview requests to 20 participants. The response was very slow, although eventually, 9 responded positively and agreed to participate in the study. The other 6 interviews were through referrals. All the interviews were confirmed on the phone and scheduled for one and a half hours each, between May and June 2019. In Johannesburg, the researcher had an opportunity to conduct some of the interviews face to face. After the 12th interview, it was determined that there was no new information being collected, as the participants were repeating the same information that the previous participants had already shared. The researcher concluded that data saturation had been reached. If the sample for this study is not enough to provide new information on this study, it will at least be helpful to take the study further for future research, when combined with questionnaire data. All the interviews were conducted in English, Sotho and Zulu respectively. For these reasons, because of translation, there might be a risk of misinterpretation bias from the author. Table 3-1 and Table 3-2 below show the participants who took part in the interviews. These participants were sampled on the basis of recent studies which gave insights into the nature of participants who can capably provide insights on the chosen topic. The chosen respondents fit into the following criteria:

- A participant who owns a Small-Medium Enterprise.
- A participant who is a security expert in a Small-Medium Enterprise.
- A participant who is employed by a Small Medium Enterprise.

Table 3-1: List of participants - Security experts

Organisation	**Position and Area of Expertise**	**Years of Experience**
Org_1	Security Manager	10 +
Org_2	Security Analyst	15+
Org_3	Head of Security	13
Org_4	Security Manager	10+
Org_5	Systems Integration Engineer	9

Org_6	Security Engineering Manager	12
Org_7	Information Security Officer	10+
Org_8	IS Awareness Analyst	15 +
Org_9	Manager, Solutions Architecture	10+
Org_10	Architect Security	9
Org_11	Security Analyst	6
Org_12	Governance and risk Manager	11
Org_13	Information Security Officer	9
Org_14	System Administrator	12

For employees, the researcher chose the participants purposefully, taking into consideration their IT levels and backgrounds and the industry their employers operate in, because the SMEs who are rendering IT services or products will most likely hire employees with IT backgrounds, whereas the SMEs in transportation industry will most likely outsource one or two IT skills and hire non-technical employees. This makes a huge difference in the collected data, as it is somehow believed that the employees with IT background will be more cautious and alert when it comes to security risks of using their own devices for work. The contributions of both technical and non-technical employees, as participants in interviews and questionnaires, were just as significant to this study because these participants are the ones who use the devices on day to day basis and are indirectly affected by BYOD risks. They also play vital roles in the development of training and awareness policies.

Table 3-2: List of participants - employees

Participants	Employees with a non-technical background	Employees with the technical background
Employed by Tech SME	3	7
Employed by non-Tech SME	4	6

3.7 Data analysis

From this study, the researcher adopted a thematic analysis approach for data collected through interviews. Thematic analysis has multiple functions in research namely: telling a story, making an argument for a specific purpose, giving a voice to the participants, summarising and describing the data collection guidelines (Braun & Clarke, 2006). These guidelines are made up of five phases: familiarisation with the data, generating initial codes through reflecting, engaging and thinking of the background of the research problem, generating initial themes, defining and naming themes and, lastly, producing the list of themes. The participants who agreed to be interviewed were also requested to take part in surveys. Data were analysed in two methods. Table 3-3 below shows the data analysis approach used for each data set:

Table 3-3: A summary of qualitative data collection and analysis methods

Format of Data Source	Research Question	Analysis Method
Interviews_1	1, 2 and 3	Thematic Analysis
Interviews _2	1& 3	Thematic Analysis
Questionnaire_1	1	Analysed in Microsoft Excel
Questionnaire _2	2 &3	Analysed in Microsoft Excel
Questionnaire_3	2 & 4	Analysed in Microsoft Excel

The researcher collected the data by herself, so there was some familiarity with the data. Because there is so much that has been written about this topic and due to the complexity and richness of the data that was collected, the researcher can spend more time studying the data and reading through each dataset individually. In so doing, the researcher would be able to take note of terms of interest around the security risks, human error, training and awareness and policies by being as inclusive as possible through active, analytical and critical reading.

The researcher started off by colour-coding and capturing all data. At this point, the researcher did not pay close attention to the themes and deliberately avoided analysing if the data met the objectives and goal of the study. Similar codes were put together and potential themes were identified. The researcher followed a similar approach for all the interview data sets. The aim was to find the key factors and meaning for each theme and then relate these to the research question. Based on the research questions, the following six themes were identified, as shown in Table 3-4 (Braun & Clarke, 2006). A similar approach was used for all the interviews that were conducted, with an end goal of identifying important themes.

Table 3-4: Thematic coding

Code	Theme	Goal
T-1	BYOD in SME	Understand the positioning of BYOD in SMEs
T-2	BYOD security concerns for SMEs	Discover the security risks of BYOD
T-3	BYOD training and awareness practices in SMEs	Understand the current training and awareness practices
T-4	BYOD training and awareness challenges	Investigating BYOD security training and awareness challenges for SMEs and solutions to overcome the challenges
T-5	BYOD training and awareness elements	Identifying the relevant elements of BYOD in SMEs
T-6	BYOD training and awareness Effectiveness	Examining the effectiveness of the training and awareness practices in SMEs

Following the interviews, surveys were conducted online through Google forms. The questionnaires were mainly around security risks, human error, training and awareness programmes, and policies from both the employee and security management perspectives. For employees, the aim was to get an understanding of how much they understood the human-related security risks and their roles in ensuring that their devices were as secure as possible. The employees were also asked to estimate the amount of effort their organisations were making to ensure that they were well equipped and knowledgeable about these risks. For security management and personnel, the survey was mainly designed to understand how organised and effective their current awareness and training programmes were and if they thought they were doing enough as security personnel to educate their employees.

The Google forms tool was selected because of its ease of use and ability to allow each participant an opportunity to complete the surveys whenever he/she liked. Participants were invited through emails. The tool provides data analysis capability through Google spreadsheets and enables users to view and analyse data in detail once it has been collected. Figure 3-2 below illustrates a summary of the data collection and analysis process.

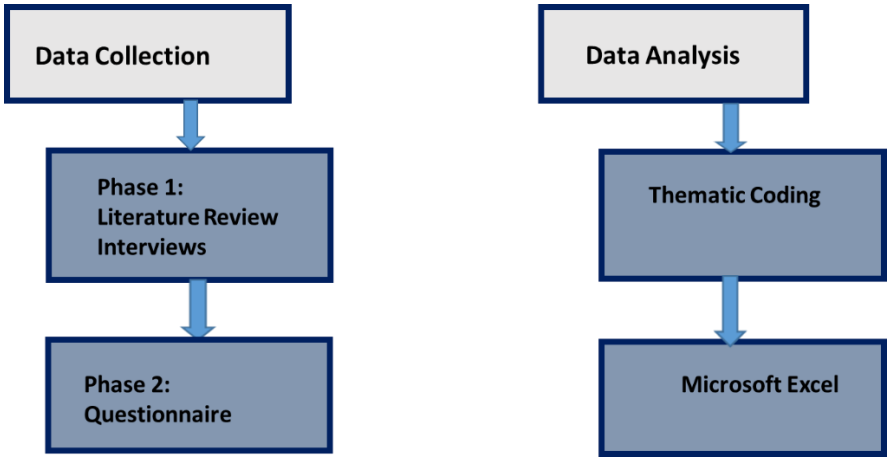


Figure 3-2: A summary of data collection and analysis process

3.8 Reliability and Validity

Assessing the reliability and validity of qualitative research is not easy. Some researchers, notably Kirk & Miller (1986), Kvale (1989) and Patton (2002) argue that reliability and validity are more appropriate for scientific and experimental studies. However, it is also believed that reliability and validity add value to qualitative research. According to Kirk & Miller (1986), validity and reliability are two very important aspects of qualitative research that determine the credibility of the study. When conducting qualitative research, to ensure that the research results and findings are a true reflection of the situation, it is important to be critical and scrutinise the quality of the research process (Patton, 2002). Validity refers to how appropriate the data collection measures used are, how accurate the analysis and results are and lastly, the generalisability of the findings (Kvale, 1989). For qualitative research, the term trustworthiness is a word used to measure the reliability and validity of a qualitative research study. Krefting (1991) and Lincoln & Guba (1985), the “trustworthiness” of qualitative research can be assessed in four ways: credibility, transferability, dependability, and conformability.

Credibility: This was addressed by collecting data from different primary sources and experts through multiple data collection methods, interviews, and surveys (Lincoln & Guba, 1985).

Transferability: In order to ensure this, experts and users from different industries and across different SME organisations were chosen. All chosen participants had wide experience in BYOD adoption.

Dependability: the researcher will ensure that the findings are consistent and representative of the true meaning of the collected data, through capturing the truth and reality of the participants (Korstjens & Moser, 2018).

Conformability: by presenting the findings that are shaped by participants (Anney, 2014).

3.9 Ethics

During qualitative research, the researchers and participants establish close relationships that can raise a range of different ethical concerns, and qualitative researchers may face dilemmas such as respect for confidentiality, establishing honest and open interactions, and avoiding misrepresentations of data (Morse, 1994;

Miller, 2012). Ethical considerations have to be taken into account as the interaction between the researcher and the participants can be ethically challenging, especially for the participants as they are involved in the crucial stage of the research. Myers (2013) describes “ethics” in research as an upholding moral principle in planning, conducting and reporting the research findings.

Anonymity and informed consent are also part of the ethical concerns that should be considered while carrying out qualitative research. The interviews followed the guidelines described by Patton (2002). The researcher treated the participants with respect and explained the purpose of the survey and interviews.

The following ethical considerations, in consent with the NWU rules and regulations of conducting research, were taken into account:

- Privacy and Confidentiality - Krefting (1991) explains that confidentiality is the way the information about the respondent is kept in a confidential way. For this study, the participants were assured that their identities and those of their respective employers will be dealt with in high confidence. The participants were also assured that their willingness to participate in this research will not be exploited for any personal benefit, by deceiving or betraying them in the research route or its published outcomes.

- Voluntary participation and informed consent - to ensure that the study is conducted in a legal manner, the researcher obtained written permission to conduct this research from the NWU research board. The researcher explained the principle of voluntary participation to the respondents and made it clear that they had the right to decide not to participate in the study at any time.

3.10 Summary

The table below represents a summary of the research methodology.

Table 3-5: Summary of Research Methodology

Methodology	**Adopted**
Ontological view	Subjectivism
Epistemology	Interpretivist
Research approach	Inductive

Research method	Qualitative
Data Collection	Interviews and surveys
Data Analysis	Thematic Coding and MS Excel analysis
Research purpose	Exploratory

Chapter 4 - Results

4.1 Introduction

In this chapter, the results of the study are outlined and examined in detail. The main goal of the study is to develop guidelines for BYOD training and awareness policies and ultimately improve the effectiveness of these policies in minimising the security risks. The interviews and survey results are presented based on the research questions. Firstly, the chapter discusses BYOD security risks in small and medium-sized organisations (SMEs). This is followed by a discussion of the human-factor related risks that contribute to BYOD security risks. The last section examines the effectiveness of security measures that are currently being implemented.

The participants were asked to rate the extent to which current security measures used in the SMEs are effective, and the results thereof are presented and discussed in the ensuing section. Lastly, the key elements of the importance and relevance of developing effective BYOD policies will be presented. All the interview questions were answered in English, Zulu and Sotho, so the researcher has translated some Zulu and Sotho words to English. The questionnaire and the Excel file can be found in appendices 1 and 2.

4.2 BYOD risks in SMEs

From the interviews, the participants identified a list of BYOD security risks they face. According to the participants, these can be identified as organisational and human-factor risks. Table 4-1 below outlines the BYOD security risks at an organisational level as mentioned by the participants. The participants confirmed the assertion from the literature about BYOD security risks in SMEs. One comment that stood out from the interviews was that it seemed in SMEs, the driving force behind BYOD adoption is lack of funding for technology investments, which also explains why the security risks are so high, relative to big organisations. The participants mentioned that most of the challenges stem from a lack of interest and support from the management. Cultural related issues were also identified as contributing to BYOD security risks. Keeping in mind that BYOD security issues are not the only technology-related risks, this study will focus on addressing BYOD security risks and how SMEs can use training and awareness policies effectively to minimise the risks.

Table 4-1: BYOD security risks findings

Risk	# of Times Mentioned
People	15
Access Control - Unauthorised access to our systems by hackers	12
Theft/Loss of devices	11
Unauthorised data distribution and data leakage	11
Phishing (Opening an email attachment from an unknown source)	9
Public WI-FI	8
Unauthorised devices	6
Clicking on a link to an unknown website	6
Security controls	5
Lack of control over a device	5
Malware	5

Table 4-1 above shows that people, unauthorised data distribution, phishing, data leakage and lost/stolen are devices are the top 5 security risks for SMEs as mentioned by participants. Employees were also asked the same question to determine how much they knew about BYOD risks and explore whether there will be any similarities in employees' responses to the risks mentioned by the security experts. This is how the interviewees responded to the questions: **Mention the top 3 BYOD security risks**

One participant mentioned that stolen customer information and business strategies are two of the biggest issues for SMEs:

Participant 1: Employees resigning from the organisation and leaving with inside information is a big issue we are currently facing. This leads to stolen ideas and customer information.

The participants noted that human factor-related risks are more of a risk for SMEs than organisational related issues. Keeping in mind the nature of BYOD, BYOD training and awareness policies may not be able to directly fix some of these risks such as lack of control of the device. However, participants stressed that, to a certain extent, training and awareness policies can mitigate most of these risks. For example, BYOD training and awareness policies will not precisely address the lack of control of a device, but training and awareness policies can be effective in improving the security culture of the organisation and, in turn, help employees to be more security-aware and knowledgeable about how to better manage and protect their devices. Most security experts mentioned that people are the biggest security risk. People were mentioned most often as a human element, because the participants commented that most of these risks arise from human error.

One participant was cited as follows:

Participant 3: People are most likely to make bad security decisions.

Participant 2 noted that even with extra investments in security, the change is unnoticeable:

Participant 2: We have doubled our budget for security training and awareness for the past year, but I cannot prove if these exercises were fruitful or all the security breaches we face are just a human error.

Participant 6 also emphasised that currently, the human factor is one of the top risks of BYOD:

Participant 6: People … are the weakest link now, in terms of hacking and phishing.

Participant 7 also emphasised that even with the known human-factor risks, BYOD was still a way to go:

Participant 7: The BYOD train has left the station and not participating will be foolish, but you can’t trust everyone, you know you will have a few bad apples.

Another participant commented on the issue and contended that people were the problem.

Participant 4: Most of the time organisations also don't inform their employees about their plans – but are quick to blame the employees, while nothing was communicated or there's little or no effort to ensure that the employees are on the same page with the security team. Few things that need to happen:

- ensure that your employees understand your plans and BYOD training and awareness policy,
- create awareness related to managing the risks – like publishing the process for remediating situations like lost phones and where data was thought to have leaked, etc.,
- people pushing back and rejecting MDM take time to understand what MDM did and didn't do,
- provide training to show employees how and what's the purpose of the MDM in particular.

If you decide to share less, just ensure that you have a consistent firewall around the messaging. A solid well-thought-out communications plan will work in your favour to allay fears, rumours, and perceptions that could undermine your efforts.

From the questionnaire, 14 out of 20 participants believed that employees were the main culprits behind the security breaches:

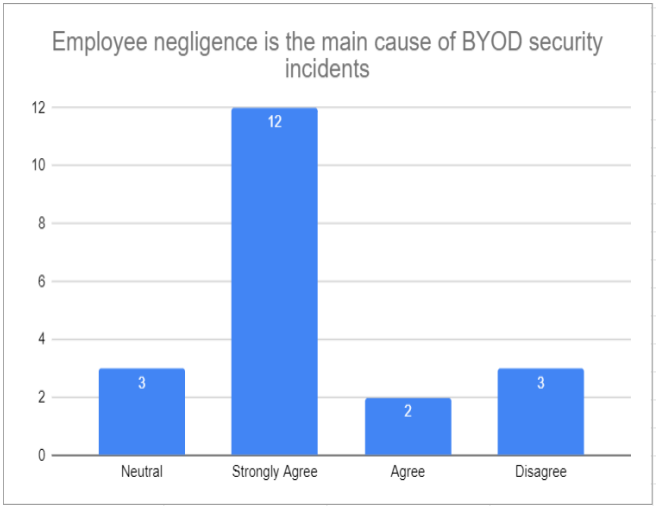


Figure 4-1: The main causes of BYOD security risks

One participant also mentioned that the human factor adversely affects the SMEs' business, as some of their employees were contracted by big organisations, who also saw this as a risk:

Participant 6: This issue is in two ways, for a big organisation, external contractors are a risk and for SMEs, the remote workers are a risk for data breaches, both have a huge impact on SMEs business with other organisations.

4.3 Human factor-related risks of BYOD in SMEs

Table 4-2: Human factor-related to BYOD risks

BYOD Risk	# of Times Mentioned
Weak Passwords	15
Data Leakage	12
Phishing (malicious emails)	11
Stolen Devices	11
Malware	9
Unsecured Networks	5

In addition to all BYOD security risks previously described in the literature review on this topic, multiple security experts mentioned that the top three, which are frequently identified and certainly the biggest BYOD risks, are mostly related to people. Table 4-2 shows that several participants noted that human-factor related risks are more of a problem than technical related issues. Weak passwords, data leakage, phishing (malicious emails) and lost or stolen devices are basically human-related. They are classified under human error BYOD risks and pretty much carried high weight of these risks.

During the interview, Participant 1 explained that the complexities of BYOD risks are usually due to human error:

Participant 1: No matter what the case, security almost always boils down to the human element and our natural trained or ingrained responses.

One participant claimed there were a lot of data breach incidents that took place because of the human-factor but are not always publicised:

Participant 2: SMEs experience a lot of data breach accidents and most organisations don't talk about it. Internally, we talk about them, but we avoid publicising these kinds of issues as they attract bad publicity to business and might harm your reputation. Even big organisations avoid this. Employees will be told of the incident and that it was handled but advised not to talk about it outside of the organisational premises.

One respondent mentioned how an incident that took place in Asbury Park's Epoch Trading Post really shook them.

Participant 7: An organisation experienced the worst, the hacker hacking their emails, cracking the two-step authentication, to even taking over their presence on social media, re-routing company websites, stealing an organisation's domain, faking ownership of the SMEs website. Apparently, this was before Black Friday 2018, one of the biggest sales events of the year. That organisation couldn't recover [its] reputation, lost sales for that day and cost to recover from that event. This was a real wake up call for us as SMEs. Some still think this will never happen to them – but the question is if it happens, will you be able to survive, or we'll have to start all over like the Asbury organisation? That organisation has the exact similar operating model as us.

Participant 3 also emphasised that the Asbury Park incident was due to a lack of control around BYOD and the people issue:

Participant 3: For all the SMEs, the Asbury Park incident really caused a panic and a wakeup call to those who didn't see a need for BYOD policies and employee management.

Despite the nature of BYOD and the fact that it gives organisations an opportunity to spend less on technology, SMEs are still finding it hard to manage its human factor security risks, such as weak passwords and data leakage. However, most participants

stressed that training and awareness can mitigate a few of these challenges, but to a certain extent and if implemented currently.

4.4 Measures that are currently being implemented

From the interviews conducted, the IT security expert who participated in the study answered the following question:

What measures are currently in place and to what extent are they effective?

Table 4-3: Security Measures in place

Measure	# of Times Mentioned
• BYOD Policies	7
• Promoting Security Culture	6
• Training & Awareness initiatives	4
• Technology	6

Table 4-3 shows the results of the interview question with the security expert. From the above table, it is apparent that organisations have several options to minimise the risks of BYOD. Four were mentioned in an interview. Due to the high risks of security threats, most of the big organisations have implemented all these means. However, for SMEs, it is a bit of a challenge to deploy and manage these security measures. Some are a bit complicated to deploy and others are expensive. Four participants asserted that they did not have any technology measures in their organisations, except for the capability that comes with mobile devices.

Participant 4 mentioned that his/her organisation had a BYOD policy in place. The policy that covered the basics:

Participant 4: We currently have a BYOD training and awareness policy in place, although it is not well documented. The aim of the policy is to enforce some basic settings (password strength and guidance for lost or stolen devices).

Participant 3 stated that his/her organisation used training and awareness:

Participant 3: we use training and awareness programmes to meaningfully increase awareness.

Participant 5 noted that culture is at the core of world-class security policies:

Participant 5: My experience stems from assessing and building a world-class security policy literally from a staff of zero security knowledge and without a supportive culture, a fundamental understanding of security starts at the IT level, resistance from various levels of leadership, and with absolutely no roadmap or path to integrating security policies. I've been through a few of these 'cattle-rides' and I see no other way to shift culture, process, financial concerns, minds, and formal sponsorship without engaging the employees, who are at the core of BYOD and can – you need to present and articulate the importance of a security policies to them. That's where culture hacking starts, and without it, the efforts might not pay off.

Participant 6 highlighted the importance of having the IT department working together with employees:

Participant 6: Security team needs to be more approachable and relatable to people, this is so important and will help encourage employees to speak up about any security related issues they face, before contacting Google and trying to fix them alone.

Participant 9 noted that affordability was a challenge when it comes to technology. SMEs' budgets are relatively small and tight:

Participant 9: Security is expensive – funding is a big issue for SMEs, and we can't afford. Management needs to put in extra investments for security technology.

4.4.1 BYOD Policies

Table 4-4 below shows the BYOD policies that participants mentioned during the interviews answering the following question, posed as a follow-up question:

The table below indicates the number of times the participants mentioned specific security policies required for BYOD.

Table 4-4: Type of Policies for BYOD

• Training and awareness Policy	7
• Access policy (Data access & zone according to class)	5
• Revocation policy (lost or stolen)	5
• Data ownership policy	3

From the survey, the results show that although the security experts understand and know the alternative measures and policies required for BYOD to protect their organisations form the BYOD security risks, most of them have not implemented the BYOD policies. Sixty-five percent (65%) of the participants responded negatively to the following question:

Does your organisation have a formal training and awareness policy that educates employees about the security risks of BYOD?

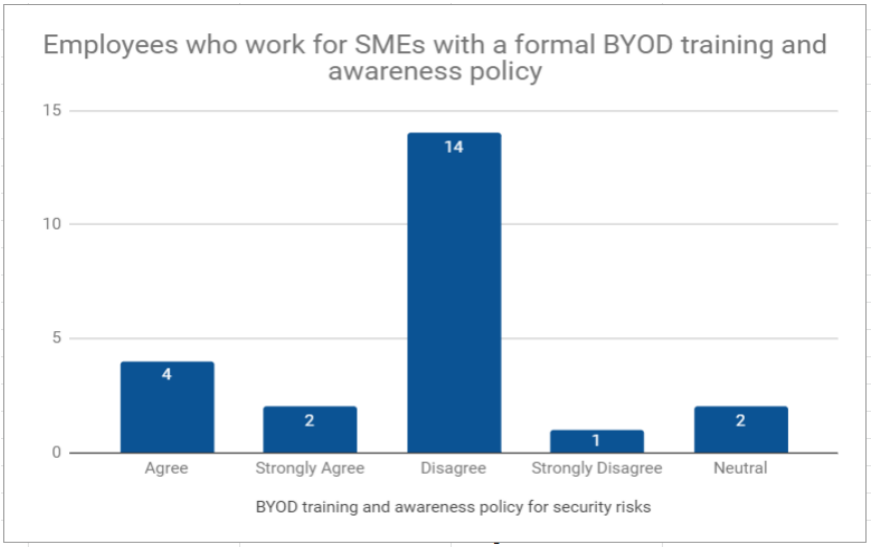


Figure 4-2: SMEs with BYOD training and awareness policy

In Figure 4-2, 60 % of the participants noted that their organisations have no training and awareness policy, while 17% of the respondents say their organisations have a well-documented policy that they have implemented for BYOD security training and awareness.

The following were added as comments on the survey:

Participant 1: Working for a company that provides IT services to the bank, they have strengthened their procedures to try and curb being infiltrated using staff members.

Participant 2: The organisation needs to invest more in employees to provide knowledge.

Participant 7: We are fairly a small organisation with diversely IT-aware employees (we're in the IT industry). We have a very strict encryption policy for all our devices and recently rolled out a data classification project which was very successful, with our employees working with us. However, there is still fear that people can install whatever they like on their own mobile devices, so what happens one day when someone decides to download this unknown malicious application and it access our confidential data? Unfortunately – it's not possible to just trust – fully trust that the user will always do the right things. Although we have sessions where we empower them from time to time, you still can't trust!

Participant 6: From the employees' side there is also a push back.

Employees also voiced their concerns regarding the SMEs' efforts to help them secure devices and data. The employees are concerned about the invasion of their privacy:

Participant 1: I feel like I am being watched.

Participant 2: Treat us as adults and respect our privacy.

Contrary to what one would expect, one participant said the following:

Participant 3: When it comes to BYOD, I find that IT worries way too much about security. employees understand that security is important. The criticality or confidentiality of the data on the phone is really that confidential or security is just being used as an excuse or nuisance to not allow employees to use their own mobile devices for work.

Another participant argued that phones were more secure than laptops:

Participant 7: Unless there's an encryption software installed. I am referring especially to the iPhone – in a sense that if you get your iPhone password wrong a few times, the phone will automatically block and the device wipes, which the laptops don't do.

4.4.2 Promoting Security Culture

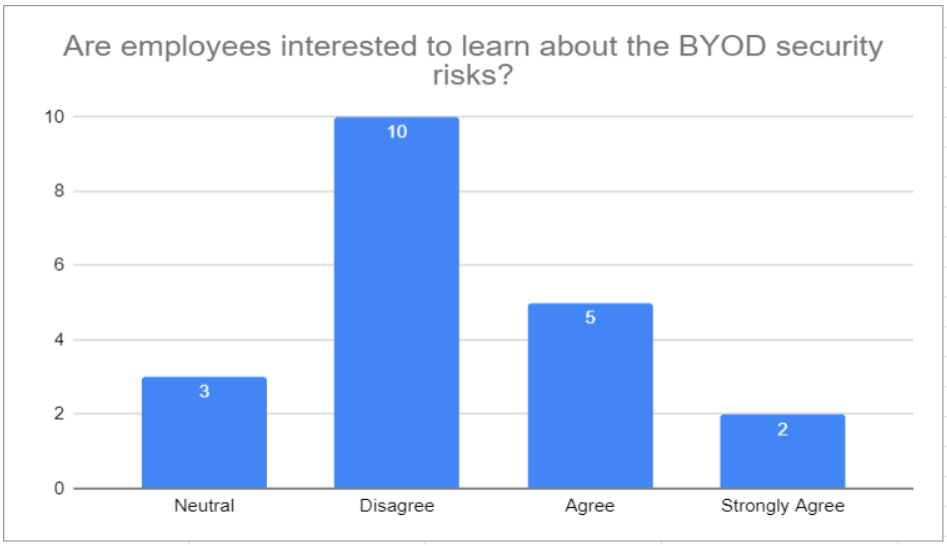


Figure 4-3: Employees interest to learn about BYOD security risks

From the above, the results show that people and culture also seem to play a huge role in the BYOD security issues, but there are different perspectives on this argument. The following comments were noted from the interviewed participants:

Participant 1: Because BYOD is to some extent pushed by employees, effective security also relies heavily on people doing the right thing. BYOD requires that security leaders optimise people through good security culture.

Participant 2: Even if you have a good security culture in your organisation, you are still susceptible to security risks and something can go wrong.

4.4.3 BYOD training and awareness policies

From the security experts, most participants noted that getting user or employees to participate in security awareness initiatives is a problem. They noted the following:

Participant 1: It's still a challenge to get the employees fully committed and invested. They tend to think we trying to be difficult.

Participant 4: It's not that we're just trying to be difficult by imposing rules, but we're working to prevent data leakage and data loss out of the organisation's network.

Participant 5: Even with the best of intentions, there will always be those who think you are out to get them.

The employees emphasised the importance of educating employees about the use of technology:

Participant 3: Security is very important when it comes to technology and end-users are not educated enough.

Participant 5: Most of the time as users, we assume that everything we download or upload to our devices it's safe to use, we believe that iOS App Stores or Play Store has done the vetting, and everything is safe.

Participant 8: People in general within organisations are not security conscious and we stand a high risk of having our devices hacked and important information stolen cloned due to lack of knowledge ad exposure of online protection of information and its manipulation.

Table 4-5: BYOD security training and awareness methods

Measure	**# of Times Mentioned**	**Addressing Risk**	**Implemented**
Best practices and Encouraging the use of password	19	Weak password	9
Training(e-learning)	10	Malicious activities and unsafe WI-FI	3
Educational programmes	9	Awareness	6
Phishing programme (monitoring clicks rates)	8	Phishing	5
conduct red-team attacks	7	Risk simulations to improve the security culture	4

From the above table, it is quite clear that organisations also understand the importance of the use of training and awareness to minimise BYOD security risks. The following were noted from the participants:

Participant 3: We conduct red team and fake attacks to understand the organisation's vulnerability to various types of attacks. We don't chase the guilty parties but keep the results anonymous.

Participant 7: Once a year we run a phishing test. Here we send fake phishing emails to everyone in our organisation and test their knowledge of phishing emails. We then release the results of the phishing test (without specific names of course, but just percentages of how many people failed to recognise the phishing emails).

Encouraging the use of passwords:

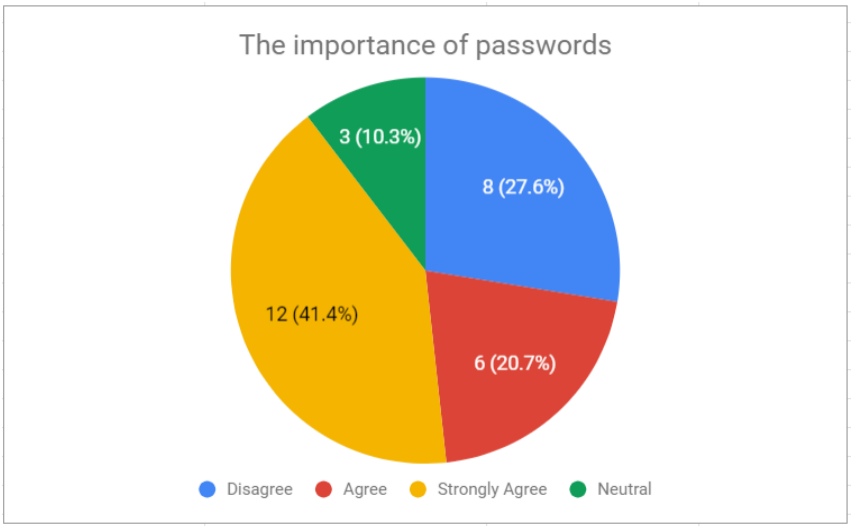


Figure 4-4*:* Importance of using passwords

Figure 4-4 shows that most participants agreed that the use of passwords on mobile devices was important in SMEs. From the questionnaires completed by the employees, 62% of the participants said they understood the importance of using passwords:

One participant mentioned the importance of encouraging users to use passwords:

Participant 1: It is important to emphasise the use of passwords. This is the minimal every organisation can do as often as possible.

Participant 5: You'd be surprised to know how many IT professionals don't know the importance of using passports to protect your phone. Training programmes don't have to be expensive or extreme. In the simplest of cases, they can consist of a PowerPoint presentation with a list of scenarios, some statistics and “Dos and Don'ts” that matter to security. In the end, I suggest using an examination to assess the effectiveness of the course. I also suggest a follow-up discussion to cover any confusing or unclear points. A refresher course every six months would also be a very good idea and it could be as minimal as a two-hour refresher, covering the high points and answering any questions that might have arisen during the discussion.

Other participant noted that using passwords also helps to secure his personal information, not just the organisational data on the device:

Participant 2: Mobile device security is not only to ensure my work data is not affected but it also impacts my personal data as well.

From the interviews, the participants noted the following technical measures as ideal security:

Table 4-6:Technology measures

Technology	**# of Times Mentioned**	**Implemented**
Hardware authentication (including Biometric)	15	12
Mobile Device Management (MDM)	11	4
Application Security	6	2
Data Loss Prevention (Encryption and tokenisation)	9	2

Table 4-6 shows that most interviewees knew about the other technological measures which were being utilised in South African SMEs, that can help minimise the security risks. Hardware Authentication, like fingerprint and voice recognition and Mobile Device Management are the most used security measures in SMEs. However, the

participants asserted that there were only a few SMEs that had implemented MDM as it was quite expensive. For those who had it, they mentioned they had only implemented the minimal package. One participant noted the following:

Participant 2: Technology alone is not enough. However, MDM is a definite need – but also a very minimal MDM, use only the features that you need and keep it as minimal as possible. Also, the ability to wipe company information ONLY – in case someone leaves the company, or when the phone gets stolen.

Another participant had a different opinion about MDM:

Participant 5: BYOD adoption has been a mixed experience for our organisation. In terms of the Mobile Device Management, we have experienced a push back from our employees, not wanting to place their personal device under MDM control, but we have been able to address the issues with the Android users, limiting the MDM control to only work-related information and applications

For iOS users, MDM does not really work well, and employees were very accommodative and willing to work together with IT personnel to make it work.

Other respondents from the interviews showed general concerns about technology as a means of reducing the risks of BYOD:

Participant 3: The issue is not technology related, and it cannot be solved by technology – the issue is physical, it's related to human behaviours and culture.

Another participant answered this question with a rhetorical question:

Participant 6: What is technology without training? Technology alone is not enough.

Answering the question about how effective the currently implemented BYOD training and awareness policies are, the responses were as follows:

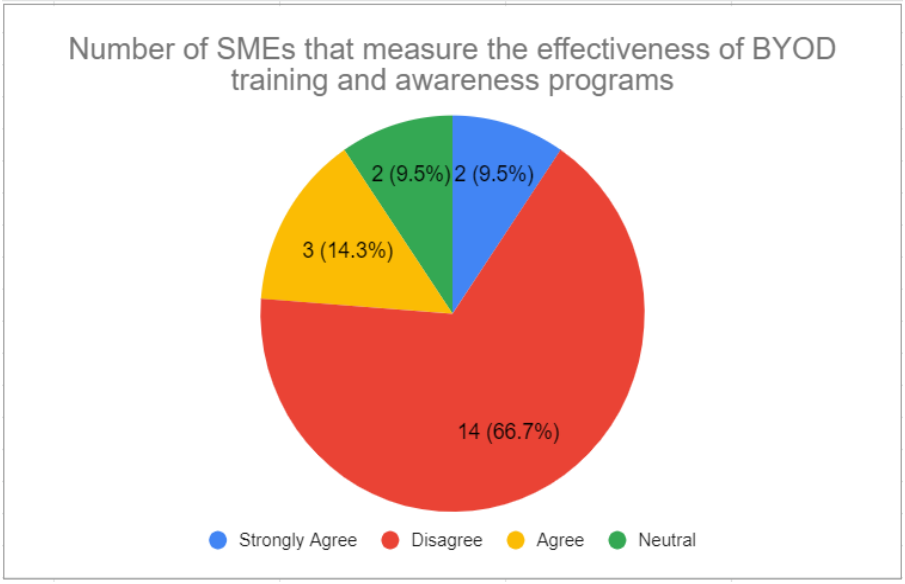


Figure 4-5: Effectiveness of the current training and awareness policies

From Figure 4-5 above, the findings from the interviews showed that there was a challenge with the current awareness programmes. Although some participants highlighted that their employees were dedicating some resources and time for employee awareness programmes, the results proved otherwise. From the interviews, the following was noted:

Participant 1: The behaviour is still not improving. The exercise is, mainly to tick the box – and don't guarantee that the employees with complying with security policies.

Participant 3: Most of the time, from us the security team, this exercise is also based on metrics, which don't translate to results.

Other participants mentioned the costs of awareness programmes as a stumbling block:

Participant 12: Awareness efforts are not cheap, so it is important to ensure that they are as effective as possible, especially for SMEs where funding is a big problem.

Participant 4: Employees are generally not interested in security. They perceive the measures as a waste of time and burden and, therefore, seldom pay attention.

When asked about the importance of training and awareness policies:

Participant 5: Most highlighted risks of BYOD have one thing in common – employee awareness as a contributing factor.

What does an ideal training and awareness policy entail?

Participant 13: Rapid change in technology requires flexible and adaptive training and awareness policies – it must be adaptive and flexible.

Participant 5: Include regulatory requirements – like POPI.

Participant 8: [It] must also address unknown issues and include employee-owned devices – even “non- disclosed” devices.

The other interesting comments that were noted are:

Participant 6: There is no correlation between lack of awareness and overall spend on awareness programmes:

Participant 13: Organisations that are spending more don’t necessarily have more policy-compliant employees or fewer security issues when it comes to security issues.

4.5 Guidelines for developing training and awareness policies

From the questionnaire, when asked if the senior executives and business partners support training and awareness initiatives, the participants responded in the following way:

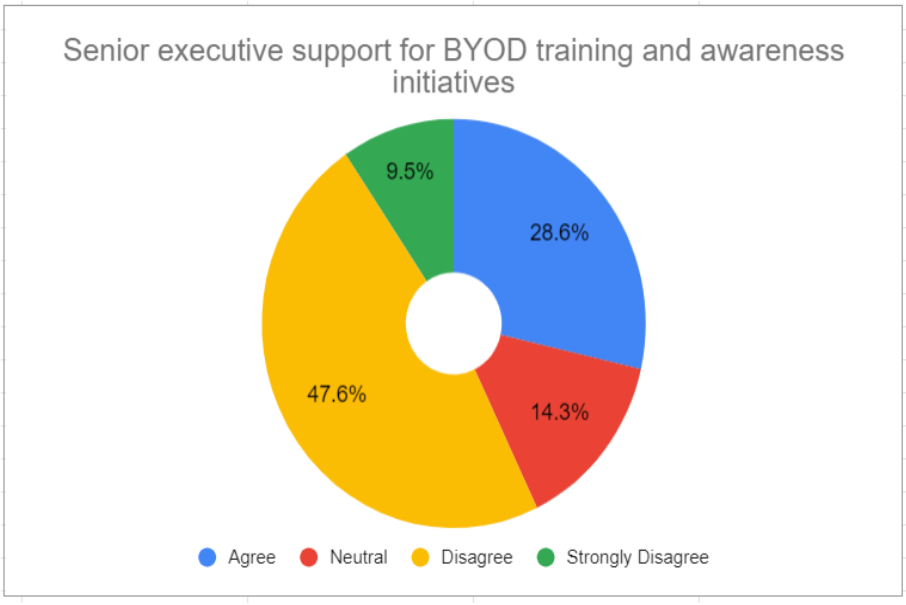


Figure 4-6: Senior executive support for BYOD training and awareness

The above responses show that lack or non-existence of support from senior executives might also be contributory to a lack of guidance and clear written guidelines for training and awareness policies. 57% of the participants mentioned that management was not interested. Only 28% of the participants confirmed that the management was supportive of the training and awareness initiatives and 15% of the participants were neutral. Below is what was noted from the interviews:

Participant 6: There are other pressing issues that management are facing, like growing the footprint and securing the next business deal. Security is not one of them, employees must do what they must do.

Participant 9: Funding is still an issue, management feels training and awareness or security, in general, is not contributing to the bigger picture and therefore doesn't get the necessary attention.

Participant 12: Hanging posters on all the wall about best practices for protecting your data and sending out emails have no impact on the end-user behaviours regarding security. If they want to make a real impact, they need to think about proper security training and awareness that entails full participation and devotion. It might be costly, but … data breaches [are] more costly. Web-based or self-paced training are also not efficient, I would suggest instructor-led workshops that are fully engaging, for better results and a much safer and more intuitive workforce.

Participant 4: This is due to a lack of ownership of the training and awareness programs and lack of policy, no one is pushing this initiative and escalating their importance to the management.

The participants answered the question about guidelines for training and awareness:

Do you have any guidelines that you follow for developing the training and awareness policy?

Participant 1: Most guidelines are available through a range of public web sites. Unfortunately, it is rarely appropriate, complete, or available in places that SMEs would think to look.

Participant 6: For most, guidance is adapted from big company practices that are not suited to SMEs.

A participant who was once employed by a big organisation noted:

Participant 9: Guidance for large enterprises tends to focus on policy, governance and comprehensive standards. Advice to SMEs, however, needs to convey arguments that will have an impact on the bottom line, as well as simple measures that address the most serious risks.

Participant 4 claimed that there were no guidelines available or being used in his/her organisation since BYOD security training and awareness level is so low:

Participant 4: There are no proper guidelines - except the templates we get from the internet.

To answer the research question about the guidelines for effective training and awareness policy, the following interview questions were also asked:

- Name 5 basic guidelines for security training and awareness policy.
- Highlight the 5 most critical points that should be included in the training and awareness policy**.**

Table 4-7: Guidelines for BYOD training and device policies

Guideline	**# of Times Mentioned**	**Addressed Challenge**
Prepare policies	12	• Clear written rules • Onboarding process
	4	• Ensure the policy is formally presented
Identify security “evangelists or ambassadors” in the business	11	• Highlight BYOD user responsibility
	11	• Involve the management and users in the planning

Create policies and audience-focused awareness efforts	9	• Access the organisation's culture regarding security and compliance
	12	• Tailor-made security and training programmes • Type of training and educational methodology
Identify the risky behaviours and assess their causes	9	• Highlight weaknesses
	9	• Covers against greatest possible threats
Track results and reiterate	12	• Monitor and allow enforcement and control
	8	• Tracking procedures
	6	• Keeping it flexible, scalable and consistent
	9	• Continuous feedback

Table 4-7 shows the results of both questions one and two, where the participants identified the list of noted guidelines and critical points when developing training and awareness policies. The above are categorised into 5 groups of criteria or relevant points, with BYOD training and awareness policy challenges being addressed. Some of these critical points were derived from the literature in the form of document analysis (BYOD training and awareness policies) as a pointer for classifying data in thematic analysis. There are some critical points which overlap between challenges, but it was kept in mind that the aim of the study is to develop the policy guidelines that can minimise the risks of BYOD security risks. For example, identifying the risky behaviours and assessing their causes will be a helpful exercise for any organisation, especially the SMEs. Before coming up with the training and awareness policy to address different kinds of risks, organisations need to educate their employees about the nature

and impact of such risks. After that, the critical points can then be paired with the challenges.

Participants pointed out that having guidelines helps to ensure that organisations do not create policies and end there, assuming they have done enough. This highlights the importance of monitoring and continuous feedback, as expressed below by different participants:

Participant 3: I would suggest that some organisations may be immature enough to believe that producing a policy document is enough to allow them to say, “You broke the rules”, or maybe “not our problem, we told you the rules, but you didn’t follow them”. As such, I think that the more mature organisation looks at the risk factors, and then decides how to develop and policy and how far to take policy. What is good policy for one organisation may turn out to be worthless in another due to that maturity level.

Participant 7 claimed that for some SMEs, the biggest challenge is the lack of time, as developing these policies takes time and knowledge.

Participant 7: In organisations where maybe, we are all busy on other things that are deemed more important, so getting all lined up to agree on policies may take an inordinately long time. I was at a conference recently where we were discussing these time constraints for conducting training and awareness in Small-Medium Business (SMB) organisations, as compared to the corporate governance provision in large organisations. As we go forward, I would suggest that we will see more networks of SMEs working together as the emerging business model, indeed our Government is driving more business through SMEs.

Participant 13: I would say have a policy – start somewhere, look at your organisation, the culture and the risk appetite and prioritise what’s important.

Participant 8: Awareness programmes require continuous feedback and updating.

4.6 Key elements for BYOD training and awareness policy

To fill the existing gap and understand the key elements to implement better training and awareness policies for safeguarding information and minimising BYOD security risks, the following questions were posed during the interview to end-users and security experts:

Highlight the key critical elements for a solid training and awareness policy.

Mention 5 key elements formulate a solid training and awareness policy.

To have an idea about which elements would tackle BYOD security policy challenges, the researcher collated the interview results. More elements were extracted from the interviews and different organisations' security awareness policies were also analysed. However, because there are many elements, only the ones which were mentioned by the participants were included. For an element to be included here, it had to have been mentioned more than once by the security experts and end-users. In the interviews, the participants were also asked to explain, in no order of importance, the challenges that specific elements would help to address. Thematic coding was used to analyse the data, with the end goal of classifying the relevant elements that could be included in the BYOD policy guidelines.

Table 4-8*:* Key Elements for BYOD training and awareness policy

Key Element	**# of Times Mentioned**	**Issue Addressed**
BYOD policies	11	To highlight all the BYOD policies needed and ensure they are also included and well referenced in the training and awareness policies
Device Access	9	Address the issues of unauthorised access who should have access to what system
Device Security:	9	• BYOD device password policy • Corporate Wi-Fi network security • Public Wi-Fi security • Lost or stolen device policies
Data Ownership	8	• Corporate and personal data on the device • Corporate and personal emails • Business contacts
Device Management	6	• Define MDM and its role • Explain MDM features
User responsibilities must be well defined when:	12	• Security updates • Logging onto networks

		• Performing software and application updates • Clicking on suspicious emails • Accessing organisational resources through their devices - cover VPN, emails, mobile apps like CRM.
Support and Maintenance	7	• Device support and software upgrades • Escalation process – for stolen or lost
Escalations	6	Reporting suspicious behaviours

According to the participants, training and awareness should be all about setting the right expectations for the employees and highlighting the acceptable cultural behaviour.

Participant 1 noted that it was important to include every threat and process and highlight and summarise their unique elements to the user, as shown in Table 4-8.

Participant 1: Training and awareness policy should be a bible for the other policies – it should highlight all the possible threats, all the available policies – including policy around device and data management, access management, device security and support. Ensure the user responsibility and acceptable behaviours are also highlighted. It is important for the user to understand the policies and their role in making BYOD secure.

The following were mentioned by security experts as key elements for training and awareness policy to minimise the risk of BYOD security risks:

Participant 5: It is important to spend a lot of time reaching out to employees, emphasising their role in protecting the organisation data and why that's important. Explain the reasons behind the other BYOD policies.

Participant 14: Employee education is important – ensuring that employees know about the policy and understand why it is important for them to implement security controls, requires education.

One participant noted that the elements will differ from industry to industry:

Participant 12: For this topic, one size will never fit all because our business and industries are so diverse. Government, banking, health care, manufacturing, online retail, all will have their own sets of standards, rules, laws, and circumstances as to BYOD training and awareness policy, even within the company boundaries. As such, the key elements that work for one may not be appropriate for all. That is why some of these often become so difficult because we are in diverse industries and geographies and what works for me may not be appropriate for you – the risk is the same, employee and client's information, financial and marketing information, patients and health information. It's all sensitive information that needs to be protected.

4.7 Summary

This chapter presented the main findings of the study, according to its relevance and rationale. First, the chapter revisited the aim of the study, before presenting the results of understanding the BYOD security risks and how training and awareness policies can be leveraged by SMEs to reduce the inherent risks. A summary of the findings about the BYOD security risks was presented, followed by the challenges SMEs face with regards to training and awareness policies in their organisations. Findings pertaining to the current measures used by SMEs were presented to illustrate how the organisations in this sector are using those measures, especially BYOD training and awareness policies. The chapter also assessed how SMEs present their concerns relating to the identified security measures. The researcher further presented the findings of critical elements that make up an efficient training and awareness policy.

Chapter 5 - Discussions

5.1 Introduction

This chapter combines both the results from interviews and questionnaires with the literature review findings. As noted in chapter this, the study is intended to answer four questions relating to BYOD and how training and awareness policies can be used to minimise the attendant security risks. The goal of this chapter is to answer the research questions by finding the commonalities and discrepancies between the three data sources, based on the analysis presented in chapter four. The research questions are as follows:

1. What risks are SMEs facing in their organisation?
2. What human factor-related risks are contributing to BYOD security risks?
3. What measures are currently being implemented and to what extent are they effective?
4. What are the key elements to formulate a solid training and awareness policy for SMEs?

Ultimately, the goal is to answer the research main/primary research question:

How can SMEs reduce security risks in their organisations using training and awareness policies?

From the reviewed literature, it is quite clear that SMEs need to embrace BYOD and to take full advantage of this initiative. SMEs do see the value of BYOD and its exceptional potential benefits for both employees and the enterprises themselves. On the other hand, it is also clear that security is a major concern for SMEs and big organisations affiliated with SMEs. From the interviews, the security experts predominantly agreed that BYOD security risks were a huge problem and highlighted their concerns about its human element. The problem that SMEs are facing is how to mitigate and minimise these risks. This is particularly true for South African SMEs. Initially, it was not clear if the employees and SMEs understood the risks and vulnerabilities that the BYOD initiative imposes and how to address the risks. This lack of clarity emanated from lack of evidence pertaining to whether or not SMEs officialise BYOD initiatives or leave it to employees to do as they like. Hence, the researcher set

to find out from the employees and the security experts, the BYOD risks that organisations are facing.

5.2 What risks are SMEs facing in their organisations?

Similar to the literature review, industry experts and employees mostly agree that SMEs are facing technological, human element, organisational and regulatory risks stemming from BYOD. Table 5-1 presents BYOD risks, and these are divided into four categories: technological, the human element, organisational and laws, and regulations.

Table 5-1: BYOD Risks

Category	Risks
Technological	• Data leakage • Phishing (malicious emails and links) • Device infections • WI-FI /Network
Human Element	• Weak passwords • Employee leaving with organization data when resigning • Data leakage • Stolen devices
Organisational	• Lack of user education • Lack of funding and support from management • Security culture • Lack of BYOD policies
Regulations and laws:	• Data regulations like POPI • Ethical use of data

5.2.1 Technological

From the interviews and questionnaire findings, the participants stated and agreed that technological risks were still a big challenge that SMEs needed to overcome. Employees still fell for malicious emails and were not able to spot unsafe WI-FI and

applications. The interviewees also highlighted phishing as one of the highest security risks that employees fall for by clicking or opening unsafe email files, which results in devices being infected. Most security experts mentioned that phishing in the form of email fraud is also quite high in SMEs because cybercriminals find it much easier to get someone to click on an email than to write a code and break into an organisation's network or system. Phishing is an email with an embedded link or some attachment that has a malicious code. It is argued that the highest email traffic malware rate was in the SMEs, with 1 out of 95 emails received containing malware (Symantec, 2017). This is an alarming rate and it shows how SMEs are vulnerable to security risks.

The use of unsafe WI-FI is more common WI-FI connection can be accessible from almost everywhere. Most establishments offer free WI-FI and because of the known data price issues in South Africa, people are always looking to bargain from free WI-FI, whether at the airport or restaurant. The only concern that most interviewees mentioned was that some of those WI-FI connections were not safe and employees would not know which ones were safe or unsafe. The survey results also confirmed that not only do most employees not know how to identify a safe or unsafe WI-FI spot, they also do not spend time to confirm this before connecting. This opens room for unethical activities, where hackers are able to eavesdrop, and steal information transmitted over these networks. Security experts agree that training and awareness policies would be valuable in highlighting these basic security activities that are needed to minimise the risks of BYOD and improve security culture in an organisation, helping employees to be more vigilant when using free WI-FI. All these efforts, when implemented correctly in the organisation's training and awareness policies will, in return, help employees be knowledgeable and empowered about the security risks of BYOD.

5.2.2 Organisational

From the interviews, most interviewees argued that only a few SMEs apply enough controls to safeguard their sensitive information while most have little or no access to security know-how and skills. This feeling is derived from the fact that SMEs do not have a budget or funding for security projects or expertise. Some interviewees indicated that lack of support from management also plays a role in the failure of training and awareness policies. Since management is very influential, their lack of support for funding security initiatives extremely limits the SMEs' ability to manage the

BYOD risks. The respondents unanimously agreed that this phenomenon was quite common in SMEs. This could be mitigated, however, by creating a common understanding of what BYOD means for individual SMEs and highlighting the roles and responsibility of each employee in the BYOD policies. BYOD training and awareness policy would basically serve as a point of reference whereby the benefits of the proposed policy would be presented to the key stakeholders, to show why the policies are important. Other participants cited the importance of defining what BYOD means for the organisation, and further argued that it is important to make it clear that BYOD is an enabler of some of the business outcomes and therefore more effort needs to be invested into making sure that the risks are managed. The participants further posited that the objective should be to highlight the importance of working with management and security experts to get to the level where the training and awareness policies are developed and fully adopted within an organisation. To make this possible, the participants recommended that the management and the employees of a given SME organisation should work as a team to drive one message.

For organisations that are still planning to adopt training and awareness policies, the long-term security goal should be to change the organisation's culture in favour of using BYOD in a safer manner. The ideal role of security experts is to safeguard all the organisation’s data and support technology initiatives like BYOD. For SMEs to reach this stage, security experts first need to do an assessment to understand the organisation’s maturity in terms of BYOD; security processes and tools in place; employee knowledge about BYOD; knowledge about security processes and technology; their needs in terms of training and awareness and lastly coordinate all the stakeholders in all different layers, including the management. The interviewees claimed that having this as a foundation prior to adopting BYOD puts the organisation in a better position as most of the time, lack of security policies and poor security culture contribute to the challenges that SMEs are facing today with BYOD. The costs of security risks are too heavy; thus, security managers need to communicate this using simple terms in order to get management buy-in for training and awareness policies to be prioritised. This would ultimately ensure that users pay more attention to securing their devices.

5.2.3 Human element

According to the interviewees, the human factor is the most common risk because of the nature of BYOD, which allows the employees take full ownership and control of their devices. The problem here is that there are no proper channels to communicate between security personnel and employees, and poor security culture in most organisations also intensifies the problem because security is not a priority for most employees. Some of the participants emphasised the importance of that communication link and how it needs to be improved. Walsh & Homan (2012) argue that as employees learn more within an organisation, their behaviour also adjusts to both their own needs and those of the organisation.

One interesting remark that was noted during the interviews is that employees expressed concern that they felt like they were being watched and that their privacy was being compromised. They argued that training and awareness policies could be more efficient if employees understood what the end goal of these policies was. The point that the interviewees were driving home was that companies come up with lots of policies that most of the time have organisations' best interests at heart. With BYOD, these policies need to be balanced through employee involvement because the device, in this case, belongs to employees. This shows that there is indeed a gap and misalignment between employees and security experts. Security experts and management need to communicate the importance of these policies clearly.

On the other hand, security experts who participated in the interviews also mentioned that somehow, employees are also resistant as, for some reason, they are inclined to regard security as someone else’s problem. Once the management, security experts and employees start working together, training and awareness policies can be developed much more easily. When all the alignment is done, they can focus on the needed technology measures and the different types of training methodologies that are suitable for the organisation.

The participants of the study also mentioned that bigger and more established organisations face similar training and awareness-related issues, but they still manage to make BYOD successfully work for them. All the security experts noted that what kept them up at night was what some of their employees might do wrong, rather than how good their security defences were. This shows that BYOD is the same for everyone. Human error is a top security risk for all organisations, but hackers target

SMEs more because of the issues mentioned above. The reason is evidently financial, as big organisations have means and processes to ensure that their employees are well educated and aware of the risks of BYOD. It should be noted that this does not mean well informed employees are not subjected to BYOD risks, but the risks diminish when security training and awareness become an ongoing process embedded at the core of organisational culture.

Other interviewees argued that they sometimes use posters and emails for awareness, but their efforts were not highly regarded. Sending ad hoc emails to users does not yield any positive results. If there were no alignment and training and awareness efforts targeted at specific needs and risks, this might be another fruitless exercise that wastes time and resources. In other words, training and awareness should be integrated in day to day activities and culture of the organisation. From when the new employees join the organisation and enrol their device for BYOD, there must be a process in place to take the new employee through the BYOD policies. This should also apply to organisations that have not officialised their policies. When the policy becomes official, all the employees must be given an opportunity to familiarise themselves with the new policy and ask questions, if needs be.

Again, the interviewees generally argued that due to funding constraints, it is difficult for SMEs to budget for some of the technological solutions to manage the risks. In addition to that, there is also lack of skilled security experts within SMEs, making it even harder to ensure that process and policies are in place. Despite all the funding and skills shortage, BYOD training and awareness policies are very essential for SMEs and they can be used to minimise the security breaches, even without deploying another technological measure (Harris *et al.*, 2013).

5.2.4 Regulations and laws

In the interviews, few participants mentioned that data regulations and laws like POPI were also a challenge for SMEs embracing BYOD. The ability to prevent company information from being compromised on the employees' mobile devices, while also being mindful of their privacy, requires necessary precautions. Since BYOD is about accessing company resources, including data on mobile devices, SMEs need to ensure that the data stored on employees' mobile devices are secure and protected. POPI places restrictions on how the organisation handles personal information. The challenge here is to ensure that the data on the employees' mobile devices are

protected. Besides the organisational data, BYOD imposes the risks of loss or breach of personal information for either clients or employees.

The legislation challenges SMEs to ensure that the data is protected. For SMEs, it is only through educating employees about the BYOD risks like phishing, data breach and device loss that this can be managed. Training and awareness policies do not only focus on the organisation's data and how to secure them, they also help organisations to be more transparent about how BYOD is beneficial for both employees and the organisation. This can be achieved by explaining the purpose and objectives of regulations like POPI and how they can ensure that employees do not feel like they are being watched but feel empowered instead. This is key to ensuring that there are fewer human errors and that the organisation's data are protected. This approach will improve how employees view security and how organisations approach this kind of regulation.

5.3 What human factor-related risks are contributing to BYOD security risks?

The human error-related risks in SMEs correspond to the human-related BYOD risks, as investigated in the literature view. Human errors are mistakes and skill-base errors that can even happen to the most experienced workers. The literature points out that almost half of the employees in every organisation recycle passwords for multiple logins, this is a clear case of compromised security. Credential theft is also a challenge as it is reported that most of the security incidents stem from the theft of credentials.

Nevertheless, one of the most interesting findings is that most employees in SMEs know about the security risks of BYOD and the dangers of not using passwords. This shows a clear inconsistency with literature, as most literature mentions that the users are not interested in securing their mobile devices and do not see the importance of putting any effort in ensuring that their devices are safe. Although employees pointed out that their frustrations with passwords are due to password lockouts, they also agreed that passwords do not provide robust enough security. From both employee and security expert standpoints, it seems clear that awareness and training are needed to emphasise the significance of passwords and how to manage them.

Another interesting finding from the interviews is that one of the biggest threats of BYOD is when employees leave an organisation with confidential data. This is due to

a lack of capability or process of ensuring that when an employee leaves the organisation, all the data on their devices are wiped. Employees end up leaving with, among others, strategic customer information which can be very harmful if it falls into wrong hands. SMEs need to look at technologies like mobile device management, which are useful for such scenarios or implement policies which stipulate that before employees leave the organisation, they need to check in with security experts to ensure that their devices are cleaned out of all the important information. Moreover, another thought-provoking finding from the participants is that they can pick up malicious activities or emails, but do not know where to report them as the processes are not clear. This shows that communication needs to improve between security experts and end-users. Participants mentioned that they also understood the two-factor authentication methodologies that they can apply to ensure that their devices are secure. Although some SMEs do not have password policy management, users understand the use of passwords and the importance of changing them from time to time. These policies need to be part of training and awareness policy to help organisations educate the users about the best practices of using passwords.

Other human element errors are theft and loss of device. Although some participants mentioned that they understood the process of contacting their mobile service provider to block the devices and use other useful functions like “locate my device” to track and trace their lost devices, they conceded that they did not know if their organisations had similar processes for such. It also emerged that in instances when employees suspected that their devices were being hacked, most could not detect the attempted compromise. Lack of policies and processes creates loopholes for hackers. SMEs need to have relevant remedial and preventive processes in place as well as educate their employees on what to do and who to contact from their organisation in case one of these unfortunate incidents happen. This can be done through training and awareness policies.

In terms of compliance, the interviewed employees said that they were unaware if there were any related policies in place. The employees also indicated that reaching out to security experts required a lot of time and effort, which is rather unfortunate as the former forego asking pertinent questions about BYOD. Thus, the majority of employees are not privy to otherwise readily available information which is critical for the growth of business and mitigation of security risks that pose a real threat to modern

enterprises. Meanwhile, security experts noted that employees really cannot be bothered. They also claimed that employees need to be reminded regularly to do the right thing. Security experts argued that their efforts to get employees to follow the rules were not working, as the process of making employees understand reasons to comply with security policies, was highly dependent on the understanding of the risk, as well as doing the right thing and being fully aware of what was at stake.

5.4 What measures are currently being implemented and to what extent are they effective?

Despite literature review and interviews showing that even companies that invest in technology can still suffer a security breach, most participants mentioned that SMEs could not afford security, while others did not think that they had much to worry about. Customer, employee and payments data are important. Not all security measures cost an arm and a leg. Investing in best practices is much cheaper as compared to technology and there is a lot of freely available information which can be used as a starting point. The security measures mentioned by SMEs security experts and end-users corresponds to the ones mentioned in the literature review

5.4.1 The use of passwords

A password is one of the most widely used mechanisms to protect devices. Any device that is enrolled for BYOD is more likely to contain sensitive organisation or customer information. Employees indicated that they understood the importance of using passwords to safeguard data located on their private mobile devices. This scenario presents organisations with some comfort to know that the devices are not a security threat. The literature review also asserts that in terms of mobile devices, passwords are not the only best way to secure devices, but they are also very easy to set up and can be used with other biometric authentication methods for the best solution. However, the most interesting finding is that most SMEs only solemnly rely on the use of hardware authentication as a primary means for security. From the interviews, security experts also cited their frustrations with password authentication and claimed they would abandon them if they could. They believe passwords are the weakest means of defence to rely on, especially when they are all one can offer in the age of BYOD. Although there is a lack of awareness around the importance of using passwords, they are the only measure that SMEs claimed to use more. This also shows that there is some discrepancy with the literature, as most of it shows that users do not

use passwords to protect their phones, but the interview findings pointed out that most SME employees use them and other device authentication methods more than other available technological solutions. This is also because these authentication methods come standard with the mobile device and cost nothing for the SMEs. Another interesting finding is that users understand the importance of using passwords on their mobile devices. From the SME side, including password management policies in the training and management policy will help to highlight the importance of passwords for BYOD and make employees aware of the specific policies and expectations from both the employee and the organisation.

5.4.2 Mobile device management

From the interview findings, it is interesting to know that SMEs can purchase customisable MDM solution with bare minimum capabilities**.** Some of the SMEs security experts mentioned that they did not have MDM yet. For those who claimed that they had it, they only implemented the minimum package, as it is quite a necessity. Participants also mentioned that they get a lot of push back from the employees, because the latter did not know what MDM does. The employees were thus reluctant to install MDM on their devices because they felt that the organisation was talking over their personal devices and watching everything that they did. But the question that one of the participants asked was: “How do you expect an employee to understand what this MDM does if you don’t explain its purpose and importance in a way that they will understand?” This also shows an incomplete process whereby organisations are also guilty of pushing this to employees without first talking to them about it.

MDM seems like a need and it is very expensive, but even with lack of funding, it is important to ensure that there are tools in place to support the mission so that all the basics are covered. Embracing BYOD means employees have all sorts of applications installed on their mobile devices. According to the interviewees, implementing MDM will be very critical for the SMEs and helpful to all parties involved. MDM gives back control to the organisation by guiding the employees on what is allowed on the mobile phone and providing visibility into the organisation in terms of who has access to the network and organisational resources. MDM blocks all the unsafe applications from accessing employees’ personal information and contacts. Not having MDM or receiving push back from employees allows unmonitored gadgets to access organisational information without knowing which other applications have access to

the same information. This' in a way, exposes organisational data to unknown risks. Employees' mindset can be changed through training and awareness policies. Highlighting these technologies and their significance in the policy would eliminate any misunderstanding that employees have about MDM.

5.4.3 Promoting security culture through training and awareness

The results of the survey support the assertion that promoting a security culture is one of the best ways to ensure that employees understand the BYOD security risks. Employees believe that if these security risks are a real concern for SMEs, then more must be done in terms of securing the mobile devices or at least training employees to follow the security recommendations from their organisations. This information is quite important for SMEs for two reasons. Firstly, once people understand why things must happen in a certain way, it gets easy for them to change their own behaviour for the best, and the change comes naturally because they would have understood the significance and outcome of the doing otherwise. Secondly, it is important to understand how employees perceive basic requirements of security like setting up a password on their devices and remembering to lock them after use. If this message is instilled from the onset or continually emphasised as a best practice and the right thing to do, in due course, it would become part of the organisational culture as employees start to understand why passwords are important and why recycling them is dangerous.

Interviewees also argued that BYOD was a very perplexing and complicated issue. An interesting comment made by the participants was that organisations assumed that people knew and understood the significance of simple actions like setting up a password and clicking on malicious links in emails, but some still do not use password and continue to click on dodgy links hence; fall for hacking tricks. Most of the interviewed experts mentioned that they conduct phishing simulations, but people still fell for scams and give away their private details. This shows that not everyone can identify a malicious email or link. For employees, doing work remotely using BYOD also means that they are more open to vulnerabilities and need to be more careful when receiving emails and sharing data.

The participants argued that it was only after a few phishing simulations that the results of the exercises began to show that people had understood. This proves that training and awareness must be an ongoing discipline in SMEs because doing it just once, in order to tick a box, has lots of disadvantages and does not promote the security culture

in any form. Some interviewees argued that the SMEs that raised awareness with their employees to be smarter both at work and home saw lots of change in employees' attitudes, thus showing the impact of sustained training and awareness programmes. Most organisations raise awareness by trying to concoct these attacks, so the employees do not fall for these traps. The participants argued that if companies engaged employees in training and awareness, they would see a 10% reduction in the number of staff members who click on the emails with a malicious links. The participant experts estimated that currently, 20% of SME organisations' employees are susceptible to clicking on malicious links.

Phishing simulators, mobile device management and password usage best practices, like encouraging the use of complex and different passwords across all the platforms, in addition to changing the passwords more frequently. These are great tools that minimise the BYOD security risks. When incorporated in training and awareness policies, this tool can be used to improve a cyber-hygiene culture that would promote and encourage the users to think before doing. It is through continuous training and awareness that employees would understand the different types of hacking, as well as how to spot an illegal website and link in an email. Cyber-hygiene culture is very simple and dependent on how an SME entity engages with its employees. The culture starts with understanding the nature of individual employees and how they behave on their devices. All this will help to promote a security culture, thus, ultimately minimising the risks and making it harder for data breaches to occur.

5.5 What are the key elements to formulate a solid training and awareness policy?

The interviewees argued that BYOD was a big thing for SMEs, and most could not function without it, thus, forcing the security experts to think about better processes to improve awareness and training on the security risks of BYOD. Some interviewees commented about not having access to tools and templates to get started, while others argued that nowadays there is a lot of information that can be easily accessible to build a good training and awareness policy. However, the interesting finding is that most participants also agreed that there was no standard process or procedure for coming up with effective policies. Several interviewees noted that employee-driven initiatives made it necessary for security experts to link training and awareness policies for BYOD with business objectives, so as to contain the costs of hacks and data breaches. The

experts further mentioned that it could be helpful to have a starting point that guides and serves as a model that can be used by SMEs, even those without in-house security skills. They believed this would be helpful as it eliminates likely excuses about lack of policies and support from management.

SMEs are encouraged to implement training and awareness policies and support these policies or face the security risks of BYOD imposed on their respective organisations. Interestingly, like literature, there is a similar opinion from the interviewees regarding the importance of coming up with key elements that cover the basics that must be at least be included in the training and awareness policy. The participant security experts believed that for SMEs to ensure the effectiveness and relevance of training and awareness policies, it was also important to have guidelines and ways to evaluate the policies regularly to ensure that they still serve the purpose or evaluate if they needed improvement.

Most of the interviewees also argued that senior management was not supportive of the training and awareness policies. To mitigate this, there was need for senior corporate executives to be fully furnished with information about hacks, data breaches and the impact of training and awareness, and how BYOD security was key to the success of the business. The interviewees emphasised on the importance of SMEs investing in broader and inclusive training and awareness competency and appropriate solutions for internal and external purposes. They also highlighted that the security culture needed to be taught from up bottom and management had to lead by example. Others argued that training and awareness policies were part of the solution to combat risks, but not the solution for BYOD security risk complexities. BYOD security experts and other interviewees cited the importance of rethinking what BYOD means for the organisation and prioritising the basic needs first because BYOD means different things to different people. Interestingly, they also advocated making this information part of training and awareness so that everyone would be on the same page.

The security experts may have different views on what a BYOD training and awareness policy should entail and how the whole process should be treated. According to the literature analysis, the interviews, questionnaire findings and reviewed training and awareness policies, the following are the key elements for BYOD training and awareness policy. Listed below are the most important guidelines that needs to be

taken into consideration when developing training and awareness policies to minimise BYOD security risks:

i. Define BYOD for your organisation – the enterprise cannot apply appropriate controls before understanding how employees are using mobile technology. In addition, the enterprise should carry out a risk assessment to ascertain if there are any privacy issues.

ii. Define the onboarding process for BYOD – the interviewees mentioned the importance of having clear written rules that guide the enrolment of BYOD or new employees that join the organisation. This will help the employers and the employees to develop the knowledge and behaviours to become effective users of BYOD.

iii. BYOD devices – it has been noted that it is important to provide a description of which devices will be accepted and included in BYOD, taking into consideration support and maintenance. There is need to ensure that this information is well documented and highlighted in the policy.

iv. Define the BYOD policies – BYOD has other different pieces of policies that make part of the training and awareness policy. Data ownership, password and device management policies help to guide and protect the organisations, and these are part of the training and awareness policy. The interviewees argued that it was crucial to define and include the above-mentioned policies in the training and awareness policy, as a point of reference and guidance on how employees should manage and handle their devices and data.

v. Responsibilities – the interviewees and literature reviews emphasised the importance of highlighting what is expected from all the stakeholders; that is, from management to the end-user, to ensure that the employees and managers understood their roles and expectations.

vi. Highlight weaknesses – several interviewees agreed that the aim of the training and awareness policies was to create awareness of the risks of BYOD. It is important to ensure that the training and awareness policy covers against greatest possible threats and risks and encourages the use of best practices and tools available to help combat risks of BYOD.

vii. Tailor the security and training – the interviewees argued that training and awareness policies should start and end with the employee in mind. It is important for business entities to understand their employees and identify the types of training and awareness methodologies like Web, instructor-led or workshops, that would be suitable for their needs. From the literature, there are lots of guidance and discussions around which methodology works best. However, the most important thing is that respective SMEs need to find methodologies that work best for them, keeping in mind the budget and funding part. the interviewees also mentioned that SMEs tended to make decisions that were beyond budget and ended up not following through with the plans because they would have been unrealistic from the beginning.

viii. Allow enforcement and control – to keep the employees in check, the interviewees highlighted that it was important to include ways to exercise control and ensure that employees comply with policies and highlight the rewards for those who would respect the policies.

ix. Escalation process – according to the interviewees, most SMEs do not have processes or ways of reporting BYOD related issues when they happen. Employees lose devices and replace them without even mentioning it to the IT department. Lack of policies and governance allows for such to happen. Including important information about where to go for assistance and enquiries in case of emergency would be very helpful.

x. Ensure the policy is formally approved and official – it is one thing to have a policy and another thing to have it officialised. Security experts mentioned the importance of getting an approval signature to officialise the policy and make a copy of the policy available for people to access and understand it.

xi. Scalable, flexible and consistent – because technology and business needs change, the interviewees argued that this policy would also need to be scalable for changing business needs and technology.

xii. Monitoring and tracking procedures – these should be instituted in order to allow for stakeholder feedback and make room for continuous improvement.

5.6 Summary

This chapter discussed the findings based on the security experts and employees' opinions about BYOD security risks and training and awareness policy and these were linked with the literature review, in order to answer research sub-questions. These sub-questions ultimately answered the main research question. SMEs are well aware of the BYOD security risks and know what they need to do. Employees, on the other hand, understand the risks, but also believe SMEs could do more to get employees more engaged in such policies because they own the devices. It is clear that there has to be a handshake between two parties for BYOD to be a success, as all the mentioned risks are dependent on both parties doing the right thing.

Organisations need to have proper adoption plans for BYOD, communicate them with all the stakeholders, including employees, and set the right expectations in terms of security and individual responsibility to ensure that they are not exposed to any risks. The security experts agreed that the human element was quite a big challenge because the employees owned the devices and were in control of them. The SMEs security experts believed that employees needed to be at the centre of training and awareness policies. Password, data access and distributions, public WI-FI, lost or stolen devices, phishing and malware all needed to be included in the training and awareness policies as these were risks related to human error.

There are other technical measures that can also be implemented to enhance security for BYOD; some are available at a cost and others are free. The SMEs experts agreed that they needed to make a call and include these technology measures in their training and awareness policies to ensure that employees were aware of the technologies and understood the processes to follow when things go wrong. The experts agreed that promoting the use of a strong password and exercising caution when using public WI-FI, reporting malicious emails and activities on their phones and reporting stolen phones were key security activities employees could do to ensure a more secure BYOD programme. The employees emphasised and agreed that there needed to be clear and open communication channels between employees and security experts, which would improve the situation immensely.

Chapter 6 - Conclusion and Recommendations

6.1 Introduction

This chapter summarises the findings and highlights the answers to the research question. The chapter also provides a conclusion and recommendations based on the work done in the previous chapters. The aim of the study is to answer the question about how SMEs can reduce security risks in their organisations using training and awareness policies. In order to attain this, the researcher conducted a literature review to understand and learn more about this topic and what has been written so far by other researchers. This was followed by interviews and surveys to get a better understanding of the security risks of BYOD; the measures currently available; the challenges SMEs are facing with developing training and awareness policies. All the possible BYOD security risks and training and awareness challenges were discussed.

6.2 Conclusion

The empirical investigations confirm that the challenges that SMEs are facing about BYOD security and training awareness stem from a range of interrelated issues, starting from high up in the organisation to the employees at the bottom. From the organisational level, lack of support from management limits the ability for SMEs to develop and implement BYOD training and security policies. BYOD security risk is not considered a big issue in SMEs, hence lack of support and resistance from management. Awareness and training are very important to cultivate a culture change, so if there is no support and push from the management, it is unlikely that employees and security experts will try harder from their end. In addition to this, the support from management also gives employees some form of official approval and authority in terms of BYOD usage. This means that when there is support from the management in favour of BYOD training and awareness policy, the security experts and employees will also come to the party.

Furthermore, for SMEs who have training and awareness policies, it looks like the policies have been created without assessing whether they fit in the organisation, as most of them have been adapted and customised from the internet. In addition to that, a lack of understanding of what BYOD means for one’s organisation and collaboration between different stakeholders makes the matter even worse.

Literature analysis and interview and questionnaire findings all corroborate that SMEs face many complex challenges related to BYOD. SMEs in South Africa are made up

of different industries like information technology, manufacturing, agriculture, infrastructure, tourism and construction and many more. It is advised that externally and internally, SMEs have to come together with their employees and security experts to create policies that are specific to SMEs, in order to make the policies more effective. However, each SME has different priorities, and this affects the likelihood of future collaboration. Henceforth, each SME used or follow its own guidelines. Internally, SMEs have not made any effort to promote the security culture and awareness or use of best practices and guidelines for safer and controlled BYOD and this has, over time, made the situation even more costly and riskier. South African SMEs also face the protection and privacy of information regulation, which applies to all the organisations doing business in South Africa. This regulation is mainly to safeguard employees and clients' information, which subsequently demands that SMEs do enough work from their end to ensure that the information is protected.

After all these challenges were identified, the current measures used in SMEs were analysed to determine they how they implemented the training and security policies to solve these problems. The results of the study show that most SMEs have not implemented formal policies, as they rely on device authentication as the sole means for security. From the findings, it is evident that the BYOD security risks originate from the human element, technological and organisational levels. From these findings, it is apparent that focusing on a single level may result in a distorted awareness and training policy. It can be argued that the training and awareness policy alone is not effective for minimising or mitigating these risks, therefore, a combination of all the technical measures is required. Training and awareness policies are becoming popular and interoperable with other measures. They also come highly recommended, as most of the security risks are human error related. Both technology and culture-related challenges can be addressed through training and awareness strategies.

Technology is primarily used in big organisations that can afford to spend money on security and have a good track record for efficiency when used correctly. The participants of the study stated that, without training and awareness, technology alone is not enough and, from the literature review there was a clear discrepancy regarding technology and its ability to minimise the BYOD security risks. This is noteworthy, considering that the finding shows that the biggest security risk for BYOD is human

error. Another interesting element was that lack of interest from users or employees was also contributing to the security risks of BYOD.

As presented above, literature and findings substantiate that training and awareness policies can minimise the BYOD security risk. SMEs experts also agree that it could be beneficial to establish easy-to-use, adaptable training and awareness policies, processes and resources specifically for SMEs to adapt when developing and implementing these policies, as the issues raised here are related to time, budgets and expertise.

Evidently, training and awareness policies can be used in conjunction with technology to promote security culture. In addition, from the findings, most participants mentioned that they did not have proper training and awareness policies and, for those who had, they used Google templates for guidance on developing the training and awareness policy. This proves that guidelines for developing training and awareness policies help SMEs to reduce the BYOD security risks and subsequently save time and money. Because there is no one-size-fits-all solution, the following fundamentals are required for developing proper guideline policies:

i. SMEs must know where to go to find appropriate advice.

ii. The provided advice must be compelling and relevant to their circumstances.

iii. There must be a clear route for taking further action.

From the literature review and interviews, the following common challenges, as presented in Table 6-1, were also noted.

Table 6-1: Common challenges and recommended actions for BYOD security training and awareness policies

Challenge	**Recommended action to address the challenge**
Lack of management support The IT management team does not understand or clearly communicate the	**Define Clear Owners for Planning** Involve management as early as possible for accountability to develop training and

expectations of training and awareness policies.	awareness policies and coordinate with other teams, including the employees.
Poor Planning Training and awareness policies are not coordinated with the organisation risks, plans and employees.	**Involve key decision-makers** Follow guidelines and decide on the impact your policy should make and key deliverables for awareness and training policy to avoid lack of direction and purpose.
Lack of Communication Security experts do not communicate expectations and requirements to employees	**Communicate Often** Communicate early and often to employees and other stakeholders as plans evolve.

Through the insights gained from the literature and interviews about the challenges of developing BYOD security risk and training and awareness policies, the researcher has come up with a recommendation to overcome problems and succeed in developing training and awareness policies, as depicted in Table 6-2 below.

Table 6-2: Process for developing training and awareness policy

Phase	**Step**
Planning	1. Plan the process of developing BYOD training and awareness policy.
Develop	2. Involve the key stakeholders. 3. Determine principles and approaches. 4. Gather all relevant data from both management and employees. 5. Develop and communicate the policy.
Monitor	6. Monitor and evaluate the progress and results.

For this process, 8 key elements were identified, as components of BYOD training and awareness policy to facilitate the solution. These elements play a significant role and

form part of the process to address the BYOD security challenges. First, it is important to define what BYOD training and awareness policy means for one's organisation. The enterprise cannot apply appropriate controls before understanding how its employees are using mobile technology, thus, there is need to start by taking a risk assessment to ascertain if there are any potential hazards. This will also help to get a buy-in from the stakeholders, as well as highlight why BYOD is important for the organisation. It is also pertinent to explain how the training and awareness policy will transform the organisation's culture and minimise security risks in the long term.

Second, the onboarding process for BYOD must be defined with clear written rules. In order to achieve this, it is important to work closely with management and end-users at different levels in the organisation and agree on what is acceptable and unacceptable behaviour. Third, acceptable and unacceptable devices should be described. The fourth step entails defining the BYOD policies pertaining to devices, data ownership, privacy and passwords. Fifth, there is need to ensure that the employees and management understand their roles and responsibilities. The sixth stage involves highlighting all weaknesses and possible threats or risks.

Seventh, the security and training must then be tailored to the type of training and educational methodology that are suitable for the organisation. The chosen methodology should make allowance for enforcement and control. In this way, the training and awareness policy efforts will address the challenges that the organisation faces, instead of just generalising.

Eighth, escalation processes should be included so that users know where to go for assistance. Step number nine entails taking measures for ensuring that the policy is formally presented and accepted. The tenth stage should take into consideration monitoring and tracking procedures to allow for feedback for continuous improvement. Eleventh, checks and measures should be made to ensure that scalability and flexibility considerations, which are key to the process, are factored in. It is important to ensure that the policy is scalable and flexible for changing business needs and technology. Lastly, all decisions and guidelines should be communicated to all stakeholders. Visuals may be used to engage with the stakeholders and management, thus effectively drive the message home.

From the interviews, there were different opinions pertaining to training and awareness policies and how they should be tailored to increase their effectiveness in SMEs. It can be argued that training and awareness policies should indeed be tailor-made for specific SMEs, as their effectiveness mainly depends on the organisation's requirements and culture. Some participants were neutral about the issue of tailor-made policies, but most argued that they could potentially be a value add. Other participants were happy to have sets of steps to follow as guidelines, rather than downloading templates that are also adopted by big organisations, which are half the time not entirely applicable to SMEs. Most participants stated that an inclusive training and awareness policy would be an optimal solution to change management perspective and improve the organisation's security culture.

6.3 Recommendations

In light of the results, the optimal way to use training and awareness policies to minimise BYOD security risks is to implement a structured approach that uses the specific elements mentioned above. These elements, which are outlined in figure 6-1 below, provide a roadmap of how training and awareness policies can be developed to combat the BYOD security risks. These guidelines are desired to ensure that training and awareness policies are as effective as possible. As already mentioned, this general approach is by no means exhaustive and depends on the organisation's BYOD priorities and needs. As other participants argued that one size did not fit all with BYOD policies, this report does not claim that there is only one approach or answer to the main research question, but it only acts as a guideline for SMEs in ideal situations that require the use of training and security awareness policies to effectively minimise the BYOD security risks. Practically, these guidelines would depend on a specific SME and its challenges.

With regards to training and security awareness being an effective way of generally minimising the BYOD security risks, using training and security awareness policies could potentially be effective because security culture is driven by habits. As much as organisations use technology to provide security, it should be noted that technology cannot compensate for lack of knowledge and poor security culture and security training and awareness. When done correctly, training and security awareness policies and programmes can help to change user behaviour and improve the security culture. Generally, this report also recommends that SMEs should involve

users as early as possible and make them the centre of training and security awareness policies, not just for accountability but for policies that are targeted and relevant. Such practices can effectively minimise BYOD security risks.

The essentials mentioned below, will be helpful for SMEs, as checkpoint to ensure that the basic necessities for BYOD security are catered for in the training and security awareness policies:

Figure 6-1: Essentials of BYOD training and awareness policy

The guidelines stipulated in figure 6-2 will help SMEs in the following ways:

i. Training and awareness improvements efforts can be more structured and targeted at little or no cost.

ii. Knowing what the training and awareness policy needs to cover would help SMEs with structuring the messages and communications of the campaigns.

iii. Having guidelines will help ensure that the basics are covered and may yield awareness and positive results.

iv. Guidelines can also serve as a starting point to benchmark one's organisation against its peers.

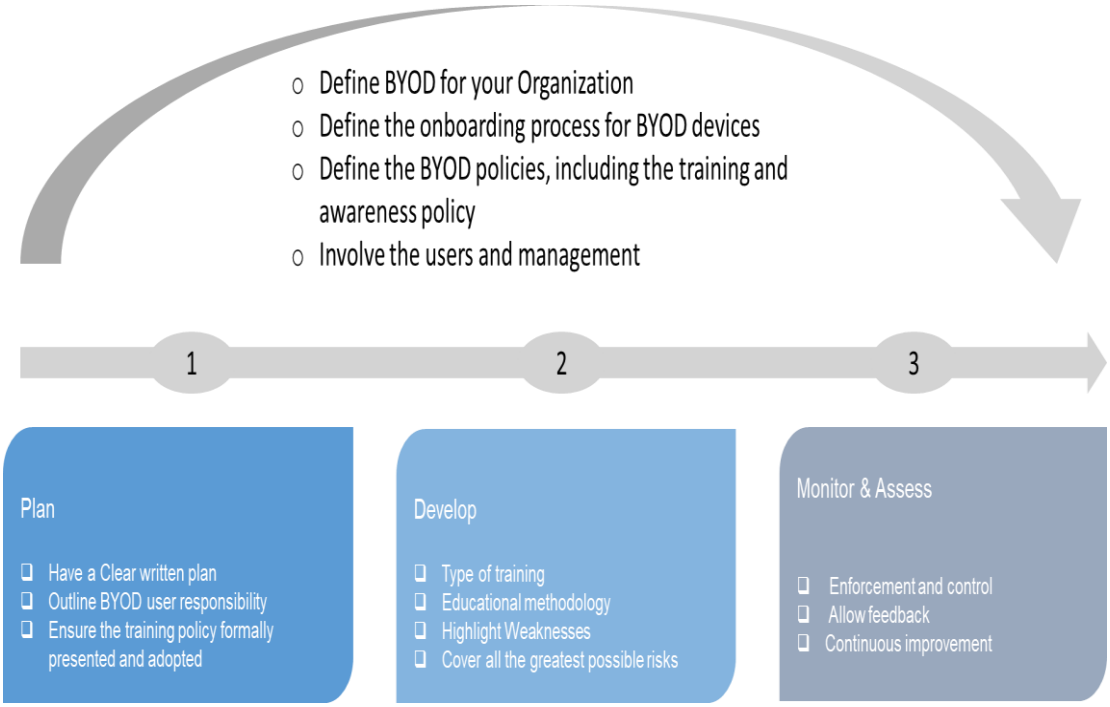


Figure 6-2: BYOD Training and awareness policy guidelines

6.4 Limitations of the study

The aim of this study was to develop the guidelines for training and awareness polices, specifically for SMEs. Hence the outcome can be generalised to a certain degree to all the SMEs in South Africa. Given that technology changes so quickly, some sections of this report are strictly for BYOD security risks only. There are two main reasons the research focused on SMEs. First, most of the big organisations understand BYOD and have budgets for implementing procedures and policies for training and awareness. Furthermore, keeping in mind that most SMEs do not consider budgets for technology and security as top priorities, adopting a well-structured training and awareness policy is thus a beneficial need for organisations in this sector. The researcher also found it relatively simpler to access information from SME security experts, as opposed to their counterparts from big organisations.

6.5 Recommendations for future studies

This report took a generic approach to explore how training and awareness policies can effectively minimise the BYOD security risks. This study asserts that BYOD will still grow and add value to SMEs. The study also shows that most SMEs do not have formalised training and awareness policies or guidelines as to what an ideal policy should entail. From this study, the researcher also discovered that SMEs have their own different challenges, in terms of training and awareness. For some SMEs, these training and awareness policies are non-existent. For those who claim to have them, they are not significantly effective and can still be improved. Due to time and budgetary limitations, this study was only focused on SMEs. For future studies, it could be ideal to take into consideration all the SME stakeholders. To advance this study, future research could be conducted to practically implement these elements to determine their effectiveness in SMEs.

Furthermore, this study revealed that too often most organisations spend a lot of time on technology, but not enough on people and processes. This would be another element that needs to be investigated further. Aside from this, experts also raised a concern that having a training and awareness policy does not guarantee fewer security risks. It would also be beneficial to investigate the impact before and after developing the training and awareness policy following the guidelines. Also, it could be interesting to investigate the lack of urgency among SMEs leaders to address BYOD security risks, particularly training and awareness issues. In conclusion, the risks, elements, and guidelines could be further advanced into a tailor-made training and awareness policy for SMEs, through applying these guidelines in practice by developing an actual policy following these guidelines for SMEs.

6.6 Summary

This chapter concludes the study and presents recommendations based on the findings and discussions from previous chapters. It presented recommendations for challenges SMEs face when developing training and awareness policies using step by step processes and, lastly, the key elements to include in the training and awareness policy to ensure efficiency and guidelines to follow when developing the policies. The chapter further discusses the limitations of this study and make recommendations for future studies.

References

Abawajy, J. 2014.User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237-248.

Abor, J. & Quartey, P. 2010. Issues in SME Development in Ghana and South Africa

Absalom, R. 2012. International data privacy legislation review: A guide for BYOD policies. *Ovum Consulting, IT006*, 234:3-5.

Accenture. 2018. Build pervasive cyber resilience now - Securing South Africa's Future Enterprise Today. https://www.accenture.com/_acnmedia/PDF-99/Accenture-Cyber-Resilience-South-Africa-POV-3.pdf

Adclick Africa Media Group. 2019. 2018/2019 SME South Africa's SME landscape survey results. https://www.bizcommunity.com/Article/196/713/184864.html

Adedolapo, A.A. 2016. Bring Your Own Device (BYOD) Adoption in South African SMEs.

Ademujimi, A. 2013. Social Media Sites as a Security Risk to SMEs. *IS Practices for SME Success Series*:7.

Akin-Adetoro, A. & Kabanda, S. 2015. Contextualizing BYOD in SMEs in developing countries.

Akin-Adetoro, A. & Kabanda, S. 2015b. Contextualizing BYOD in SMEs in developing countries*. Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists organised by: ACM. p. 3.*

Albrechtsen, E. 2007. A qualitative study of users' view on information security. *Computers and Security*: 276-289.

Albrechtsen, E. & Hovden, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. *An intervention study. Computers & Security, 29:432-445*.

Ali, S., Qureshi, M.N. & Abbasi, A.G. 2015. Analysis of BYOD security frameworks. I*nformation Assurance and Cyber Security (CIACS). Conference on organised by: IEEE. p. 56-61*.

Alvesson, M. & Sklödberg, K. 2008. Reflexive methodology : new vistas for qualitative research. Los Angeles: Sage.

Anney, V.N. 2014.Ensuring the Quality of the Findings of Qualitative Research: Looking at Trustworthiness Criteria

Armando, A., Costa, G. & Merlo, A. 2013. Bring your own device, securely. *Proceedings of the 28th Annual ACM Symposium on Applied Computing organised by: ACM. p. 1852-1858*.

Astani, M., Ready, K. & Tessema, M. 2013. BYOD issues and strategies in organizations. *Issues in Information Systems*, 14(2).

Ayoade, A. 2016. BYOD: The security risks of mobile devices.

Bajpai, N. 2011. Business Research Methods.

Bann, L.L., Singh, M.M. & Samsudin, A. 2015.Trusted security policies for tackling advanced persistent threat via spear phishing in byod environment. *Procedia Computer Science*, 72:129-136.

Beckett, P. 2014. BYOD–popular and problematic. *Network Security*, 2014(9):7-9.

Bell, E., Kothiyal, N. & Willmott, H. 2017. Methodology-as-Technique and the Meaning of Rigour in Globalized Management Research. *BJOM British Journal of Management*, 28(3):534-550.

Bell, M. 2013. Considerations when implementing a BYOD strategy. *IS Practices for SME Success Series*, 1(1).

Bennett, L. & Tucker, H. 2012. Bring your own device. *ITNow*, 54(1):24-25.

Blaikie, N.W.H. 2009. *(In* Blaikie, N.W.H., *ed.* Designing social research: the logic of anticipation. 2nd ed ed. Cambridge: Polity.

Bogdan, R. & Biklen, S.K. 2007. Qualitative research for education : an introduction to theory and methods. Boston: Pearson/Allyn and Bacon.

Botha, J., Csir, D., Eloff, M. & Swart, I. 2015. The Effects of the PoPI Act on Small and Medium Enterprises in South Africa.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77-101.

Brodin, M. 2017. Security strategies for managing mobile devices in SMEs.

Bruyn, M.d. 2014. TheProtection Of Personal Information POPI Act.

Bryman, A. 2012. Social research methods. Oxford; New York: Oxford University Press.

Burrell, G. & Morgan, G. 2019. Sociological paradigms and organisational analysis : elements of the sociology of corporate life.

Byol, K.E., Joohyung, O. & Chaete, I. 2014. A Study on Security Threats and Dynamic.

Caldwell, C., Zeltmann, S. & Griffin, K. 2012. BYOD (Bring Your Own Device).

Chang, J.M., Ho, P.-C. & Chang, T.-C. 2014. Securing byod. *IT Professional*, 16(5):9-11.

Chen, H., Li, J., Hoang, T. & Lou, X. 2013. Security challenges of BYOD: a security education, training and awareness perspective.

Creswell, J.W. 2014. Research design : qualitative, quantitative, and mixed method approaches. Los Angeles: Sage.

Crossler, R.E., Long, J.H., Loraas, T.M. & Trinkle, B.S. 2014. Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, 28(1):209-226.

D'Arcy, J., Hovav, A. & Galletta, D. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1):79-98.

Damopoulos, D., Kambourakis, G., Gritzalis, S. & Park, S.O. 2014. Exposing mobile malware from the inside (or what is your mobile app really doing?). *Peer-to-Peer Networking and Applications*, 7(4):687-697.

Dang, D.P., Pittayachawan, S. & Nkhoma, M.Z. 2013. Contextual difference and intention to perform information security behaviours against malware in a BYOD environment: A protection motivation theory approach. Australasian Conference on Information Systems (ACIS) organised by. p. 4-6).

de las Cuevas, P., Mora, A., Merelo, J.J., Castillo, P.A., Garcia-Sanchez, P. & Fernandez-Ares, A. 2015. Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications*, 68:83-95.

Dedeche, A., Liu, F., Le, M. & Lajami, S. 2013. Emergent BYOD security challenges and mitigation strategy.

South African Department of Trade and Industry. 2018. Annual review of small business in South Africa.

Dingwayo, M. & Kabanda, S. 2017a. BRING YOUR OWN DEVICE (BYOD) AND INFORMATION PRIVACY COMPLIANCE IN SOUTH AFRICAN ORGANIZATIONS.

Dingwayo, M. & Kabanda, S. 2017. BRING YOUR OWN DEVICE (BYOD) and information privacy compliance in south african organizations.

Downer, K. & Bhattacharya, M. 2015. BYOD security: A new business challenge. SmartCity/SocialCom/SustainCom (SmartCity). International Conference IEEE. p. 1128-1133.

Ellis, L., Saret, J. & Weed, P. 2012. BYOD: From company-issued to employee-owned devices.

Eschelbeck, G. & Schwartzberg, D. 2013. BYOD risks and rewards. *How to keep employee smartphones, laptops and tablets secure*.

French, A.M., Chengqi, G. & Shim, J.P. 2014. Current Status, Issues, and Future of Bring Your Own Device (BYOD).

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

Frumento, E., Freschi, F., Andreoletti, D. & Consoli, A. 2017. Victim Communication Stack (VCS): A flexible model to select the Human Attack Vector. Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM. p. 50.

Furnell, S., Gennatou, M. & Dowland, P. 2002. A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5/6):352-357.

Galliers, R. & Land, F. 1987. Choosing appropriate information systems research methodologies. *Communications of the ACM*, 30:901-902.

Garba, A.B., Armarego, J., Murray, D. & Kenworthy, W.2015. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information privacy and security*, 11(1):38-54.

Gartner. 2018. Implement Mobile Print Solutions to Reduce Security Risks and Drive Productivity. https://www.gartner.com/document/3879165

Gessner, D., Girao, J., Karame, G. & Li, W. 2013. Towards a user-friendly security-enhancing BYOD solution.

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

Gladyng, C. 2013. Can it harm your business. 31-34.

Grljevic, O., Bosnjak, Z. & Mekovec, R. 2011. Privacy preserving in data mining-Experimental research on SMEs data. (*In*. 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics organised by: IEEE. p. 477-481).

Guba, E.G. 1990. The Paradigm Dialog: SAGE Publications.

Hallebone, E. & Priest, J. 2009. Business and management research : paradigms & practices.

Harris, M., Patten, K., Regan, E. & Fjermestad, J. 2012. Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility? In 18th Americas Conference on Information Systems (Seattle, Washington, USA, August 9- 11, 2012).

Harris, M.A. Patten, K. & Regan, E. 2013. The need for BYOD mobile device security awareness and training.

Harris, M.A. & Patten, K.P. 2014. Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management and Computer Security, 22, 1, 97-114.*

Hovav, A. & Putri, F.F. 2016. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, 32:35-49.

Intel. 2011. Best Practices for Enabling Employee-owned Smart Phones in the Enterprise.https://www.intel.com/content/dam/www/public/us/en/documents/best-practices/enabling-employee-owned-smart-phones-in-the-enterprise.pdf

Jasek, R. & Sarga, L. 2014. Human Factor: The Weakest Link of Security? (*In*. European Conference on Cyber Warfare and Security organised by: Academic Conferences International Limited. p. 317).

Johnson, D.B. & Maltz, D. 1996. Mobile computing: Kluwer academic publishers Dordrecht.

Kabanda, S. & Brown, I. 2014a. Bring-your-own-device (BYOD) practices in SMEs in developing countries–the case of Tanzania.

Kabanda, S. & Brown, I. 2014b. Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries –The Case of Tanzania. *25th Australian Conference on Information Systems (Auckland, New Zealand, December 8 -10, 2014).*

Kadena, E. & Kovacs, T. 2017. The need for byod security strategy. *Hadmérnök*, 12(4).

Karr, C. 2015. Endpoint protection attitudes and trends. Cupertino:Bromiun, 2015

Katsikas, S.K. 2000. Health care management and information systems security: awareness, training or education? *International journal of medical informatics, 60(2):129-135.*

Kendall, K. & McMillan, C. 2007. Practical malware analysis*. Black Hat Conference, USA organised by. p. 10.*

Ketel, M. & Shumate, T. 2015. Bring your own device: security technologies*. South East Con. IEEE. p. 1-7.*

Keyes, J. 2016. Bring your own devices (BYOD) survival guide: *Auerbach Publications*.

Kirk, J. & Miller, M.L. 1986. Reliability and validity in qualitative research. *Beverly Hills: Sage Publications.*

Knapp, K.J. & Ferrante, C.J. 2012. Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*, 13(5):66-80.

Koh, E.B., Oh, J. & Im, C. 2014. A study on security threats and dynamic access control technology for BYOD, smart-work environment*. Proceedings of the International MultiConference of Engineers and Computer Scientists organised by. p. 1-6.*

Kongolo, M. 2010. Job creation versus job shedding and the role of SMEs in economic development.

Korstjens, I. & Moser, A. 2018. Practical guidance to qualitative research.

European Journal of General Practice, Volume 24 120 - 124

Krefting, L. 1991. Rigor in Qualitative Research: *The Assessment of Trustworthiness.*

Kruger, H.A. & Kearney, W.D. 2006. A prototype for assessing information security awareness. *Computers & security, 25(4):289-296*.

Kumar, R. & Singh, H. 2015. A proactive procedure to mitigate the BYOD risks on the security of an information system. *ACM SIGSOFT Software Engineering Notes*, *40(1):1-4.*

Kuhns, E. & Martorana, S.V. 1982. Qualitative methods for institutional research.

Kurpjuhn, T. 2015. The SME security challenge. *Computer Fraud & Security*, 2015(3):5-7.

Kvale, S. 1989. Issues of Validity in Qualitative Research.

Lapan, S.D., Quartaroli, M.T. & Riemer, F.J.2012.Qualitative research : An introduction to methods and designs.

Leavitt, N. 2013. Today's mobile security requires a new approach. *Computer*, 46(11):16-19.

Leclercq-Vandelannoitte, A. 2015. Managing BYOD: How do organizations incorporate user-driven IT innovations? *Information Technology & People*, 28(1):2-33.

Lennon, R. 2012. Changing user attitudes to security in bring your own device (BYOD) & the cloud. Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania organised by: IEEE. p. 49-52.

Liginlal, D., Sim, I. & Khansa, L. 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *computers & security*, 28(3-4):215-228.

Lincoln, Y.S. & Guba, E.G. 1985. Naturalistic Inquiry.

Lydon, E. 2014. The Benefits and Threats of BYOD in a SME Enterprise: A Systematic Literature Review.

Markelj, B. & Bernik, I. 2012. Mobile devices and corporate data security. *International Journal of Education and Information Technologies*, 6:97-104.

Marshall, C. & Rossman, G.B. 1995. Designing qualitative research. Inglaterra: Thousand Oaks.

Marshall,C. & Rossman, G.B. 2006. Designing qualitative research. *Thousands Oaks, Calif: Sage Publications.*

McCoy, C. & Fowler, R.T. 2004. You are the key to security: establishing a successful security awareness program. *Proceedings of the 32nd annual ACM SIGUCCS conference on User services organised by: ACM. p. 346-349*.

McCrohan, K.F., Engel, K. & Harvey, J.W. 2010. Influence of awareness and training on cyber security. *Journal of internet Commerce*, 9(1):23-41.

Merriam, S.B. 1998. Qualitative research and case study applications in education. San Francisco: Jossey-Bass Publishers.

Miller, K.W.,Voas, J. & Hurlburt, G.F. 2012.BYOD: Security and privacy considerations. *It Professional*, 14(5):53-55.

Miller, T. 2012. Ethics in qualitative research. *London: Sage*.

Mitrovic, Z., Veljkovic, I., Whyte, G. & Thompson, K. 2014. Introducing BYOD in an organisation: the risk and customer services viewpoints. The 1st Namibia Customer Service Awards & Conference organised by. p. 1-26).

Morrow, B. 2012. BYOD security challenges: control and protect your most sensitive data. *Network Security*, 2012(12):5-8.

Morse, J.M. 1994. Critical issues in qualitative research methods. Organised by Thousand Oaks: Sage Publications.

Myers, M.D. 2013. Qualitative research in business & management.

Neneh, B.N. 2014. Determining high quality SMEs that significantly contribute to SME growth: regional evidence from South Africa.

Neneh, B.N. 2011.The impact of enterpreneurial characteristics and business practices on the long term survival of Small and Medium Enterprises (SMEs).

Nene, B.N. & van Zyl, J. 2012. Towards establishing long term surviving small and medium enterprises (SMEs) in South Africa: An entrepreneurial approach.

Niekerk, B.V. 2017. An Analysis of Cyber-Incidents in South Africa.

Njiva, M.W. 2015. An investigation of the factors affecting BYOD adoption by SMEs in South Africa and the information security implications.

Patton, M.Q. 2002. Qualitative Evaluation and Research Methods. Sage.

Peltier, T.R. 2005. Implementing an Information Security Awareness Program. *Information Systems Security*, 14(2):37-49.

Peng, W., Li, F., Han, K.J., Zou, X. & Wu, J. 2013. T-dominance: Prioritized defense deployment for BYOD security. Communications and Network Security (CNS), 2013 IEEE Conference on organised by: IEEE. p. 37-45.

Pillay, A., Diaki, H., Nham, E., Senanayake, S., TAN, G. & Deshpande, S. 2013. Does BYOD increase risks or drive benefits?

Ponemon. 2018a. IBM Security Services – The 2018 Cost of a Data Breach Study

Ponemon, I. 2018b. 2018 Cost of a Data Breach Study: Global Overview.

Putri, F.F. & Hovav, A. 2014. Employees compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory.

Reid. 2013. Cryptography in the Workplace.

Renaud, K. 2016. How smaller businesses struggle with security advice. *Computer Fraud & Security, 2016(8):10-18.*

Republic, T. 2014. Research: BYOD booming with 74% using or planning to use.

Rivera, D., George, G., Peter, P., Muralidharan, S. & Khanum, S. 2013. *Analysis of security controls for BYOD (bring your own device)*.

Romer, H. 2014. Best practices for BYOD security. *Computer Fraud & Security*, 2014(1):13-15.

Rose, C. 2013. BYOD: An examination of bring your own device in business. *The Review of Business Information Systems (Online)*, 17(2):65.

Sage. 2017. Support for small businesses in South Africa

Saunders, M., Lewi, P. & Thornhill, A. 2007. Research methods for business students. Harlow: Financial Times Prentice Hall.

Scarfo, A. 2012. New security perspectives around BYOD. *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on organised by: IEEE. p. 446-451.*

SEDA. The small, medium and micro enterprise sector of South Africa.

Seed-Academy. 2017. The real state of entrepreneurship in South Africa.

Seigneur, J.-M., Hochleitner, C., Busch, M. & Kölndorfer, P. 2013. A Survey of Trust and Risk Metrics for a BYOD Mobile Worker World.

Shim, J.P., Mittleman, D., Welke, R., French, A.M. & Guo, J.C. 2013. Bring your own device (BYOD): Current status, issues, and future directions.

Shumate, T. & Ketel, M. 2014. Bring your own device: benefits, risks and control techniques. *SOUTH EAST CON. IEEE. p. 1-6.*

Singh, M.M., Siang, S.S., San, O.Y., Hashimah, N., Malim, A.H. & Shariff, A.R.M. 2014. security attacks taxonomy on bring your own devices (BYOD) model. *International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol*, 4.

Singh, N. 2012a. B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel".

Singh, N. 2012b. BYOD genie is out of the bottle–"Devil or angel". *Journal of Business Management & Social Sciences Research*, 1(3):1-12.

SME-South-Africa. 2019. South Africa's SMEs are Young, Vulnerable and In Need of Support.

Smith, K.J. & Forman, S. 2014. Bring your own device - challenges and solutions for the mobile workplace. *Employment Relations Today*, 40(4):67-73.

Spears, J.L. & Barki, H. 2010. User participation in information systems security risk management. *MIS quarterly*:503-522.

Stewart, C. 2013. Corporate Cyberstalking - A guide for SMEs *IS Practices for SME Success Series*.

Straw, K. Free Wi-Fi: The hidden dangers.

Styles, M. 2013. Constructing positive influences for user security decisions to counter corporate or state sponsored computer espionage threats. International Conference on Human Aspects of Information Security, Privacy, and Trust organised by: Springer. p. 197-206.

Sumaili, A., Dlodlo, N. & Osakwe, J. 2018. Towards a Framework for the Adoption of Mobile Information Communication Technology Dynamic Capabilities for Namibian Small and Medium Enterprises. International Conference on Applied Informatics organised by: Springer. p. 280-291.

Swartz, P. & Da Veiga, A. 2016. PoPI Act-opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment. *Information Security for South Africa (ISSA) organised by: IEEE. p. 9-17.*

Taylor, S.J., Bogdan, R. & DeVault, M.L. 2016. Introduction to qualitative research methods : A guidebook and resource.

Tech Pro. 2014. Interest high in wearables despite low adoption rates

https://www.techrepublic.com/article/research-interest-high-in-wearables-despite-low-adoption-rates/

Terre Blanche, M., Durrheim, K. & Painter, D. 2006. Research in practice: Applied methods for the social sciences: Cape Town: UCT Press.

Thomson, G. 2012. BYOD: Enabling the chaos. *Network Security*, 2012(2).

Thomson, M.E. & von Solms, R. 1998. Information security awareness: educating your users effectively. *Information management & computer security*, 6(4):167-173.

Tokuyoshi, B. 2013. The security implications of BYOD. *Network Security*, 2013(4):12-13.

Twinomurinzi, H. & Mawela, T. 2014. Employee perceptions of BYOD in South Africa: Employers are turning a blind eye? *Proceedings of the Southern African Institute for*

Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology organised by: ACM. p. 126.

Vignesh, U. & Asha, S. 2015. Modifying security policies towards BYOD. *Procedia Computer Science*, 50:511-516.

Walsh, P.K. & Homan, J.V. 2012. Measuring the effectiveness of information security training: A comparative analysis of computer based training and instructor-based training, Issues in Information Systems. *Issues in Information Systems*, 13:215-224.

Waterfill, M.R. & Dilworth, C.A. 2014. BYOD: Where the Employee and the Enterprise Intersect. *Employee Relations Law Journal, Vol. 40 no. 2, Autumn 2014*.

Weeger, A. & Gewald, H. 2014. Factors influencing future employees decision-making to participate in a BYOD program: Does risk matter?

Wilson, M. & Hash, J. 2003. Building an information technology security awareness and training program. *NIST Special publication*, 800(50):1-39.

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*. Social Computing (SocialCom), International Conference on organised by: IEEE. p. 411-416.*

Appendices

Appendix A: Email template for interview requests

Dear ***

I would like to request an hour of your time to interview you about the research I am conducting research on the topic of Security awareness and training policy guidelines to minimise the risk of BYOD in a South African SME for a fulfilment of master's thesis in Computer Science. I would like to get your input on this topic. A list of potential questions is attached. In brief, I'm most interested in exploring the BYOD security risks and how training and awareness policies can be leveraged in SMEs to minimize the risks.

Please let me know your availability in the coming week, I will send you a consent form and book a call or do a face to face meeting with you.

Thanks

Kgabi

Appendix B: Information sheet and consent form

Security Awareness and training policy guidelines to minimise the risk of BYOD in a South African SME

Kgabi Kholoanyane
North-West University

Information for participants

Thank you for considering participating in this study which will take place on June – November 2019. This information sheet outlines the purpose of the study and provides a description of your involvement and rights as a participant, if you agree to take part.

1. What is the research about?
the aim of this research is to develop guidelines for security awareness and training policy to minimise the BYOD security risks. As part of data collection, interviews will be conducted to obtain clarity on the topic under investigation.

2. Do I have to take part?
It is up to you to decide whether or not to take part. You do not have to take part if you do not want to. If you do decide to take part, I will ask you to sign a consent form which you can sign and return prior to the interview or sign at the meeting.

3. What will my involvement be?
You will be asked to take part in an interview, where you will be asked a few questions about your experience/knowledge of BYOD security risks in SMEs and training and awareness policy. It should take approximately 45 mins.

4. How do I withdraw from the study?
You can withdraw from the study at any point until the end of July, without having to give a reason. If any questions during the interview make you feel uncomfortable, you do not have to answer them. Withdrawing from the study will have no effect on you. If you withdraw from the study, we will not retain the information you have given thus far, unless you are happy for us to do so.

5. What will my information be used for?
We will use the collected information for an academic research paper in fulfilment of the requirements for the master's degree in Computer Science.

6. Will my taking part and my data be kept confidential? Will it be anonymised?
The records from this study will be kept as confidential as possible. Only [myself and my supervisor] will have access to the files. Your data will be anonymised – your name will not be used in any reports or publications resulting from the study. All digital files, transcripts and summaries will be given codes and stored separately from any names or other direct identification of participants.

Limits to confidentiality: confidentiality will be maintained as far as it is possible

8. Who has reviewed this study?
This study has undergone ethics review in accordance with the NWU FNAS Ethics committee.

9. What if I have a question or complaint?
If you have any questions regarding this study please contact the researcher my supervisor, Prof J.B Jordaan at Dawid.Jordaan@nwu.ac.za

If you have any concerns or complaints regarding the conduct of this research, please contact the NWU FNAS Ethics committee.
If you are happy to take part in this study, please sign the consent sheet attached.

CONSENT FORM

Security Awareness and training policy guidelines to minimise the risk of BYOD in a South African SME
Kgabi Kholoanyane

PARTICIPATION IN THIS RESEARCH STUDY IS VOLUNTARY

I have read and understood the study information dated June 2019 or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	YES / NO
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and that I can withdraw from the study at any time up until 31 July 2019 without having to give a reason.	YES / NO
I agree to the interview being audio recorded	YES / NO
I agree to maintain the confidentiality in the interview	YES/NO
I understand that the information I provide will be used for the master's thesis and that the information will be anonymised.	YES / NO
I agree that my (anonymised) information can be quoted in research outputs.	YES / NO
I understand that any personal information that can identify me – such as my name, address, will be kept confidential and not shared with anyone	YES / NO

Please retain a copy of this consent form.

Participant name:

Signature: _____ Date _____

Interviewer name:

Signature: _____ Date _____

For information please contact Elisa Kholoanyane - elisa.kgolwanyane@gmail.com

Appendix C: Sample Interview questions and answers
Employees

1. Could you mention top 3 BYOD / mobile device security risks
2. Are you aware of the concepts hacking, pishing and malware and how do you protect your device from this?

➔ With this information I can determine to some extent the level of awareness in an organization and to explore whether employees will mention the same risks or different risks

3. How do you keep your mobile devices secured? Is it required by your organization BYOD policy?
4. How do you protect the corporate data on your mobile devices?
5. Please mention 3 security risks of using public wifi and how do you protect your device from unsecure wifi hotspots?
6. How do you distinguish between softwares or applications that are safe to download and softwares or applications that are not safe to download?
7. How do protect your sensitive information in e-mail communications and keep your email account secure against unathorized access, lost or compromised device?
8. How do you identify a malicious e-mail, link and website address?
9. What do you do when you suspect some malicuous activities on your device?
10. Name 5 basic guidelines for security training and awareness policy
11. Highlight the key critical elements for a solid training and awareness policy

Security Experts:

1. Can you highlight three most concerning BYOD security risks related to employees in your organization?
2. Mention the policies needed for BYOD

3. For your organization's BYOD employee training and awareness policy, did you follow any guideline when developing this policy? If any, please share
4. Mention top 5 challenges of developing the BYOD training and awareness policy?
5. Can you highlight 5 most critical points that should be included in the training and awareness policy?
6. Mention 5 key elements to formulate a solid training and awareness policy?

Sample of Interview Scripts – Security Experts

Questions	Participant 1	Participant 3	Participant 8	Participant 5
1. Can you highlight three most concerning BYOD security risks related to employees in your organization?	- employees resigning from the organization and leaving with inside information is a big issue we are currently facing. This leads to stolen ideas and customer information - Weak password - Data leakage - Lost or stolen device	People are most likely to make bad security decisions Unauthorized access Loss of stolen device Phishing - Attackers are persistent and well trained	- Unauthorized access - Lost or stolen device - Phishing	- People - Human factor is a big problem…while most organizations invest in security tools and technologies to prevent this – the major challenge is still people. - Data leakage - Public Wi-Fi / unsecure networks - Networks are not scanned frequently for vulnerabilities - Weak password
2. Mention the policies needed for BYOD	- Data access policy - Device policy - BYOD policy	Data Ownership policy Network/ wi-fi policy	Access Policy Training and awareness policy Access policy	Training and awareness policy Data access policy Device policy
3. For your organization's BYOD employee training and awareness policy, did you follow any guideline when developing this policy? If any, please share	No – we use our own policy that we created, according to our environment - we didn't have a policy. We still used our general IT controls - It's not easy to protect complex and dynamically changing environment – and attack also change all the time.	We downloaded a sample policy and customized it – there's a lot of them on the internet	No – we just created our own template that we thought made sense for our environment we use training and awareness programs to meaningfully increase awareness.	No- we have changed our old laptop policy to accommodate mobile devices. We currently have a BYOD training and awareness policy in place, although it is not well documented. The aim of the policy is to enforce some basic settings (password strength and guidance for lost or stolen devices.)

4.	Mention top 5 challenges of developing the BYOD training and awareness policy?	No one cares No support from management - There's generally lack of adequate security staff with the necessary skills - this is a problem for most SMEs Lack of know-how on what need to be included	No time No one is taking the lead or driving this Lack of resources or skill	We don't have BYOD policy or device policy – awareness policy needs to include those.	You are never sure if you have included everything – no template or guidelines. We are adopting what other people have built because we don't want to reinvent the wheel
5.	Can you highlight 5 most critical points that should be included in the training and awareness policy?	Onboarding process Clear Rules Involve everyone affected	Weaknesses Ensure control Involve management and users	Covers against greatest possible threats Training offering After training assessments – ensure efficiency	Ensure its official User responsibility - Human factor is a big problem…while most organizations invest in security tools and technologies to prevent this – the major challenge is still people. Assess your weaknesses Know your environment and your employee Pre-planning
6.	Mention 5 key elements formulate a solid training and awareness policy?	Password policy Outside networks access for those working from everywhere – data access Phone management Personal vs company data Organization data – when people leave Who has access to what? Exercise control on security	Device management Reporting malicious activities Email on mobiles phone Employees Management	employee responsibility Phone and security updates Management responsibility Rewarding good behaviours	Reporting lost or stolen phone Data ownership Ensure process are well defined and explained Include technology Get management on board Highlight key issues – all policies must be known Have someone taking responsibility of lead this initiative Sponsors and buy in of management

Appendix D: Sample Questionnaires

BYOD - SME employee survey

Please answer the following questions where:
1 = **Strongly Disagree** and 5 = **Strongly Agree**

1.	Do you think it is important to use a passwords to access your device?	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
2.	It is important to set your mobile device to require a passcode to unlocked it after a period of non-use?	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
3.	I often access work-related e-mail or documents on a non-encrypted mobile device (e.g. device that can be accessed without a password) on my personally owned device?	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
4.	My organization provide software/application that allows encrypted (e.g. password-protected) access to e-mail or other documents on mobile devices?	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
5.	I often work with sensitive information (on my device / laptop screen) while in a public location where the information could be observed	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
6.	I often download and store documents containing sensitive company or client information on my device.	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
7.	I often handle sensitive information as part of your job	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
8.	The risk of my organization being harmed if employees lose their “BYOD” device with sensitive information on it is high	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
9.	It is a burden to consistently remember to secure my device to protect the sensitive information on my device	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
10.	My mobile device automatically lock after a period of inactivity	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
11.	The risk of my organization being harmed if I do not electronically “lock” my device is high	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
12.	I understand the risk of opening suspicius email attachments or clicking on a link in suspecious e-mail	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
13.	I can easily identify a suspicious URL or e-mail or link	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
14.	I often use public wifi to perform work related tasks and to access work related e-mails	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**
15.	I often make an extra effort to verify and ensure that the Wi-Fi is legit and secure	**Strongly Disagree**	1	2	3	4	5	**Strongly Agree**

Sample of Responses:

Participant no:	Timestamp	Do you think it's important to use a password to access your device?	It is important to set your mobile device to require a passcode to be unlocked after a period of non-use	related e-mail or documents on a non-encrypted mobile device (an e.g. device that can be accessed without a password) on my	provides software/application that allows encrypted (e.g. password-protected) access to e-mail or	sensitive information (on your device/laptop screen) while in a public location where the information could	I often download and store documents containing sensitive company or client information on my device.	I often handle sensitive information as part of your job	organization harmed if en lose their "B device with s information high
Participant 1	6/3/2019 12:56:17	Disagree	Neutral	Agree	Neutral	Agree	Agree	Agree	Agre
Participant 2	6/12/2019 15:27:35	Neutral	Agree	Disagree	Strongly Disagree	Disagree	Disagree	Agree	Disagr
Participant 3	6/12/2019 20:06:00	Agree	Neutral	Disagree	Neutral	Disagree	Agree	Disagree	Agre
Participant 4	6/13/2019 9:35:47	Agree	Agree	Agree	Strongly Disagree	Agree	Agree	Agree	Agre
Participant 5	6/17/2019 17:09:47	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Agree	Agree	Agre
Participant 6	6/18/2019 10:56:34	Disagree	Agree	Disagree	Neutral	Agree	Disagree	Agree	Agre
Participant 7	6/18/2019 18:28:09	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Agree	Agree	Agre
Participant 8	6/23/2019 17:00:40	Strongly Agree	Agree	Agree	Strongly Disagree	Disagree	Disagree	Agree	Agre
Participant 9	7/2/2019 8:36:33	Strongly Agree	Neutral	Agree	Neutral	Disagree	Agree	Disagree	Agre
Participant 10	7/3/2019 10:22:16	Disagree	Disagree	Disagree	Neutral	Disagree	Disagree	Agree	Agre
Participant 11	7/3/2019 12:34:30	Agree	Neutral	Agree	Strongly Disagree	Agree	Disagree	Agree	Agre
Participant 12	7/3/2019 15:26:35	Strongly Agree	Agree	Disagree	Strongly Disagree	Disagree	Agree	Agree	Agre
Participant 13	7/3/2019 17:25:44	Strongly Agree	Neutral	Agree	Strongly Disagree	Agree	Disagree	Agree	Agre
Participant 14	7/3/2019 18:09:10	Strongly Agree	Neutral	Disagree	Neutral	Disagree	Agree	Agree	Agre
Participant 15	7/16/2019 23:29:59	Disagree	Neutral	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree	Strongly A
Participant 16	7/17/2019 7:22:13	Agree	Agree	Disagree	Disagree	Agree	Agree	Strongly Agree	Strongly A
Participant 17	7/17/2019 8:26:22	Disagree	Agree	Strongly Disagree	Strongly Agree	Neutral	Agree	Agree	Strongly A
Participant 18	7/17/2019 9:45:11	Strongly Agree	Agree	Agree	Strongly Agree	Strongly Disagree	Disagree	Agree	Strongly A
Participant 19	7/17/2019 10:58:01	Disagree	Agree	Disagree	Strongly Agree	Neutral	Neutral	Neutral	Agre
Participant 20	7/17/2019 11:58:28	Agree	Agree	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree	Strongly A
Participant 21	7/17/2019 13:46:56	Agree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree	Strongly A

Form Responses 1

.11 | Strongly Agree

H	I	J	K	L	M	N	O	
I often download and store documents containing sensitive company or client information on my device.	I often handle sensitive information as part of your job	organization being harmed if employees lose their "BYOD" device with sensitive information on it is high	It is a burden to consistently remember to secure my device to protect the sensitive information on my device	My mobile device automatically lock after a period of inactivity	The risk of my organization being harmed if I do not electronically "lock" my device is high	I understand the risk of opening suspicious email attachments or clicking on links in suspicious emails	I can easily identify a suspicious URL or Email or links	I often u perform tasks an related e informat
Strongly Agree	Strongly Agree	Agree	Agree	Disagree	Disagree	Neutral	Strongly Disagree	S
Agree	Agree	Agree	agree	Disagree	Disagree	Disagree	Disagree	
Agree	Agree	Agree	Agree	Agree	Agree	Agree	Agree	
Agree	Agree	Agree	Disagree	Disagree	Disagree	Disagree	Disagree	
Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	
Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Disagree	Str
Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	
Strongly Agree	Strongly Agree	Neutral	Agree	Strongly Agree	Neutral	Strongly Agree	Strongly Disagree	S
Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Str
Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Str
Neutral	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	
Disagree	Agree	Strongly Agree	Strongly Disagree	Strongly Agree	Neutral	Strongly Agree	Strongly Agree	Str
Agree	Agree	Strongly Agree	Neutral	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Str
Agree	Strongly Agree	Strongly Agree	Neutral	Agree	Agree	Strongly Agree	Agree	
Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Str
Agree	Agree	Agree	Disagree	Disagree	Disagree	Disagree	Disagree	
Disagree	Agree	Agree	Agree	Disagree	Disagree	Disagree	Agree	
Agree	Agree	Agree	Disagree	Agree	Disagree	Agree	Agree	
Disagree	Agree	Agree	agree	Disagree	Agree	Disagree	Disagree	
Disagree	Agree	Agree	agree	Disagree	Agree	Disagree	Agree	
Agree	Disagree	Agree	Disagree	Agree	Disagree	Agree	Disagree	

Form Responses 1

Appendix E: Abbreviations and Acronyms

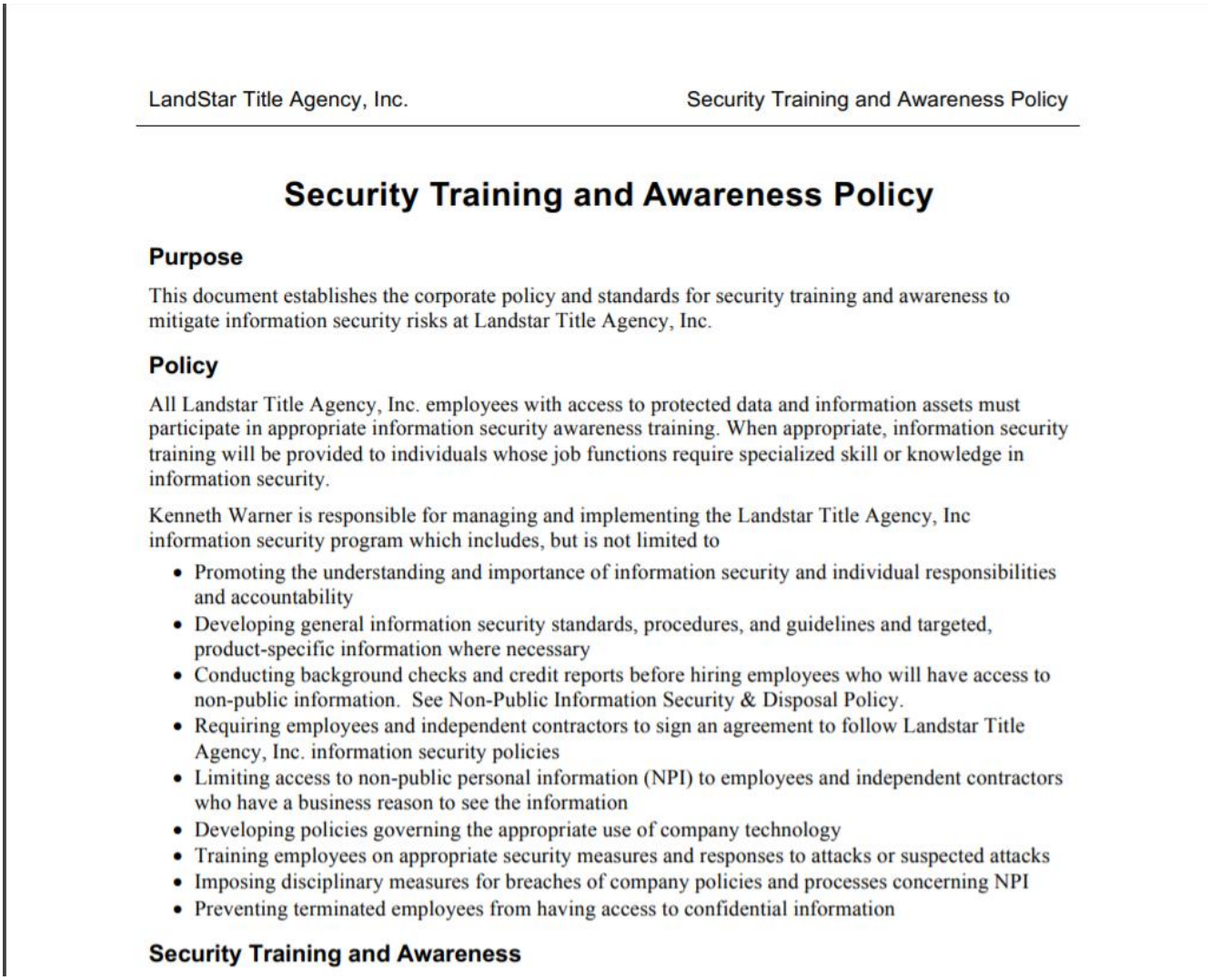
BYOD	Bring your own device
SMEs	Small Medium-sized Enterprises
POPI	Protection of Personal Information Act
IT	Information Technology
SEDA	Small Enterprise Development Agency
MDM	Mobile Device Management
DLP	Data Loss Prevention
VPN	Virtual Private Network

Appendix F: Training and awareness policies reviewed:

- BYOD Policy Template
- SAMPLE BYOD POLICY TEMPLATE
- BYOD (bring-your-own-device) policy
- 6 free online templates you can use to write your IT policy
- Greenwich Uni IT Policies and Procedures
- https://docs.gre.ac.uk/__data/assets/pdf_file/0009/1514916/Information-Security-and-Data-Protection-User-Awareness-and-Training-Policy.pdf
- NB model policy on security awareness & training - ISO 27001 Security
- Security Awareness Training and Privacy - SANS.org
- Security Awareness and Training Policy | Resolver
- TRAINING AND AWARENESS | Information Security Team
- Information Security Training Policy - Colorado Department of Education
- Training and Awareness Policy - Pomona College
- Security Awareness and Training Policy - NC.gov
- ICT security awareness procedures - Derbyshire County Council

- Security Training and Awareness Policy - LandStar Title
- Information Security Awareness and Training Policy - Gordon State ...
- Security Training and Awareness Policy - Massachusetts Maritime ...
- Information Security Awareness Policy | Villanova University
- Security Training and Awareness Policy - Fitchburg State University
- Security and Privacy Awareness and Training Policy
- Cyber Security Awareness Training and Education Sample Policy
- Security Awareness and Training Policy - Community Health Plan of ...
- Training and Awareness · Manchester Metropolitan University

Sample Policy:



LandStar Title Agency, Inc. Security Training and Awareness Policy

Security Training and Awareness Policy

Purpose

This document establishes the corporate policy and standards for security training and awareness to mitigate information security risks at Landstar Title Agency, Inc.

Policy

All Landstar Title Agency, Inc. employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training will be provided to individuals whose job functions require specialized skill or knowledge in information security.

Kenneth Warner is responsible for managing and implementing the Landstar Title Agency, Inc information security program which includes, but is not limited to

- Promoting the understanding and importance of information security and individual responsibilities and accountability
- Developing general information security standards, procedures, and guidelines and targeted, product-specific information where necessary
- Conducting background checks and credit reports before hiring employees who will have access to non-public information. See Non-Public Information Security & Disposal Policy.
- Requiring employees and independent contractors to sign an agreement to follow Landstar Title Agency, Inc. information security policies
- Limiting access to non-public personal information (NPI) to employees and independent contractors who have a business reason to see the information
- Developing policies governing the appropriate use of company technology
- Training employees on appropriate security measures and responses to attacks or suspected attacks
- Imposing disciplinary measures for breaches of company policies and processes concerning NPI
- Preventing terminated employees from having access to confidential information

Security Training and Awareness

Kenneth Warner promotes on-going information security awareness via

- Distribution of employee manuals to all employees requiring annual sign-off of agreement and compliance
- Regular articles published in corporate newsletters
- Information security bulletins distributed to all employees to address security policy modifications, security alerts, and other urgent security issues

Note: When necessary, the information security program must provide or coordinate training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training must focus on expanding knowledge, skills, and abilities for individuals who are assigned information security responsibilities.

Violation of Policy

Failure to adhere to all requirements stipulated in this policy and all related documents may result in disciplinary actions, up to and including

- Immediate removal of any applicable hardware/software/access to the Landstar Title Agency, Inc. computer network or business systems

63

- Formally reporting the incident to Landstar Title Agency, Inc. senior management
- Termination of employment
- Any other action deemed necessary by Landstar Title Agency, Inc. senior management

Review

Landstar Title Agency, Inc. has voluntarily adopted this policy for its sole and exclusive use. This policy and all related documents will be reviewed annually or as needed based on prevailing business conditions.

Approved

Kenneth Warner, Esq., Vice President and Senior Counsel

Appendix G: Categories of analysis

‘Start list’ of thematic codes

- BYOD in SMEs
- BYOD Security Risks in SMES
- Implemented / available toolsets and measures to mitigate the risks
- Policies
- Training and Awareness policies
- Training and awareness methodologies
- Training and awareness policy elements