Vaal University of Technology

Framework for Adoption of Information and Communication Technology Security Culture in SMMEs in Gauteng Province, South Africa

Research thesis submitted for the degree:

Magister Technologiae in Information Technology

In the Department of Information and Communication Technology,

Faculty of Applied and Computer Sciences

MA Mokwetli

Student Number 215271319

Supervisor: Prof. Tranos Zuva

Co-Supervisor: Nkoana Tshepiso

Author's declaration for submission of a dissertation

I, **Moraba Andrew Mokwetli**, student number: 215271319 hereby declare that this dissertation titled "Framework for adoption of the ICT security culture in the Gauteng province South Africa" was written as a part of MTech in Information Technology at Vaal University of Technology. I pronounce that I am the only author of this dissertation and it has not been previously submitted either in full or partially at any recognised educational institutions. All the sources used or quoted have been explicitly indicated and acknowledged by references.

I thus approve Vaal University of Technology to advance this dissertation to anybody including learning associations and anyone with the end goal of scholarly research study.

I additionally allow Vaal University of Technology to imitate this dissertation by different means including photocopying, altogether or in part of, at the request by different associations or any people for the sole reason for insightful research.

I'm completely mindful that my dissertation might be made electronically accessible to people in general.

_____ _____

Signature Date

Dedication

This dissertation is devoted to the following key individuals: To my lovely wife, Matshidiso Jacqueline Mokwetli who soldered on during the time of difficulties more especially the awkward hours of research. You are the best woman in my life. To my children, Matome, Tshepiso, Tebogo and Lesedi who could not complain when I was depriving them of family quality times and knowing that everything has a reason. Lastly, to my mom, sister and brother who kept me in their prayers for me to pull on.

Acknowledgements

My sincere indebtedness is channelled to the following exceptional individuals:

- My heavenly father who provided me with courage, strength and protection throughout the research process. I couldn't pull through if it was not his kindness and grace.
- To my mentor who is also my supervisor, Prof. Tranos Zuva. Thanks for encouraging me to hold on even if the situation was not possible. You showed true maturity in this field you are the best. Also to my co-supervisor Nkoana Tshepiso making sure that everything is aligned.
- To my fellow students who showed some love and passion to assist were it was difficult for me to handle.

Abstract

Information and Communication Technology (ICT) has become prevalent in our everyday business and personal lives. As such, users and organisations must know how to protect themselves against human errors that led to more companies losing or sharing information that should not be shared. The issue emanates from lack of ICT security culture both in individuals and organisations. This research is based on a wide theoretical review that is focused on proposing a conceptual model on technological, environmental and organisational factors that influence the adoption of ICT security culture and implementation in Small Medium and Micro Enterprises (SMMEs). Factors or determinants that influence the adoption of ICT security culture in SMMEs in the Gauteng province were investigated. Questionnaires were distributed to examine the perception of ICT security culture adoption among SMMEs in the Gauteng province South Africa. A sample of 647 individuals from different SMMEs in the Gauteng province returned the questionnaire. The results of the research study show that technological context (perceived benefits), environmental context (government regulations) and organisational context (management support) determinants have direct influence on the ICT security culture adoption. The recommendation is that information security awareness programmes must be put in place. Further research is recommended using more determinants that might have a positive impact toward the adoption of the ICT security culture. In order to minimize data breaches due to human error it is recommended that SMMEs around Gauteng Province in South Africa adopt the framework as outlined in this research study.

Key words: ICT Security culture, Information Security culture, SMMEs, ICT, Adoption, human error

TABLE OF CONTENTS

List of Abbreviations

SMMEs	Small, Medium and Micro Enterprises
ICT	Information and Communication Technology
GDP	Gross Domestic Products
TOE	Technology, Organisation and Environment
BYOD	Bring Your Own Device
TQM	Total Quality Management
ISMS	Information Security Management Systems
ISC	Information Security Culture
BCP	Business Continuity Planning
MFA	Multi-Factor Authentication
DRP	Disaster Recovery Plan
TAM	Technology Acceptance Model
PU	Perceived Usefulness
PEOU	Perceived Ease of Use
UTAUT	Unified Theory of Acceptance and Use of Technology
RFID	Radio-Frequency Identification
SPSS	Statistical Software Package for Social Sciences
EPS	Equally Probability of Selection
AVE	Average Variance Extracted
CR	Composite Reliability

KMO	Kaizer-Meyer-Olkin
PCA	Principal Component Analysis
DTI	Department of Trade and Industry

List of Tables

List of Figures

Publications:

Moraba Mokwetli and Tranos Zuva (2018), Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa, 2018 IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 6-7 August 2018, ISBN 978-1-5386-3059-4 pp.380-387

CHAPTER ONE

1 INTRODUCTION

To realise objectives in the 21st century, capability to confront the latest multifaceted problems must be built, countries across the globe need to develop ideas based on social and economic knowledge; and finally, the countries must know how to protect those ideas. Through the intervention of Information and Communication Technology (ICT), these ideas can be transformed into reality. (ICT is defined as the infrastructure and components that enable modern computing). For ICT to ensure that businesses realise their strategic objectives information security culture must be embedded across all their business units. Information security culture entails all socio-cultural aspects that support technical security methods to ensure that information security becomes a daily activities of every user (Schlienger and Teufel, 2002). According to Martinez-Ruiz et al., (2007) many established states have decided that their prospect relies on maximizing investment in the fundamental capability of the knowledge economy and providing an environment that supports swift conversion of new concepts into actual business prospects.

According to Tudorache et al., (2012) ICT was recognised as the key contributor of the knowledge economy in the global world. According to Dyerson et al., (2008) the developing worldwide marketplace is utilised extensively by ICT which is considered critical for competitiveness of both larger organisations and SMMEs. An increasing number of SMMEs are adopting electronic trade or e-commerce because of flexibility offered and ability to respond to new opportunities and innovations. However, the key issue is how the information security is maintained to ensure that those innovations are protected (Cosgun and Dogerlioglu, 2012). According to Faraji et al., (2011) e-commerce is capable of achieving commercial development, improved competition, improved commercial prospects and improved admittance to the latest market.

With the advancement and adoption of ICT at a fast pace, it is critical to address the concern of adopting information security in this type of inter-connected environment. SMMEs are hampered by minimal time for adoption and endorsement of standards in their environment as a result of the intricate environment of information security standards and the absence of capabilities and finances to purchase those competences in this sector (Chan et al., 2006). A robust information security culture is equally a mind-set and manner of procedure which is combined into daily rationalization coupled with decision making processes that is pioneered by adoption of the organisational culture (Andress and Leary, 2017). In order to win the mind-set of individuals you must put the adoption of the information security culture within individuals' day to day program and let them own the process (Alnatheer and Nelson, 2009b).

According to Al-Alawi and Al-Ali (2015) the adoption of ICT security culture in an organisation requires top management support whereby the 'do as I do' slogan will be well understood by their business units. The company might have well written policies, standards and procedures on how to follow the internal processes but if top management are not leading by example, human errors will periodically emerge even though they are preventable by those governance documents. The current modern and technology-dependent businesses cannot afford to restrain themselves with just the technical aspects of information security, therefore in order for their businesses to realise the strategic business objectives, they need to adopt a culture of scrutinising, evaluating and treating information as a business issue, as opposed to technical issue alone, (Khan, 2010).

The framework to implement, maintain, monitor and improve information security has to be aligned to the organisational culture but trying to change organisational culture to fit the information security is often not possible ISO (2005). SMMEs in Gauteng are dependent on their information systems and networks to deliver services to customers and meet their strategic business objectives. However, the use of those technologies brings new opportunities for

enhanced business performance and operations while on the other hand introducing several information security and privacy risks. Addressing those risks plays a substantial role in business success and development as increasing security threats may potentially disrupt business continuity and possibly cause monetary, reputational, as well as other types of losses to SMMEs. According to Corris (2010), integration of information security culture into business functionality should not be viewed as an add-on, but it should be seen as significant and become integral to the organisational culture.

This study seeks to propose the framework for the adoption of the ICT security culture within SMMEs in Gauteng Province. The effectiveness of this framework will not only give guidance on how to protect the institutional information asset but also guide the users on how to protect themselves in the cyberspace, whether on the road or at home. The general underlying premise is that the introduction of information security culture within the institution will assist in protecting the information asset of all levels of employees. As per Veseli (2011), the effective adoption of information security culture influences knowledge, behaviour and attitude of the users or participants.

1.1 Definition of Small Medium Micro Sized Enterprises

There is no agreed worldwide definition of SMMEs according to OECD (2009). Mylenko et al., (2011) pointed out that many organisations globally are utilising the most shared characterizations constructed on sales income, workforces or entire resources or loan size. Based on the South African Small Business Act, "Small business organisation" means any entity, either combined or listed under any law, which comprises mostly of individuals carrying on small business concerns in any economic sector, or which has been set up to promote the interests of or speaking to independent venture concerns, and incorporates any alliance comprising entirely or mostly of such affiliation, and furthermore any part of such organisation.

The SMME environment has been categorised as follows:

- Fewer than 200 employees
- Annual turnover of less than R64 Million
- Capital assets of less than R10 Million
- Direct management involvement by owners

1.2 Problem Statement

Having the policies, standards and procedures for information security programs in place does not guarantee that those processes will be understood and implemented by the users in the SMMEs. The real threat to information security is human error, which is difficult to circumvent in order to shift the mind-set of users. According to IBM (2014) 95% of information security incidents involve human error. According to Saran (2016) 62% of the incidents reported based on the data obtained by Egress Software Technology were accounted to human error. In this technological environment, where many organisations rely on information, the improper handling of such important assets can bring SMMEs it to its knees. For the above reasons, end users are putting their personal and business information at risk, whereby SMMEs suffer reputational damage, data breaches, loss of income and law-suits by the affected parties or sanctions by the governance authorities.

According to Deursen (2015), the following items signify elements of human error:

- System Misconfiguration;
- Poor patch management;
- Use of default username and passwords or easy to guess passwords;
- Lost devises;
- Disclosure of information via an incorrect email address;
- Sharing credentials or login details with other individuals;

- Leaving computers unattended when outside the workplace; and
- Utilizing personal portable gadgets that connect or have access to the organisation's network.

Gundu and Flowerday (2013) supported the previous statement by highlighting that having and implementing data security governance does not naturally ensure that all workers will comprehend their responsibility in guaranteeing the security and protection of data resources. Information security awareness is one of the elements that must cement the awareness of information security in an engaging manner. The challenge now is how to change the culture of the users towards information security in order to minimise human error.

Within this research program the premise is to evaluate the determinant through the study of literature that influences the adoption of ICT security culture in SMMEs and propose the framework fostering its implementation.

1.3 Primary research questions

Based on the research objectives the following primary research question can be outlined:

- How can the adoption of ICT security culture be supported in SMMEs to minimize human errors?

1.4 Secondary research questions

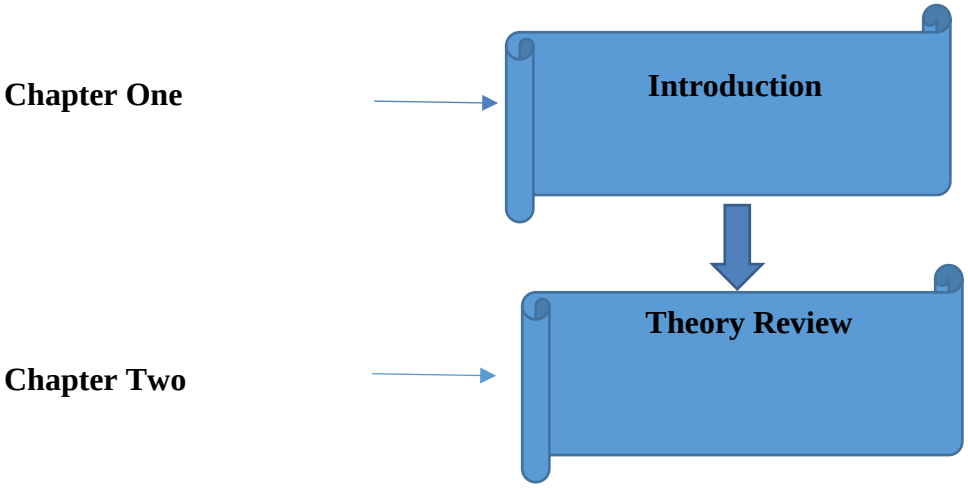
- What has been done to minimize security breaches through human error in Information Technology?
- What are the determinants that influence the adoption of ICT security culture in SMMEs?
- How can the effectiveness of framework for adopting ICT security culture be measured in SMMEs?

1.5 Research Objectives

- To investigate the literature and existing framework on what has been done to minimize security breaches as a result of human error.
- To determine the factors or determinants that influence the adoption of ICT security culture in SMMEs.
- To propose a framework for the adoption of an ICT security culture that will help in minimizing the human error in SMMEs.
- To measure the effectiveness of the framework for adopting ICT security culture in SMMEs.
- To recommend the model for the adoption of the ICT security culture in SMMEs

1.6 Layout of the research study

This research study was structured into five chapters as depicted below in figure 1-1:



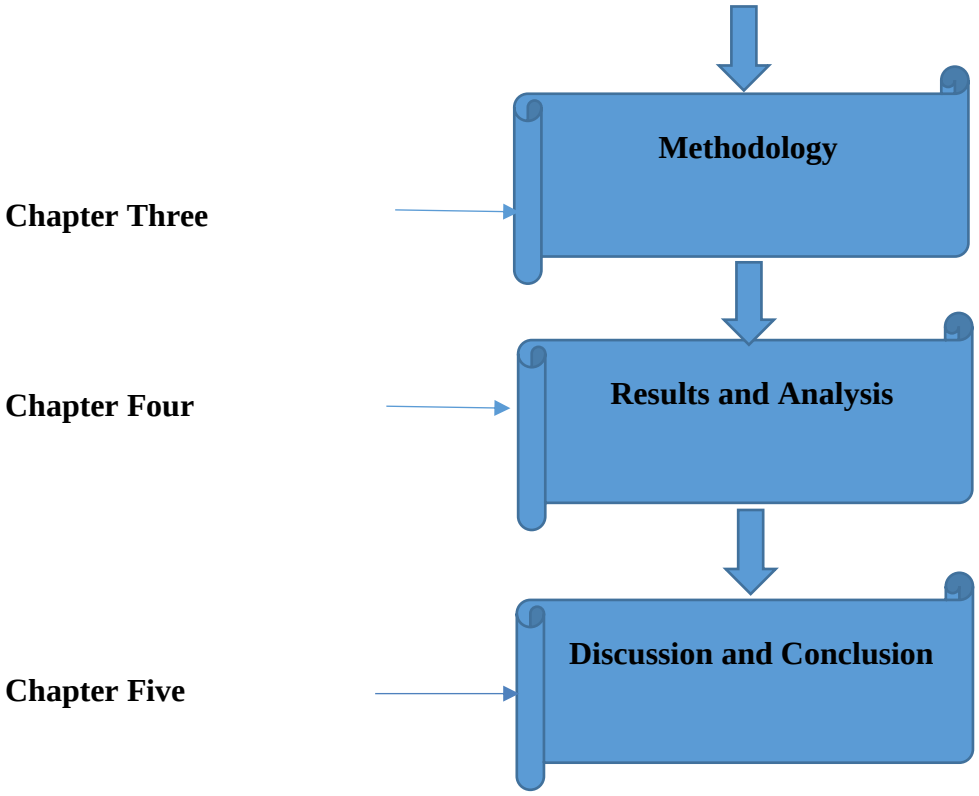


Figure 1-1: Research Study Layout

CHAPTER TWO

2 LITERATURE REVIEW

2.1 Introduction

This chapter highlights the understanding of the key concepts including SMMEs, Security Culture, Information Security Culture, Information Security Management Systems and lastly the adoption of these concepts. The SMMEs concept entails environments linked to the South African context. The explanation of security culture was provided from different researchers based on their insights into the concept. Frameworks pertaining to the information security culture were outlined and the process on how to manage both the technological systems, information and data through ISMS (Information Security Management System) was detailed. Lastly the concept of adoption was deliberated taking into account the Technological, Organisational and Environmental model or framework (TOE) used for the innovation adoption and their constructs.

2.2 South African SMMES

Globally, there is consent amongst policy-makers, economists and business experts that SMMEs are significant drivers of economic growth, irrespective of the economic developmental stage. A robust SMMEs sector contributes significantly to the economic growth by generating multiple job prospects, producing maximum capacities of goods, maximising transfers across the globe and presenting innovations and entrepreneurship skills. According to Ayyagari et al., (2005), in the year 2004 alone, the World Bank Group approved around $2.8 billion in support of SMMEs. The statement alone shows the recognition of the role that SMMEs play in supporting both global and regional economic recovery. SMMEs are the initial footstep towards the industrialisation economies both in emerging and established countries

Fida (2008). According to Daniels and Ngwira (1994), it was projected that SMMEs employs around 22% of the grown-up population in emerging countries.

SMMEs plays a pivotal role to the contribution of GDP (Gross Domestic Product) and employment opportunities (Seda, 2016). In numerous occasions, SMMEs are viewed as efficient in economic development and job creation, as compared to their larger corporate counterparts. According to Leboea and Ryan (2017), SMMEs are viewed as the main feeder stream into the bigger business and keeps them going. On the other hand, it acts as the fuel that South African' economic engine uses to grow. Millinuex (1997), pointed out that the SMME sector contributes more to the employment of both youth and adults than the multinationals in any nation. The study by Quartely and Abor (2010), estimated that 91% of formal business entities in South Africa are SMMEs and they contribute between 52% and 57% to GDP and also contribute about 61% to employment in the country.

With the flourishing of ICT within developing and developed countries, SMMEs across the globe are obliged to adapt since more benefits could be reaped by adopting ICT (McIvor et al., 2003). As South Africa is regarded as one of the developing countries, the usage and protection of ICT systems by SMMEs is still in its infant stage. According to Swift (2009), the usage of ICT across SMMEs has minimized the manual process and the time taken to provide good service to their customers. Some of the benefits entails submitting of tax returns to the receiver of revenue using an online process instead of the manual process that was used before. The usage of ICT, whether in developing or developed countries, required some level of protection to ensure that services will not be impacted, and customer data or information will not be disclosed unintentionally by the employees (Alam and Noor, 2009).

According to OECD (2009), there is no approved universal characterization of SMMEs. Mylenko et al., (2011) pointed out that numerous organisations globally are utilizing the

available communal characterizations that are linked to sales revenue, personnel's or total assets or loan size.

According to the Seda (2016), perspective shown in Table 2-1 the environment falls under the following categorization to be regarded as an SMME:

Table 2-1: SMMEs definitions

Category	Employees	Asset Value	Characteristics
Micro Enterprises	Normally owner run, and it does not have more than five workforces	Minimal	In most cases it lacks business formality and premises. Generally, are survivalists that owned which are of basic in nature. Their level of income generation is normally lower than the income standards or the poverty line.
Very Small	Generally, the owner run the business with up to 20 personnel	Moderate and to high based on stock levels	Generally, the business has premises and basic infrastructure. The business has bank account and meets basic legal compliances.
Small	Generally, the owner run the business with up to 50 personnel.	High – based on stock level and	Generally, it is more established with a traceable trading history. The programme has succession planning mechanisms. The establishment will have a bank

		accumulated assets	account as a results of positive trading history and have access to finances
Medium Enterprise	Generally, it has 100 employed personnel. The owner still manages however it has more complex management structure.	Very high – because of the stock level and accumulated assets.	Based on its decentralization of power, management differentiates medium from small. Regarded as well-established backed by traceable references and established trading history.

Table 2-2 below summarises both the formal and informal SMMEs in South Africa.

Table 2-2: Summary of Formal and Informal SMMEs

Division	**2015Quarter 2**
Total quantity of SMMEs	2 251 821
Total quantity of formal SMMEs	667 433
Total quantity of informal SMMEs	1 497 860
SMMEs landlords as percentages of overall employed in the sector	14%
Total number of percentages functioning within trade and accommodation	43%
Total number of percentages functioning within communal services	14%

Total number of percentages functioning within construction sector	13%
Total number of percentages functioning within the finance and business sectors	12%
Total number of percentages linked to black owned formal SMMEs	34%
Total number of percentages worked by income categories of<R30k per annum	7%

Source: StatsSA (2015)

According to StatsSA (2015) as stated in table 2-2 above there is a substantial dissimilarity amongst the formal and informal sector which is most noticeable in the trade and accommodation sector. According to Government (2007) the separation between the informal sector and the formal sector is not always clear, as it includes various definitions used across the different countries in trying to differentiate the categories of economic activities. Further to that, categorizing businesses according to size can be accomplished in multiple ways, thus leading to situations where businesses that is identified as small when using one criteria are not necessarily small based on the sector's criteria. Nonetheless, the formal-informal distinction is not that simple based on the literature reviews.

Challenges faced by SMMEs

SMMEs are just as vulnerable to cyber-attacks than larger organizations, however, majority of SMMEs are of the view that it is only the bigger players who are at risk. The fact of the matter is cyber-attacks to SMMEs are not a matter of when, but of who is next (Amrin, 2014). The noticeable major difficulties faced by SMMEs is human error, which makes it practically impossible to manage because of resources limitation as the little resources they have are

directed to the technical aspect of security (Whitman, 2003). In recent times SMMEs are creating or producing vast volume of data that are stored internally and that increases the risk for the organisations to go down should the cyber-attacks materialise. Another challenge is the embedding of ICT security culture to every personnel function within SMMEs (Siponen, 2000). Lack of processes to embed security culture is a challenge as ICT security relies mostly on how the culture of the organisation views the importance of security (Louw et al., 2006).

Even though SMMEs are seen as a pillar of domestic economy, few African governments have outlined policies to enhance their growth and survival. The Majority of African governments do not have an act governing SMMEs or have reliable statistics on SMMEs (NEPAD, 2001). Established businesses are in support of their organisational culture, however, SMMEs are not at liberty to do so as they put more focus on providing services than on considering the social aspect of the service organisations. According to Rogerson (2004), in South Africa, the majority of SMMEs focusses hugely on merchandizing and comprises of survivalist functions that naturally struggles with low level of throughput, incompetent and out-of-date knowledge as well as inadequate access to credit, information and training prospects. Below is a list of challenges faced by SMMEs (Netshandama, 2006), however, it has to be noted that not all SMMEs are affected by these challenges:

- Majority of SMMEs cannot access financial assistance because they are not credit worthy;
- Securing information and data assets adequately;
- Because of stiff competition within the SMMEs, some are selling products of low quality at a cheaper price;
- Majority of SMMEs don't have the adequate required skills;
- Access to finance and markets by SMMEs is still a major challenge;

- Some of the SMMEs are not coordinated accordingly to provide the complete set of services required for growth and development;
- Development of SMMEs suffer because of poor corporate governance, poor financial management and the lack of business understanding;
- Lack of resources to mitigate cyber threats;
- Lack of understanding the impact of human error to the protection of their ICT systems, information and data assets.

For SMMEs to be protected against cyber threats, their security culture should support all the organisational functions so that information safeguarding turns into a normal feature within the daily functions of all personnel (Schlienger and Teufel, 2002). Security culture helps to enforce the information security policies and practices within the organisation. Based on that, every organisation should strive to be capable of achieving an operative information safeguarding culture in their area. By embedding a security culture within the organisation the information security culture will appear to be stronger and become visible in the behaviour and activities of the personnel (Da Veiga et al., 2007). The next section will deliberate about the significance of security culture in SMMEs.

2.3 Security Culture

Based on the literature review, most researchers define security culture in their own perspectives. These perspectives are discussed in detail below.

According to Schlienger and Teufel (2003), security culture is a set of moral values, shared by everyone in an organisation, that decides how individuals are required to consider security and determine how people are expected to think about security. A security culture is essential to having an effective personnel who are free from danger or cyber threats. Security culture encapsulates all socio-cultural processes that provide back-up to the technical security

measures to ensure that information security becomes a standard process or activity of the users on a daily basis.

According to Martin and Eloff (2002), security culture is being explained as:

- A combined units of information security characteristics that are valued within the service organisation;
- The postulation or assumption on what is tolerable or adequate and what is not based on information safeguarding;
- The postulation based on what information safeguarding conducts is instigated and what is not;
- The technique towards what individuals act in parallel to information safeguarding within the service organisation.

Dhillon, (1995) defined security culture as the overall behaviour within an organization that add value to the safeguarding of all information.

Recent research on information security culture theory had encapsulated theories pertaining to the concept from difference perspectives. Details include organisational culture (Lin and Chang, 2007); organisational behaviour (Von Solms and Van Niekerk, 2003), and as a part of national culture (Chaula, 2006). According to these research studies, it was observed that information security culture comprised of a number of unrelated factors that influence the behaviour of anyone within the vicinity of the organisation.

According to Schlienger and Teufel, (2002), the information security programme disregards the human element that forms part of security culture and focusses mainly on technical and procedural processes. Most organisations view users as security opponents rather than as security champions of the service organisation. According to Van Niekerk and Von Solms (2010) information is regarded as one of the most valuable assets to any service organization

and protecting it becomes important to ensure the organisation can provide services to their customers.

By embracing the security culture within the service organisations, employees, 3rd parties' contractors, and visitors can assist in minimizing vulnerabilities from both internal and external attacks (Lacey, 2010). By embedding the security culture in employees behaviour, the organisation can rest assured that their ICT components are being safeguarded (Meyer, 2005). To embed a security culture in service organisations, they will require a behavioural change with regards to security. Before embarking on changing the behaviour towards a security culture, the service organization must be clear in their vision and have a coordinated strategy (Ogbonna and Wilinson, 2003). The strategy will ensure that participation is consistent, doable and meaningful. Before any process could commence for the inception of the programme to change behaviour towards a security culture, whether it is small or big, it is imperative for the organisation to be clear on the following (Chang et al., 2007):

- The objectives must be clear, this entails both vision and strategy;
- The size and scale of the change must be determined, this entails gap analysis (the present state versus the future state);
- The process to implement the change must be clear and this include any required interventions;
- The service organisation readiness for the changes including the time required for the change, management support and availability of resources;
- How the process will be communicated both to the important stakeholders and the targeted audiences; and
- How the evaluation and reviews of the change will be measured, which includes the key performance indicators.

Currently there is no one size fit all for behavioural changes toward the security culture, however, each organisation uses an adapted method to suit their particular needs and requirements.

Information security culture provide guidance on how processes are followed in organisations, pertaining to information safeguarding, in line with the objective of shielding information assets and eventually persuading personnel's' security behaviours. According to Von Solms and Van Niekerk (2010) information is one of the critical strategic assets of any service organisation and securing it proved to be significant to ensure a stable economy. According to Von Solms and Van Niekerk (2010) the setback of reaching a protected work place for information assets in an organization is related to the activities and behaviours of personnel when dealing with the information assets. With the latest research on data breach it was highlighted that employees could be the reasons for numerous breaches whether intentionally or unintentionally (Verizon, 2012). The ICT market or environment is characterized as being very competitive as SMMEs are providing different services to their customers on a 24/7 basis. Therefore, for SMMEs who want to survive, it is essential to adopt ICT security culture. Theory reviews have highlighted that ICT security culture is a vital determinant in keeping an acceptable baseline of information safeguarding in organisations and has even proclaimed that only a substantial change in security culture can minimize the number of security breach incidents experienced (Maynard et al., 2007).

A study steered by PWC (2013), specified that human errors, and not technology, are the instigators among numerous security breaches experienced by service organisations. Information system security activists have recommended that organisations can influence personnel's behaviour by adopting ICT security culture that encourages security-awareness and adherence to security governance processes (Von Solms and Von Solms, 2000). According to Eloff and Da Veiga (2010), an information security-conscious culture will curtail dangers

towards the information resources and minimize the dangerous misbehaviour of insiders towards the information assets. According to Furnell (2007) organisations should make some efforts to build ICT security culture and integrate its practices into the corporate culture to ensure that internal personnel have the essential knowledge to act accordingly. An organisational culture that embraces the information communication technology ethos will reduce threats to the information assets and will eventually minimise the risks of internal users misbehaviour and detrimental interaction with the information assets (O'Brien et al., 2013). According to O'Brien et al., (2013) continuous usage of Bring Your Own Device (BYOD) and mobility by personnel will force the organisation to implement an appropriate rigorous information and communication technology security culture. After studying the users security behaviour, it was recommended that strengthening an organisation's security culture could be beneficial as employees will be in a good position to know the acceptable and non-acceptable behaviour within the service organisation (Nelson et al., 2010). According to Nelson et al., (2010) having a clear understanding of the complex dynamic and uncertain features of personnel who perform unauthorised and authorised information security activities is viewed as critical and is an extremely challenging responsibility.

According to Schlienger and Teufel (2003), information security culture entails all the socio-cultural procedures that support the practical methods to ensure that the information security turns into a standard feature as a daily activity of every employee. The implementation of information security that must be a culture of the organisation should be laid out as follows Schlienger and Teufel (2003):

- Stage 1: Commitment of the management;
- Stage 2: Communication with organisational members;
- Stage 3: Courses for all organisational members;
- Stage 4: Commitment of the employees.

The above stages were elaborated as follows: stage one ensures that there is buy-in from top management and that they are committed to the programme; the following stage makes sure that understanding and acceptance of the programme is communicated to the employees; within stage three, the organisational employees are trained and educated; the last stage encompasses the change of security culture that entails universal awareness campaigns and specific security processes based on the organization's desire for security .

Assertion made by Von Solms and Von Solms (2000) was that, security culture need to be developed in an organisation by instilling the features of information safekeeping to everyone who is interacting with the information assets of the organisation in a natural way based on their daily functions. According to Alnatheer and Nelson (2009a) most of the developing and developed countries have invested in creating and building information and communication technological infrastructure, however, relating to information security ethos and practices it is assumed to be a difficult subject to be adopted and implemented.

According to Mohammed (2015) the existing literature analyses have not categorized determinants that have meaningful effect on the ICT security culture adoption. However, the few identified determinants entails the following: management support; launching effective governance documents including policies; standards and procedures; compliance enforcement; ethical conduct policies and service organisational culture.

According to Longley (2015) human errors constitutes a major security risk for the majority of the United Kingdom's Small and Medium Enterprises, as a third of SME owners are unconsciously biased about what private information entails. Majority of businesses are failing to provide training that details the procedure to suitably recognize and discard of sensitive data that could lead to expensive information breaches (Mohammed, 2015). The following tips were identified to spot data security errors before they materialise (Ren et al., 2009):

- Scheduling periodical information security audits to spot any problem area;
- Ensure the availability of data classifications;
- Scheduling ongoing information security awareness training.

Benefits of security culture:

- Employees are involved and take accountability and responsibility for security matters;
- Increased compliance level towards the protection of security measures;
- The risk of security incidents and breaches is minimized by inspiring employees to reflect and make decisions in more security conscious manner;
- The probability of employees reporting activities or behaviour of concern is high.

Security culture is the backbone of all security aspects of the organisation as it highlights how personnel should behave within the SMME environment (Kankanhalli et al., 2003). By virtue of understanding the characteristics of security culture, it will be easier to employ the same process or method to information security culture (Greene and D'Arcy, 2010). Information is the blood of every organisation as such it must be protected accordingly (Scarrott). Security culture is laying a solid foundation within every organisation and information security culture is depending on it. The next section deliberates on the significance of information safekeeping culture and its definition as described by multiple researchers.

2.4 Information Security Culture

Information security culture revolves around the awareness of and attention to information safety problems and policies (Margulies et al., 2015). It can be perceived that the information security culture is part and parcel of the organization ethos because the information security has been viewed as an organisational function or activity. According to Mirza and AlHogail (2014) information security culture could be viewed as a subculture that is concentrating on

information security and placing more emphasis on making information safekeeping a normal procedure within the day to day lives of users.

In most of the theory reviews, information security is linked to the technological environment whereas the risk perception is associated to human characteristics. A great information security culture ensures that employees will always be in a position to know what to do should an unforeseen cyber threat materialise. In most cases, an information security culture is developed when users or employees interact with the information security procedures and controls. According to Xiong et al., (2013), in order for the organisations to understand the varied range of likely information security threats, further emphasis must be on creating and increasing a security aware culture. According to Mirza and AlHogail (2014) information security culture is expressed as the accumulation of viewpoints or perceptions, attitudes, morals, expectations and know-how that provides guidance on how processes are to be followed within the organisation to make sure that there is consistency with the intention for safeguarding the data assets. This will also influence safety behaviour of in an environment that is endeavouring information security to become the second nature.

The requirement is to ensure that personnel comprehend the risk they might face regarding the information that they are processing on a daily basis. According to Da Veiga and Martin (2015) a culture of data safekeeping should be upheld where evidence of acquiescence attitudes for all critical and classified information and data is maintained. As per Da Veiga and Eloff (2010), the organisational values ought to be taken into consideration during the cultivation of data safekeeping principles to make certain that the correct security measures are recognized and implemented in a successful way.

The research paper that provided most details pertaining the ICT security culture framework was made available by Warren et al., (2006). According to Eloff and Martins (2002), research

on information safeguarding philosophy highlighted that an accommodating ethos that involves an information safeguarding ethos that is a shared way of a transcendental nature and can be designed by an organisation's management. Nosworthy (2000) indicated that the organisational culture plays a significant part in data safety, as it permits the organisation to counterattack the changes experienced by its structure. As more theory reviews agree regarding the significance of the safekeeping ethos for ISMSs, no transparent description of the perception of security culture occurs, and several viewpoints exists (Ruighaver et al., 2002);

- Dhillon (1997) has an eagle-eye view pertaining to the concept of security culture, and describes it as the behaviour of an organisation's personnel where they place more effort on the safeguarding of data, information and know-how;
- Loch and Straub (2002) advocates that with Information systems, it is constantly presumed that an individual belongs to a sole principle, and these authors therefore proposes using the theory of social identity as a basis for research into the information security culture.

The idea behind the social culture is that everyone is influenced by ethical aspects, each country's legislation and the organisation of security. This culture influences the way in which the individuals interprets the significance and importance of information security. Below are their positions:

- Siponen (2000) highlighted that the perception of information security is a situation whereby organisational personnel are aware of their task to keep the organisations data safe. These tasks are categorised in dual folds: (i) the application model that set, accredit and institutionalise events; and (ii) the content or characteristics of the situation;

- Vroom and Von Solms (2004) on the other hand, suggested the formation of a training ethos and collaboration with personnel on the basis of the measured acceptance of the organisation's safekeeping supervision, personal values and personnel behaviour;
- Martin and Eloff (2002) characterizes the data security culture as an arrangement of data security attributes, for example, respectability and the accessibility of data;
- Ilvonen and Kuusisto (2003) recommends a process within which the security culture is formed based on the interaction between the focal model and their features;
- Lastly, Mauriel et al., (2000a) considers the security culture to be a key part of ISMSs and has built up a general model for data security which depends on eight measurements. Ruighaver et al., (2002) applied these eight measurements to the territories of data security and recognized the vital components of data security in each measurement.

According to Murphy and Taylor (2004) SMMEs exhibits concerns pertaining the difficulties involved in nurturing a data safeguarding culture. The truth of the matter is that the security culture has a progression of extra issues in respects to their implementation. According to Warren et al., (2006), when compared to the larger organisations SMMEs are in particular intolerant about considering a data culture because of the following reasons:

- SMMEs lack of time and learning required to facilitate data security or to force a data security culture in a proficient way (Helokunnas and Livonen, 2003, Gennatou et al., 2000);
- SMMEs are incapacitated to have governance documents on their sites or describe the responsibilities of their data structure personnel Helokunnas and Livonen (2003);
- When contrasted with established organizations, SMMEs are progressively defenceless to national impacts, for example, changes in legislation Warren (2003).

Based on the several security management frameworks (Schlienger and Teufel, 2002; Jedynak and Bugdol, 2015; Martin and Eloff, 2002; Gani and Zakaria, 2003; Vroom and Von Solms, 2004; Kuusisto and Helokunnas, 2003; Von Solms and Von Solms, 2004) for the improvement of a data security culture within their environment, these frameworks are largely oriented towards the larger organisations.

2.4.1.1 Information security culture objectives

Torkzadeh and Dhillon (2006) highlighted sixteen information system security objectives. Inasmuch as these objectives are not by definition declared as part of information security culture, they share similarities with the already identified aspects of security culture. The objectives are outlined as follows:

- Understanding personal beliefs / principles – it ensures the creation of an environment in which personnel are celebrated and understood. It also embeds moral values and ethics into the organisational culture;
- Ensuring censure – it ensures that there is a creation of fear of undesirable responses prompted by noncompliance, including, but not limited to job losses, being mocked, etc.;
- Improve understanding of financial status of personnel – this objective ensures no monetary benefits are received for supplying competitors with information;
- Understand personnel characteristics – this ensure understanding of the individual characteristics lifestyle of employees.
- Maximise accomplishment of personal needs – this objective provides choices to the employees regarding position improvement and to be able to eventually improve self-actualisation needs;

- Understand the work condition – the objective is creating an atmosphere or environment where revenge will be the last resort and to ensure that there is a minimum of disgruntled personnel;
- Promote responsibility and accountability – ensure the clear delegation of responsibility and advocate for accountability by maximising the level of commitment from employees;
- Ensure obtainability of information – this objective ensures that there is a creation of procedures that will make sure that the correct information is available to all employees;
- Improve authority structures – communicates the definition of delegation of authority to all personnel which will minimize excessive control and eventually minimize access to the information stores from diverse positions;
- Ensure legal and procedural compliance – eliminate any ignorance towards laws; lower the tolerance of information misuse; ensure personnel have an understanding of legal and regulation processes; develop a procedure that allows for an information audit trail;
- Clarify centralisation or decentralisation – ensure that there is an adequate balance between centralisation and decentralisation of functionality within the enterprise;
- Establish ownership of information – educate personnel about ownership within the organisation and the significance of confidentiality. Subsequently create a contract of confidentiality;
- Optimise work allocation practises – share the workload in an equitable and optimal manner. Subsequent to this process, assess and adjust free time;
- Maximise awareness - to ensure that there is an understanding of the organisational culture and encourage awareness by balancing the practical and communal facets of information safekeeping system;

- Provide open communication – ensure clear communication in between the Information Technology department and other personnel in order to encourage information sharing.
- Increase trust – increase loyalty, show employer belief in personnel, and develop an environment that encourage organisational responsibility.

2.4.1.2 Assessment of Information Security Culture

The significance of having the information security culture instrument within the organisation assist to measure if the baseline of information security culture is improving the safeguarding of data resources. The assessment outcomes from the instrument provide a blueprint to positively encourage the development areas pertaining to the personnel behaviour and attitudes. According to Da Veiga and Eloff (2010) the baseline blueprint will measure and report on the organisational security appetite pertaining to the information security culture. According to Cavusoglu et al., (2010), personnel's' attitudes towards the information security are mainly impacted by three aspects, cost of compliance, benefits of acquiescence and price of no acquiescence. Based on the viewpoint of Cavusoglu et al., (2010) the benefits of acquiescence is formed by inherent advantage, safeguard of possessions and return on investment, whereas the price of acquiescence is designed by labour disturbances. The price of non-compliance is formed by inherent cost, vulnerabilities of possessions, and consents.

According to Da Veiga et al., (2007) there are many methods to test the information security culture in companies but the most effective method is using Likert scale for answering questions whereby employees choose a number set between a low number that represent strongly disagree and a high number that represent strongly agree. Below are some of the statements linking to the questions of information security culture within the organisation:

- The organisation safeguards both its information and data assets adequately;
- It is significant to comprehend cyber threats to both the information and data assets;

- Threats to safeguard the information and data assets are measured sufficiently in my business unit;
- Information security is essential within my business unit;
- All the information assets used on a daily basis should be protected, whichever physically or automatically;
- I'm confident that the section employed in will endure should the disaster struck resulting in the loss of systems, people and/or buildings;
- I feel protected within the place where I work;
- I trust that both the information and data I'm working with is sufficiently safeguarded.

2.4.2 Vital Characteristic of Information Security Culture

According to Van Niekerk and Von Solms (2010) the elementary description of information security culture is one whose net effect would be in-line with the minimum requirements for other industry standards. According to Nel (2017) the most important information security culture aspect includes two themes, namely:

- Information security culture framework;
- Information security awareness and training program initiatives;

2.4.2.1 Information security culture frameworks

The information security culture models or frameworks could be utilised to begin or launch an information security culture in an organisation. The significance of the frameworks highlight the variety of components constituting an information security culture and demonstrate the collaboration and impact between those components; and afford better understanding of information security culture (Da Veiga, 2008). Various conceptual frameworks or models were proposed by researchers to help organisations in launching or establishing an information security culture.

The framework from Da Veiga and Eloff (2010) emphasised more on practical, bureaucratic and personnel behavioural components by highlighting the cohesiveness of those aspect towards the information security culture. Table 2-3 below shows how the information security components influence employee's behaviour subsequent to cultivating a robust information security culture. The arrows in Table 2-3 depict how the information security culture is impacted. The main constructs or environmental setup influences the information security attitudes in the company that will cultivate the information security culture.

Table 2-3: Features of Information Security Culture

FEATURES OF INFORMATION SECURITY CULTURE				
Information security types →	Influences →	Information security behaviour →	Cultivates →	Information security culture
	Organisational Tier	**Group Tier**	**Individuals Tier**	
Leadership (management) and Governance	Sponsorship; Strategy; Governance; Risk management; ROI			Organisational artefacts and creations; organisational values; Organisational assumptions
Security management and operations	Legal and regulatory	Program organisation		
Security Policies	Policies; Procedures; Standards; Guidelines; Certifications; Best practices			
Security program management		Monitor and audit; Compliance;		Group artefacts and creation; Organisational

FEATURES OF INFORMATION SECURITY CULTURE				
Information security types →	Influences →	Information security behaviour →	Cultivates →	Information security culture
	Organisational Tier	**Group Tier**	**Individuals Tier**	
				values; Organisational assumptions
User security management		Trust; Education and training	Employees awareness; Ethical conduct; Privacy	Group values; Group assumptions
Technology protection and operations		Asset Management; System Development; Incident management; Physical operations; Technical operations; Business Continuity		Individuals artefacts and creations; Individual values; Individual assumptions

FEATURES OF INFORMATION SECURITY CULTURE				
Information security types →	Influences →	Information security behaviour →	Cultivates →	Information security culture
	Organisational Tier	**Group Tier**	**Individuals Tier**	
		management; Physical and environment		
Change management	Change management	Change management	Change management	

Maynard et al., (2002)

Maynard et al., (2002) developed a model that could be utilised to discover the safeguarding ethos and assess its robustness within the organisations. The framework was established on the prototypical projected by Mauriel et al., (2000a) in line with the morals that ensure an actual Total Quality Management (TQM) culture. The researcher Maynard et al., (2002) used the TQM values established by Mauriel et al., (2000a) to the security culture, establishing it into eight cultural areas. The researcher correlated information security to those eight values linking them to several case studies actioned within the organisations.

The eight values are: the base of certainty and reasonableness; the nature of time horizon; inspiration; steadiness against transformation, modernization, and individual development; positioning to effort, duty, and co-workers; separation against teamwork; regulate, harmonization, and accountability and alignment and concentration.

The authors are of the view that security is significant within the organisation and should be supported by maximising the participation, to ensure that the decision making is aligned to the security objectives. The research by Maynard et al., (2002) must be praised for their allusion to their long-term thinking and accepting change also by highlighting that information security should be treasured. The case studies that was steered by the above-mentioned team assist in the realism of their research viewpoint. The challenge is that, their research never gave a resolution on how to advance the value of data safeguarding attitude within the organisations.

Schlienger and Teufel (2002) offered a model for managing the data safeguarding attitude in the organisations grounded on the philosophy on internal marketing. The researchers highlighted that managing the information security culture is a living process of assessment, change and/or maintenance. The framework comprises of five major areas that entails: pre-assessment, tactical forecasting, operational scheduling, execution and post-assessment.

The assessment procedure entails identifying the major gaps that are amongst the governance guidelines and the viewpoint of personnel; also categorizing the environment that seek enhancement. ***The tactical forecasting*** procedure is initiated by outlining the strong purposes for the enhancement of a suitable safekeeping ethos that can be well-defined. Subsequent to the above process would be to categories members of an organisation into a variety of groups and to put in place special measures for each category. ***The operational scheduling*** entails internal communication, top management support, also the safekeeping alertness and training program. ***The execution stage*** is categorised into four separate phases: the managers pledge, inside communication, knowledge allocation and pledge by employees. The setback of the framework is that it still needs more practical application to test the enactment of the anticipated framework to determine if it could transform or preserve a suitable safety ethos.

Gani and Zakaria (2003) established a conceptual information security culture checklist that could be utilised as a guidance to the management in developing the data safety ethos in organisations. Checklists is significant as it can also be used to raise personnel awareness pertaining how to handle information in a secure manner. Based on the authors Gani and Zakaria (2003), a checklist has been referred to as a theoretical as it is not comprehensive based on data safety as it periodically changing with new ideas emerging; thus, the checklist will required periodic update and adapted to suit the current situation.

According to Gani and Zakaria (2003) the checklist relies on the three cultural levels developed by Schein (1985) namely: surface manifestation; values; and basic assumption level. Inside those three levels a variety of elements are defined, for example, on the surface manifestation level that encapsulates artefacts, norms and languages.

The research by Gani and Zakaria (2003) shows an integration between organisational culture and information security which could be utilised to enhance data safety within the company. The checklist can provides an adequate base for understanding what could be considered into deliberation while developing a datasafety culture. Within the proposed checklist an organisational behaviour was not incorporated and that could have been useful to comprehend how the employees behaviours could be influenced.

Warren et al., (2005) deliberated the change procedure on the organisational transformation and proposed the use of theoretical change over typical change for changing the data safety attitude within emerging companies. The proposed conceptual framework was adapted from the transition process framework developed by Bridges (2003) that highlight that the effectiveness transition of information security culture is categorised into three stages:

- ***Ending:*** within this stage, management team should encourage employees to forget about the historical points and progress on. Announcement or engagement is a

significant tool in this phase to assist employees to alter how they view things, in an innovative and diverse way.

- ***Impartial Sector:*** this stage is regarded as being the greatest multifaceted and perplexing stage within the change process, during which management should define the prerequisites and provide guidance to the employees.
- ***New Beginning: during*** this stage anxiety about the start of the information security transition occurs, which require management to remain prepared to support the innovative environment.

The major contribution of Warren et al., (2005) is based on providing academic researchers and commited managers with a thoughtful explanation of the change procedure for achieveing data safety value transition in SMMEs. As the authors highlighted, the proposed conceptual model still need validation of its applicability within different orgnanisational settings.

Von Solms and Van Niekerk (2005) defined a model for security cultural change, titled "An all-inclusive context for the nurturing of data safety sub-values within an organisation". The model highlighted key aspects, including results-based tutoring, business knowledge and business ethos in order to take into consideration the acquaintance and attitudes of personnel pertaining to data safety. The significance behind the model was based on the assumption that personnel having enough know-how, coupled with erroneous behaviour or attitudes on data safety, as well as personnel with the acceptable attitudes but lacking in knowledge, should definitely not be the pursued individuals to handle the data in a protective way. Therefore, personnel should be educated. Von Solms and Van Niekerk (2005) opted for outcome-based learning as a way to comprehensively look into know-how and attitudes and to certainly encourage data safety ethos in a company.

In-line with their framework, the organisational culture levels of Schein was used to improve the understanding of data safety culture Von Solms and Van Niekerk, (2005). Based on the original Schein model (1985), three organisational culture levels was determined, namely artefacts, values and assumptions. Von Solms and Van Niekerk (2005) added the fourth level that is knowledge. Those four levels where used as a baseline of safety in which a smallest point of departure is equating the dissimilar cultural baselines. Based on the researcher's assessment for the ideal security culture, all four outlined levels have to be stronger than the acceptable minimum baselines and should be interrelated to each other. The viewpoint held by both Von Solms and Van Niekerk (2006) does not encapsulate organisational behaviours links to the proposed model. For the model to be regarded as useful to the traditional organization instrument more study need to be undertaken.

Lin and Chang (2007) presented a model that looked into the associations between organisational values and Information Security Management (ISM) to ensure that influences of organisational value constructs are effective on the efficiency of realizing ISM. Organisational cultural constructs entail the flexibility-established constructs like cooperativeness and innovativeness; and control-oriented attributes like steadiness, and efficiency. In order to assess the impact empirically, a questionnaire where used and regression analysis was employed to analyse data.

The significant input from Lin and Chang is in providing an improved thoughtfulness of the association between various organisational cultural constructs and the efficiency of ISM implementation, which provides a better picture of how to ensure the successful implementation of information security initiatives.

Ahmad et al., (2009) presented a model that helps organisations to measure the span of the required data safety values entrenched within the organisational values and discover the nature

of association amongst them. The proposed research framework was adapted from the literature review combined with the cultural viewpoint of Mauriel et al., (2000b). The model apprehended three categories of associations between organisational culture and information security culture (ISC): ISC is not a portion of the organisational culture but is a sub-culture within the organisational culture, which is entirely entrenched within the organisational culture. The initial category of association is where employees within the organisation are not involved with security implementation, have minimal knowhow about information security and feel excluded from having responsibility towards security challenges. This is a result of the data safety activities being engaged by the information technology section.

The key contribution of Ahmad et al., (2009) is that they pointed out the association between business values and data safety culture and also proposed a model that provide suggestions for organisations trying to acquire the desired level of ISC to make sure that employees are influenced in data safety activities and behaviour to ensure safeguarding of organisational data assets. The main drawback of the proposed model is that it had been tested on a minimal scale within only two organisations, therefore, additional experimental research is required to corroborate the significant of this model.

2.4.2.2 INFORMATION SECURITY AWARENESS AND TRAINING

According to Peltier (2005), during the process of creating and awareness programme, it is significant to take the business objectives into consideration to ensure that they are aligned and that personnel understand the significance of the programme and lastly making sure that the programme is explained in a language that is understood by all personnel. According to Peltier (2005) an awareness programme should meet the following business objectives:

- Risk analysis – to ensure that factors that could potentially become problematic are identified and assessed.

- Risk assessment – to ensure that possible threats to organisational assets are determined and prioritised so that the best appropriate security measures could be put in place.
- Policies – Ensure that the achievement and purpose of safeguarding the data is highlighted, and to indicate what is expected from the personnel during the usage of the organisational assets.
- Procedures – it ensures that a step by step process to complete each task is detailed and also help in the discouragement of asset misuse and fraud and clarify the return on investment.
- Standards - it prescribes the baseline on process or tasks that should be done.
- Business continuity planning (BCP) – it ensures that all the procedures to follow during or after an incident has occurred are followed.
- Effective communication – it ensures that there is a clear chain of communication between employees, management structure and the security officers.
- Compliance – it ensures that there is a monitoring process for compliance to the security objectives.

According to Peltier (2005) the value of business objectives within an awareness programme is important as it ensure that those in managerial positions take the process seriously. Grounded on the corporate objectives, the organisational culture will dictate the aspects of data safety values to be emphasised.

The concept of data safety principles is significant within a service organisation; however, it is not complete if the management process is not understood and embraced. ISMS act as an umbrella ensuring that all features of ICT safety culture are in motion. ISMS encapsulate all the processes to ensure the realisation of ICT security systems, information and data assets protection. Within the organisational areas, ISMS is regarded as a bundle of policies and

procedures for thoroughly managing an organisation's critical information and data assets. The main objective of ISMS is to lower the risks and ensure business continuity by proactively minimising the impact of a security breach. The next section deliberates on the significance of ISMS in organisations and what it entails, to make sure that business strategic assets are protected, and security culture is embraced.

2.5 Information Security Management System

According to Sanchez et al., (2015), ISMS is well-defined as a managing structure utilised to create and preserve the protected area of information and data assets. The significant goal post pertaining ISMS is to make sure that procedures and measures required in managing the information and communication technology are put into practice and maintained. To develop data security values within organisations, various approaches are required to be taken into consideration based on policies, information security awareness, training and education (Gennatou et al., 2000). According to Velilla and Rosanas (2005) management initiatives cannot ensure major impact on personnel behaviours. Schultz (2005) asserted that it is important to grant the special care on personnel behavioural aspect.

According to Shain and Longley (1991) data safekeeping could be described as "the protection of, also retrieval from, unauthorised or unwanted demolition, alteration, revelation, or usage of data resource, either unintentional or intentionally." The end objective of data safety supervision is averting or minimizing the harm to the organisation assets by developing and sustaining the quality of information infrastructures, processes and their procedures Von Solms and Van Niekerk (2005). According to Gupta et al., (2014) there are ten areas that represent all information security management events. The areas are discussed as follows:

2.5.1 Top Management Support

Senior managers support provides key guidance throughout the planning, designing, developing, deploying and post-deploying of an information security management system. As all users or employees will be observing management commitment to the process, their key mandate is also to encourage constructive user attitude towards the data safekeeping supervision process within an organisation. Several deliverables linking to senior management responsibility entails the following:

- Compliance toward the information security policies;
- Attitudes of management versus all employees;
- Organisational security culture and overall risk management;
- Ensure the effectiveness of information system security;
- Provisioning of resources towards the information security efforts; and
- Financial backup to setup the information security infrastructure.

The significant aspects to guarantee appropriate management support entails the following: "top management must understand the important of information security, top executives attend information security meetings, top executives availability during the information security related decision making, and allocations of resources including financials and manpower for information security activities" Gupta et al., (2014). According to Cavusoglu et al., (2010), to ensure that all users comply with all the security policies the process will be influenced by: the compliance benefits that entails rewards, inherent benefits and safety, noncompliance cost that entails vulnerabilities, inherent cost and sanctions.

The following segment deliberates about the information security policy.

2.5.2 Information Security Policy

The details below highlight the significance of data safekeeping procedure mapping to safety culture.

An information security policy is a document that highlight how a service organisation put a strategy or a plan in place to safeguard its infrastructural assets. It highlights the direction and management support of all the information security activities, or in a nutshell, is a document outlying management intent. In most cases the document entails generic statements pertaining to organisational goals, purposes, views or beliefs, morals and responsibilities, and frequently designates the process to obtain them Saint-German (2005).

The key focal areas of an information security policy include the following:

- Policy framework;
- Policy essentials, characteristics and exposure;
- Design, execution and adoption;
- Process for reporting information security incidents;
- Alignment of information security policy to the organisational strategy;
- Aligning employees or users behavioural attitudes towards procedure acquiescence;
- Highlighting pivotal function of data safekeeping vigilance within the policy compliance;
- Ensuring policy communication throughout the organisation;
- Ensuing policy effectiveness to achieve the intended objectives; and
- Highlighting the policy violations to the users.

Significant areas within an information security policy entails: policy documentation of the organisation, roles and responsibilities should be defined in simple understandable terms,

policy documentations are reviewed regularly or if changes occurred, and lastly the processes for information security policy must be clearly defined and documented.

The following section deliberated into information and data safekeeping training towards the safety values.

2.5.3 Information Security Training

The significance of establishing data safekeeping training is to construct or embed knowledge in employees to make sure that it yields the relevant and required skills and capabilities besides the technological aspects. Everyone having access to the data and information must be knowledgeable with regards to information security. In most cases training takes longer than awareness as participants should have a strong understanding of the procedure. The expectation is that users or employees should be capable to resolve any difficult issues after attending the training programme. Significant areas pertaining to the information security training entails the following:

- Meeting all the training requirements of personnel;
- Highlight differences between training versus awareness and education;
- Used as a data safekeeping training instrument; and
- Used as a data safekeeping compliance instrument.

The key deliverable for the information security training to all the users of information and data entails the following: service organisations should conduct more information security training to the users, and an information security advisor must be handy to organize the information security roles Gupta et al., (2014).

The following sector deliberates about the information security awareness.

2.5.4 Information Security Awareness

Though the contents of awareness are not similar to the contents of formal training it should not be viewed as informal training. The significance of awareness appeal to the attention of users towards the security subject and provide lessons for basic countermeasures. The significance of awareness is to let users to identity the issues for information security and communicate to them on how to respond accordingly. According to Katsikas (2000), information security programmes teaches the short-term, instant and explicit knowledge that must be repetitive to ensure constant awareness.

The significant areas of information security awareness entails:

- To ensure compliance to the information security policies;
- Ensure changes in information security behaviours;
- Mitigation of gaps between talking and action;
- Ensure shift of knowledge and attitude of users;
- It is not static, and its process is ongoing; and
- To ensure that all users receives the message;

The significant construct for information security awareness involves the following: "all personnel are aware of security policies and guidelines for the service organisations, programmes are organised to ensure users are conscious about information security policies and guidelines of the organisations, users roles and responsibilities are simplified and properly communicated, users are versed in terms of the do's and don'ts of information systems and assets' acceptable and unacceptable expectations, and guidelines for violating the information security in terms of punishment is communicated Gupta et al., (2014)"

The next section delves into the information security culture.

2.5.5 Information Security Culture

The information or data safekeeping values is the supervisory aspect details how processes are followed within an organisation pertaining to the data or information security. The current section takes centre stage in the whole research study. According to Mirza and AlHogail (2014), the main focal point of information security culture is to influence user's security behaviours. A vigorous information security culture is in existence when all personnel are vigilant pertaining their roles and responsibilities, are aware of any potential risks and mitigating processes as well as the consequences of non-compliance and by refining measures to improve the process to safeguard the information within the organisation. The focal area of information security culture entails the following:

- Organisational values are embraced by all;
- Ensure compliance to data and information safekeeping policies;
- Ensure the understanding of the organisational security culture proportions;
- Changing of attitudes, norms, views, values and knowledge of users and other stakeholders; and
- Shifting the user's information security behaviours.

The key areas within the data and information safekeeping values entails the following: "creation of data and information safekeeping processes between all personnel, ensure that information security become the first priority to all personnel, ensure that information safeguarding become the norm to all personnel; ensure that there is a dedicated team to run the programme, confirm that all employees are conscious pertaining cyberthreat towards their information and data assets, and to ensure that there is a specific forum that provide management with direction and support" Gupta et al., (2014).

2.5.6 Information Security Audit

To conduct an information security audit a sovereign organisation or an individual must scrutinize and assess the security of an organisational information structures. The process is to assess the eminence of data and information safekeeping controls, to assess user compliance and recommend changes to enhance the comprehensive information security. According to Saint-German (2005) it is imperative to conduct an annual audit and subsequent to that be certified based on certain standards. Main areas that should not be overlooked in an information security audit include:

- Planning of the information system risks ensuring that business is aligned;
- The human factor;
- The internal audits;
- 3rd party audits; and
- Monitoring of compliances pertaining to the rules and guidelines.

The key factors that included in an information security audit are: a committee need to be established to conduct information security, an organisation must periodically conduct internal information security audits, and lastly, the business has to introduce an external audit routine Gupta et al., (2014). In as much as auditing is significant, it is also imperative to have best practices in places.

2.5.7 Information Security Management Best Practices

The importance of having best practice in place is to ensure that organisations assess any possible security risks, to confirm that proper security controls and countermeasure are in place, and to conform with the organisational regulations and legal requirements. In most instances best practises are based on standards that are flexible as they can be improved to a variety of organisations Saint-German (2005). Key significant factors pertaining to best practices

includes: the clean desk policy is in place, anti-virus software is used within the organisation and are up-to-date and able to protect against the cyber threats, a suitable authentication process is essential for the external connections like Multi Factor Authentication (MFA), to ensure that proper acceptable controls are in place, risk assessment and management processes are adhered to and followed, and to ensure that systems are upgraded or updated based on the structured plan and not in an adhoc fashion.

2.5.8 Asset Management

Within the computer infrastructure there are three important assets namely data or Information, hardware and software. Based on their formation, each of those parts are faced with several vulnerabilities that need to be monitored throughout the information security forecasting phase.

To accurately manage the organisational assets, all assets need to be identified, the potential risk needs to be understand and measures should be in place to mitigate or to prevent them should a security threat materialise (Margulies et al., 2015).

Major problems of asset management entails:

- Asset categorization and control;
- Asset ownership;
- Risk assessment;
- Asset threats and safety; and
- Access regulation to information technology facilities.

2.5.9 Information Security Incident Management

To ensure that the organisation is ready in terms of security incident response, a document titled incident response plan will be utilised to ascertain how to deal with the incident. According to Margulies et al., (2015), the procedure should outline what constitute an incident,

recognize or identify the accountable party should the incident materialised, and should also outline the action to be taken.

According to Gupta et al., (2014), The significant factors pertaining to the information security incident management are:

- Documented business continuity plan (BCP) and disaster recovery plan (DRP) must be in place within the organisation;
- Procedures must be clearly defined on what to do together with on who to call for support during the security incident event;
- disciplinary action must be taken against anyone violating the information security rules;
- Both the BCP and DRP are discussed and communicated to all the users;
- To confirm accessibility and reliability of critical data processing and communication services, a backup and recovery processes must be in place;
- If a backup and recovery processes are in place, the organisation can survive the calamity that may result in the loss of infrastructure including, but not limited to: systems, buildings, and historical records; and
- The information security measures must be reviewed regularly, the least being annually.

According to Gupta et al., (2014), it has been proven that both the asset and information security incident management are interrelated within the information security management.

2.5.10 Information Security Regulation Compliance

To ensure data and information security systems compliance with both standards and guidelines as dictated within the security policy and any related security documentation, a regular security audit must be observed. It must be explicitly outlined that failure to comply with the processes will lead to inadequate information security is punishable. Both the

independent team and internal staff must ensure that information security compliance is adhered to Margulies et al., (2015)

Main issues with the information security regulation compliance includes:

- The information security standards;
- Both the information security laws and regulations;
- Ensuring compliance to both the information security rules/procedures/standards; and
- Adhering to organisational data safekeeping policies.

According to Gupta et al., (2014) the significant aspects of regulation compliance entails:

- Both data privacy and polices must be in place within the organisation;
- To ensure compliance and acknowledgement of processes all users should sign both the data privacy and the protection agreement;
- External employees like 3rd party vendors must sign both the data privacy and protection agreement while doing their function with the organisation;
- Organisation must adhere to the industry standards pertaining to the information security management;
- Ensure that a dedicated forum for observing organisational compliance to data protection is in place.

Within the technological innovation adoption space, there are many adoption models used to implement the proposed framework constructs as a method of assessing how effective or efficient they are. The following section highlight several models used to adopt theoretical models or frameworks.

2.6 Adoption Models

According to Mohammed (2015), adoption is the process of accepting and continuing utilizing the invention, amenity or idea. Before any consumer could decide to adopt an innovation or services they must go through the process of being educated, convinced, making decisions, confirming and finally go through the process of implementation.

Technology Acceptance Model (TAM)

The TAM framework is an augmentation of the Theory of Reasoned Action framework created by Fishbein and Ajzen (1975) to clarify client acknowledgment or acceptance of information systems as represented in Figure 2-1 below.

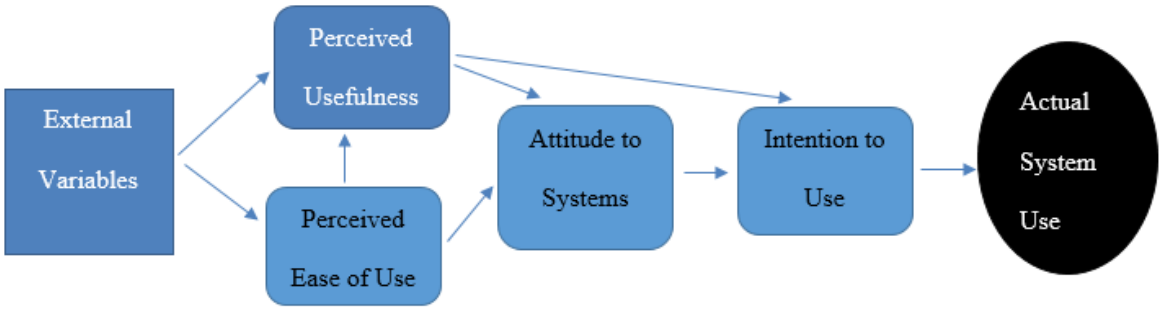


Figure 2-1: Technological Acceptance Model

The above intention-based framework dictates how users could be in either acceptance of the usage of technology or discard it on the bases of principles which impact attitudes towards the intention to use the proposed systems. According to the model, there are two factors that have significant impact on the acceptance of IT innovation, namely Perceived Usefulness (PU) that "denotes the level to which individuals trusts that utilising a specific structure will improve their performance" and Perceived Ease of Use (PEOU) that "denotes the degree to which a person's trusts that utilizing an exact technology will be free from exertions" (Nahlik et al., 2009). According to Bwalya (2009) the TAM framework has been put into usage by majority of researchers in studying the acceptance of technology. The framework has been viewed as

the leading model for elucidation and envisaging the system use. The drawback of the model is that it considered the individuals but disregarded or overlook the social procedures of information systems progress and application as well as the social impact of system usage Bagozzi (2007).

According to Durodolu (2016), the Technology Acceptance Model is one of the established theoretical models that endeavours to investigate the features impacting technology adoption.

Unified Theory of Acceptance and Use of Technology Model (UTAUT) Bala et al., (2013)

The UTAUT framework is an expansion of Davis's (1989) theoretical Technological Acceptance Model, created in an effort to amalgamate the major contending user acceptance theoretical models. Details of the model are shown in figure 2-2 below.

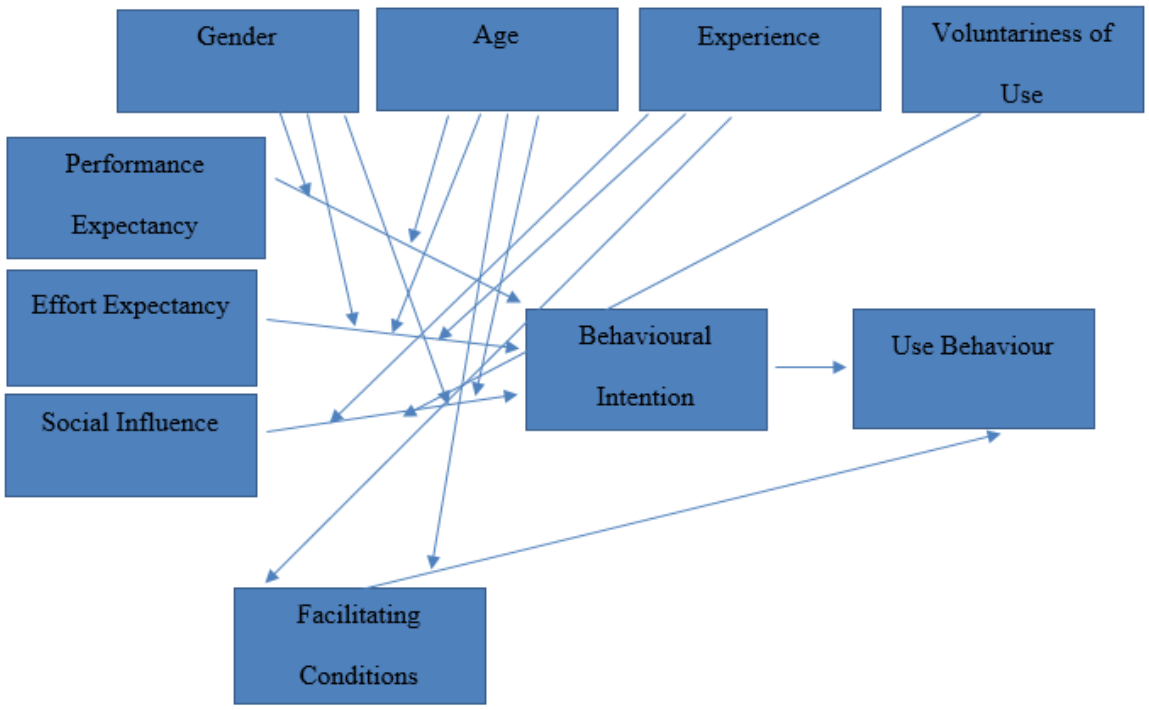


Figure 2-2:(UTAUT) Unified Theory of Acceptance and Use of Technology Model by Bala et al., (2013)

The UTAUT conceptual model addresses the shortfall of TAM on the social aspect, the construct is based within the social influence context. According to Bwalya (2009), the

UTAUT conceptual model assist managers to measure the probability of success for latest innovations as well as comprehending the determinants of technological acceptance.

According to the theory review there are several factors that perform a major function in the specific context of personnel adoption and usage towards the behaviour. These Factors entails: performance expectancy that indicates the level of users trusts that utilizing the innovation will assist him or her to achieve improvements in function performances, effort expectancy that denotes the level of ease relating to the system usage, social influence that denotes the level of users that hope that it is significant for other to trust the new systems, while enabling circumstances denotes the level users trust that the service organisation and its technical equipment in existence will assist in the use of the new system. The drawback of UTAUT conceptual theory is the scales that are used to assess the mail factors which influence the contents validity. It is proposed that there is a requirement to measure UTAUT in future research to make sure that appropriate scales, based on individual constructs, are addressed to remedy the issues experienced with content validity.

Hyland and Sukanlaya (2012) used the UTAUT model to determine aspects prompting the acceptance of innovation in a structure of buildings. Seven constructs were used to determine the acceptance that will lead to adoption process and entails the following: performance anticipation, simplifying environments, determination anticipation, societal effect, personal confrontation to change, senior management backing and regulating variables that entails age, sexual category, education, and computer knowledge. The outcome shows determination anticipation, simplifying environments, and senior management backing having an impact towards the personnel intent to utilize Information Technology.

Naenna and Phichitchasopa (2013) utilised the UTAUT model to examine the factors influencing Information Technology services in healthcare. The outcome shows the construct

having a significant effect on performance anticipation, efforts anticipation and simplifying environments.

Rahayu and Day (2015) developed a model adapted from the TOE framework. Multiple variables were projected to investigate features influencing SMEs in emerging states in accepting electronic commerce. The TOE framework was categorised into four factors namely: technological, organisational, environmental, and individual factors. The outcomes outline that perceived benefits, technological keenness, owner's pioneering, owners' information technology aptitudes and titleholders' information technology knowledge are the determining features that influences Indonesian SMEs in their acceptance of e-commerce.

According to Shoemaker and Rogers (1971) the technological innovation must go through the following phases to ensure that all the correct boxes were ticked:

- Education (Knowledge)
- Persuasion
- Confirmation
- Implementation
- Decisions

Before any innovation can be either rejected or adopted it must go through several phases to test or observe as to whether it will provide the required benefits or not. According to Frambach (1993) this emphasises that the innovation phases outlined by Rogers is the procedure whereby service organisations or individuals go through the process of knowing the innovation. Subsequent to that they establish either positiveness or negativeness towards the modernization as to whether it would be implemented of not. As a result of the preceding phases it will confirm the decisions.

The five innovation phases in the decision process are deliberated as:

Education phase: the preliminary adopter has supplementary knowledge above anyone trying to adopt the innovation at a later stage.

Persuasion phase: this is the phase where self-assurance towards the modernization adoption is established. By envisaging upcoming gratification and foreseeing risk of adoption, the prospective adopter would be developing either encouraging or damaging attitudes towards the modernization adoption.

Pronouncement phase: this phase transpires after the adopter has engaged in events that led to the innovation being either adopted or rejected.

Implementation phase: as per Rogers' assessment, information processing and judgement comes to an end however the behavioural variation commences.

Confirmation phase: this phase only happens subsequent to the adoption of innovation whereby the adopter periodically checks their outcomes of their decisions. In this process, it is possible for the adopted innovation to be rejected after being implemented.

According to Reed et al., (1996), the option for the adoption and eventual implementation of the decision might be separated by action and timeframe. In a nutshell, adoption could be defined as the acceptance and continuation usage of a service that might have impacted the five phases (education or knowledge, persuasion, confirmation, implementation and decision making).

Technology, Organisation, and Environment Framework developed by Tornatzky and Fleisher (1990)

The TOE contextual model established by Tornatzky and Fleisher (1990) (as depicted in Figure 2-3 below) is one of the most popular research frameworks used for the acceptance of technological innovation. Grounded on the TOE model, a conceptual model for ICT security

adoption was proposed to test the constructs. The conceptual model entails six determinants towards the adoption of the ICT security culture within the three factors. The six determinants towards the adoption of innovation as used by other researchers includes: (1) management support, (2) financial resources, (3) organisational competence, (4) perceived benefits, (5) perceived complexity, and (6) government regulation. The above variables are clustered in three context that are: technological factor, environmental factor and organisational factor. The conceptual research model was outlined in this chapter together with its constructs and the relationships hypotheses among the constructs. According to Mallat (2007) the TOE conceptual model was originally used within Information Technology research studies as it has provided a valuable analytical basis and reliability although detailed factors within the main context may be different. The conceptual model was used by many researchers for innovation adoption. Examples are as follows: Zhu et al., (2006b) viewed the Technology Organisation and Environment framework as the significance backgrounds to understand the diffusion of business. Whereas Lee et al., (2009) projected a technological organisational and environmental conceptual model for the consideration of Radio-Frequency Identification (RFID) adoption in manufacturing organisation that wishes to improve their process efficiency. On the other hand Lin (2007), used a TOE theoretical prototype to evaluate aspects that influenced the adoption of green practices by SMMEs service organisation.

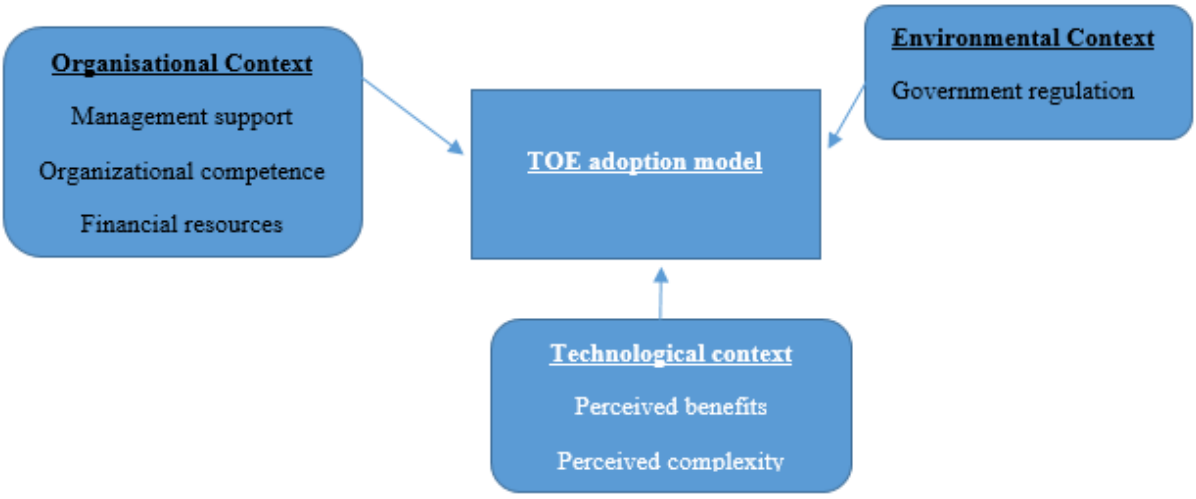


Figure 2-3: TOE model developed by Tornatzky and Fleisher (1990)

2.7 Chapter Summary

Security culture background and issues surrounding its existence together with the security explanation of the concepts from multiple researchers were discussed. The technological models and their summaries were explained with the sole purpose of formulating the research framework in the subsequent chapter. The next chapter provided details surrounding the research approach, method, data validation, etc. and how the research data was collected and analysed of which are the building blocks of the research programme.

CHAPTER THREE

3 RESEARCH METHODOLOGY

3.1 Introduction

The contents in this chapter outlines the research methodology and measures used to address the research study objectives and questions in detail. Subsections of this chapter includes the research strategy, research design, population, sampling procedures, data collection, study limitation sampling technique, data validity and reliability, questionnaire development, data analysis and ethical matters associated with this research project. Furthermore, it deliberates on the process used to analyse data validity and reliability as well as testing of the hypothesis based on adoption of ICT security culture in SMMEs in the Gauteng province in South Africa. Multiple regression analysis was used to assess the association amongst ICT safekeeping culture variables and the intention to adoption ICT security culture variable.

3.2 Research Strategy

According to Yin (1994), the most significant method for distinguishing amongst multiple research strategies is to recognize the research questions asked. As shown in table 3-1, there are five main research strategies to utilise during the collection and analysis of empirical evidence, namely experiment, survey, archival analysis, history and case study.

According to Yin (1994), individual strategies have their advantages and disadvantages depending on several circumstances. Firstly, the kind of study questions, secondly is the researcher's independence on authentic behavioural measures and the last one being the focus on contemporary versus historical phenomena. The key note is that the boundaries between the methods are not always strident and clear, and they frequently overlap each other as shown in Table 3-1.

Table 3-1: Relevant situation for different research strategies. Sources Yin, 1994, P.6

Strategy	**Form of Research Question**	**Requires control over behavioural events**	**Focus on contemporary event**
Experiment	How, Why	Yes	Yes
Survey	Who, What, Where, How many, How much	No	Yes
Archival Analysis	Who, What, Where, How many, How much	No	Yes / No
History	How, Why	No	No
Case Study	How, Why	No	Yes

The research strategy relies on features of the itemized research question/s. The major goals of this research study is to (1) determine how the adoption of ICT security culture can be supported in SMMEs to minimize human errors, (2) determine what has been done to minimize security breaches through human errors in Information Technology, (3) decide what are the determinants that influences the adoption of ICT security culture in SMMEs, and (4) how to measure the effectiveness of using this framework for adopting ICT security culture in SMMEs? The study questions of the current research are in the shape of *what and how,* consequently, the most suitable research strategy is to do a survey. In this research study, the quantitative survey process was used as strategy mechanism.

3.3 Research Design

According to Nachmias and Nachmias (2004), research design is a plan that allows the researcher to propose solutions to problems and direct him on the numerous phases of the research accordingly. Schindler and Cooper (2011) summarizes the importance of research design as an action- and time-based plan that is always linked to the research questions. The descriptive research design was used to study a population of interests by choosing samples and analyse the existence of occurrences at any given time (Orodho, 2008). A descriptive research design was used in this research study, whereby the participants feedback and opinions where collected, accumulated and deliberated or analysed in order to understand the types of participants within the research area. The usage of the chosen design was justified for the research study as it considered the present perspectives or viewpoints and existing connections, and furthermore the scrutiny of the variables included in the research. The focal benefit and purpose of utilizing descriptive research design was to transform information and data into a statistical format.

The structured questionnaire was used for data collection to ensure that the formality of response is adhered to. The questionnaire was designed to determine the participant's insight into the adoption of ICT security culture in the SMMEs in the Gauteng province in South Africa. Regression analysis was utilized to establish association amongst variables of this research. Research information was assessed by means of the Statistical Software Package for Social Sciences (SPSS) version 25.

The beta value (β) was used as a measurement of how strong the individual independent variable influences the dependent variable, it was also used in previous research like (Jafari et al., 2010). The individual regression coefficient represents an approximation of the change in

dependent variable, this will be established when all other independent variables are seized constant.

3.4 Data Collection

For data collections, online Survey Monkey and hard copy distributions were utilised for the respondents to provide feedback. Firstly, the online survey was utilised as a vehicle to collect data from the SMMEs employees based in the Gauteng province in South Africa through the questionnaire instrument. The reason online survey was recommended was because it is easy to reach more participants within a short space of time and it enables participants to respond to the questions at their convenience using a variety of devices that can connect to the internet. The second method was distributing hardcopies around the SMMEs within ease of reach. Although this process is expensive with regard to time and resources, it is worthwhile as not all employees who uses e-mail can access the specific online survey link. The data collection method used in this research study was also used in the previous study by Al-Alawi and Al-Ali (2015)

3.5 Piloting

To be certain that the research instruments utilized in data collection were structurally comprehensive, included the relevant questions and would gather effective contents, the researcher in this study submitted pilot questionnaires to the professionals in this field of study, for assessment. The rationale was to assess if the questionnaire were structurally sound. The researcher piloted the questionnaire to a sizeable group of 15 participants whose data was not included within the final research information. The outcome of the pilot process assisted the researcher to rectify items of the questionnaire that were ambiguous towards the participants.

3.6 Population and Sampling Design

3.6.1 Population

A population defines the samples of participants in the area of research through which data was collected from and eventually produced findings so that the researcher may generalize the entire population Zikmund (2003). According to Kothari (2004) a population is viewed as the total number of items (respondents) from which information or data was desired. In this research, the population comprises of SMME employees who are based in the Gauteng province in South Africa.

3.6.2 Sampling Design

3.6.2.1 Sampling frame

According to Dillman et al., (2008), a sampling frame symbolizes the community of interest that can be identified, accessed and evaluated throughout the research study. The researcher can select a controllable sample of the targeted community of interest from a sample frame. As it is practically impossible for the researcher to reach the entire community of interest in any type of research study, a researcher has to depend upon a sampling frame to characterize all of the individuals of the community of interest. The sampling frame can embody every one of the communities of interest or part thereof. In this research study, the population comprised of SMMEs in the Gauteng province in South Africa who registered with the department of Department of Trade and Industries (DTI). The conditions used for the selection of the sample organisations was as follows: the service organisation must have used or currently use ICT solution in all or part of their business, and their characteristics for being SMMEs must fall within the SMMEs as characterised by the South African government. According to Lucey (2002) research sampling is the procedure of examining a representative set of objects or people

out of the entire population to realize or understand some attribute of the same group or population.

3.6.3 Sampling Technique

Sampling techniques are means that are utilized to choose a sample from the population of interest by minimizing it to a controllable and representative size. According to Dillman et al., (2008) sampling techniques are applied when interpretations are made pertaining the population of interest. Two sampling technique namely: probability and non-probability are mainly used within the research area. The probability sampling is the technique whereby every sample within the targeted audiences has a chance greater than zero of being chosen to represent the whole population accurately. Whereas a non-probability sampling technique is grounded on the basis that samples are selected based on the subjectivity judgement of the researcher, rather than random selection. According to Kanupriya (2018), when each component in the population have the same probability of selection it is referred as 'equally probability of selection' (EPS) design. In this study, both probability and non-probability sampling technique were utilised. Within the probability sample, the simple random sampling was utilised because each member has an opportunity of being selected and represent the community of interest and from the non-probability sample the purposive subsection was used. The reason being, the researcher chose a sample on the account of their knowledge of the community of interest and the study itself. The participants were chosen on the account of study purposes.

3.6.4 Sample Size

According to Kothari (2004), the number of people who were chosen from the population of interest constitute a sample size. In this study, a total number of 665 responses were received of which 18 were non-usable or incomplete and subsequent to that, 647 responses were used

for data analysis. A sample size of 647 individuals from different SMMEs in the Gauteng province was used. Though it does not represent all the SMMEs in the area, the number of respondents was enough to get a sense of the population of interest's views points. The sample size of 647 participants made it manageable because of time and resources constraints and it also provided critical analysis of the contents under study.

3.7 Developing the Questionnaire

A questionnaire is a procedure for getting data from the participants by utilizing a sequence of questions pertaining to the specific subject matter. According to Birks and Malhotra (2000) a questionnaire should have three specific objectives, namely: (1) decoding the desired data into questionnaire, (2) maximizing inspiration of the participants near partaking in the programme, and (3) lessening reply faults which occurs based on manipulating, miss-recorded or miss-analysed responses. Within this research, the structured questionnaire was utilised to ensure that there is no ambiguity in response. According to Birks and Malhotra (2000), to design the questionnaire properly, the researcher should take question wording into consideration which might have a direct impact on the response from the participants if they are difficult to understand. It is imperative to use simple language that would not surpass knowledgeable capacity of targeted audiences.

The constructed questionnaire intended to capture the respondent's opinion pertaining ICT security culture and other determinants that might impact decision making to adopt ICT security culture in SMMEs. The research questionnaire comprised of 28 items that were used to measure variables. As discussed previously the Technological, Organisational and Environmental conceptual model encompasses three constructs, namely: Technological construct; Organizational construct and Environmental construct. The TOE construct comprises of the following variables within the Technological construct: perceived benefits

with 4 items, and perceived complexity also with 4 items. Within the Environmental construct the variables are government regulations with 5 items whereas the Organisational construct comprises of management support with 4 items, financial resources also with 4 items and organisational competence using 3 items. The perceived intention to adopt the ICT security culture was measured by 4 items. The significant of the questionnaire was to measure the research framework construct's effect towards the adoption of the innovation and determine whether each variable have a positive or negative impact on the dependant variable (adoption of ICT security culture). Questionnaires and items were adapted from the previously published research papers to align with the current research paper.

To quantity participants views, five-point Likert scale was employed that comprises of the following options: (1) signifying "**Strongly disagree**"; (2) signifying "**Disagree**"; (3) signifying "**Neither agree or disagree**"; (4) signifying "**Agree**" and (5) signifying "**Strongly agree**".

The questionnaire consisted of two parts: Within **Section A: Demographic information,** the participants were asked about their demographic setup to ascertain the type of respondents that participated, as this will assist in improving future research study in similar setup. The demographic data was not used to determine factors to adopt but to provide information about the type of respondents who participated. While in **Section B: Technology Adoption associated questionnaires**, the portion was considered as the main question groups where multiple factors which were based on the proposed conceptual model were put into test and hypothesis were developed to determine the relationship towards the adoption of the proposed innovation. Table 3-2 below shows where the questionnaires were adapted from the previous research papers.

Table 3-2 : Sources of statements used to measure each construct

Construct	Item Codes	Statement / Items	Revised from
Demographics Information		Education Level, Age, Experience, Position Held	Al-Alawi and Al-Ali (2015)
Management Support	MS1	Management encourages employees to be ICT security champions.	(Roberts and Premkumar, 1999, Pai et al., 2014)
	MS2	Management will make resources available for the adoption of the ICT security culture	
	MS3	Adoption of innovation activities is widely communicated and understood throughout the organization	
	MS4	Management demonstrate strong commitment to promote information security culture.	
Government Regulations	GR1	We believe that there are effective ways to adopt ICT security culture	kanaan-Jebna et al., (2016); Zhu et al., (2006a)
	GR2	We believe that the SMMEs environment (business culture) is conducive enough to adopt ICT security culture	
	GR3	We believe that government policies or regulations (Laws) will effective minimize human error through adoption of ICT security culture	

Construct	Item Codes	Statement / Items	Revised from
	GR4	We believe that government will demonstrate strong commitment to promote ICT security culture	
	GR5	Proper handling of economic, political instability and human rights issues will allow the adoption of ICT security culture	
Organizational Competence	OC1	We have a good understanding of ICT environment where we are doing business	Lertwongsatien and Ravichandran (2005);Molla and Licker (2005)
	OC2	Our organization have a good understanding of product / services classes within our business environment.	
	OC3	Our organization have competent resources to assist towards the adoption of ICT security culture.	
Perceived Complexity	PC1	The adoption of the ICT security culture will not inconvenience the way we are doing business.	Davis (1986);Chau and Tam (1997)
	PC2	Learning to adapt the adoption of ICT security culture will be easy.	

Construct	Item Codes	Statement / Items	Revised from
	PC3	It is easy for our SMMEs employees to become skilful in using the innovation.	
	PC4	Interacting or Adoption of ICTs security culture will be flexible.	
Perceived Benefits	PB1	Adoption of ICT security culture will improve service productivity.	Davis et al., (1989)
	PB2	Human errors will be minimized after the adoption of the ICT security culture.	
	PB3	It will be easier for me to become skilful in adjusting to the adoption of the ICT security culture	
	PB4	Unnecessary down time of systems will be minimized.	
Financial Resources	FR1	The service organization has not difficulties in finding all the necessary resources. (i.e. initial investments, time) to adopt innovation	Boonsiritomachai (2014); Ellinger et al., (2011)
	FR2	The service organisation will maximize profit through the adoption of ICT security culture	
	FR3	The adoption of ICT security culture will signify an investment with valuable returns.	

Construct	Item Codes	Statement / Items	Revised from
	FR4	The cost logistics to support the adoption of the ICT security culture will be high. (i.e. Cost to train employees)	
Intention to Adopt	ITA1	Intent to use measures in the future	Gavgani et al., (2016)
	ITA2	Plan to use measures as soon as possible	
	ITA3	Intent to use measures as soon as possible	
	ITA4	Plan to use measures in the future	

3.7.1 Variables and Functional Definition

Table 3-3 below illustrates the clarification of research construct and their functional definition. It highlights the extent to which users views the construct having impact on the adoption of the technological development of which in this current study is ICT security culture.

Table 3-3: Study construct and functional definition

Construct	Functional definition
Management Support	The level on which personnel trust that management support will improve the adoption of ICT security culture in SMMEs.
Government Regulations	The extent to which users believe that government regulations will enhance the adoption of the ICT security culture in SMMEs.

Construct	Functional definition
Intention to Adopt ICT security culture	The degree to which users aim to partake in the adoption of the ICT security culture in SMMEs.
Financial Resources	The scope to which personnel trust that the organizational financial resources will enhance the acceptance of ICT security culture.
Perceived Benefits	The scope on which personnel trust that perceived benefits will improve the adoption of ICT security culture in SMMEs.
Perceived Complexity	The scope on which personnel trust that perceived complexity will improve the acceptance of ICT security culture in SMMEs.
Organizational Competence	The degree on which personnel trust that organisational competence will improve the adoption of ICT security culture in SMMEs.

3.8 Proposed Research Model

As discussed in literature reviews, the IT adoption literature associated with SMMEs has recognized and exposed the effect of a widespread range of construct linking to adoption of multiple innovation. Within the similar custom, also as an endeavour to achieve the study determination, it is thus significant to find determinants that were viewed within this research

to be substantial to the adoption of ICT security culture in SMMEs in the Gauteng province in South Africa.

The research framework used within this study was derived and adopted from the Technological Organisational and Environment framework (TOE) as projected by Tornatzky and Fleischer (1990) (See figure 3-1 below). The below model was widely used by researchers for the adoption of ICT innovation hence it has been adopted in this study to determine the factors that have a significant effect on the adoption of the ICT security culture in SMMEs in the Gauteng province in South Africa.

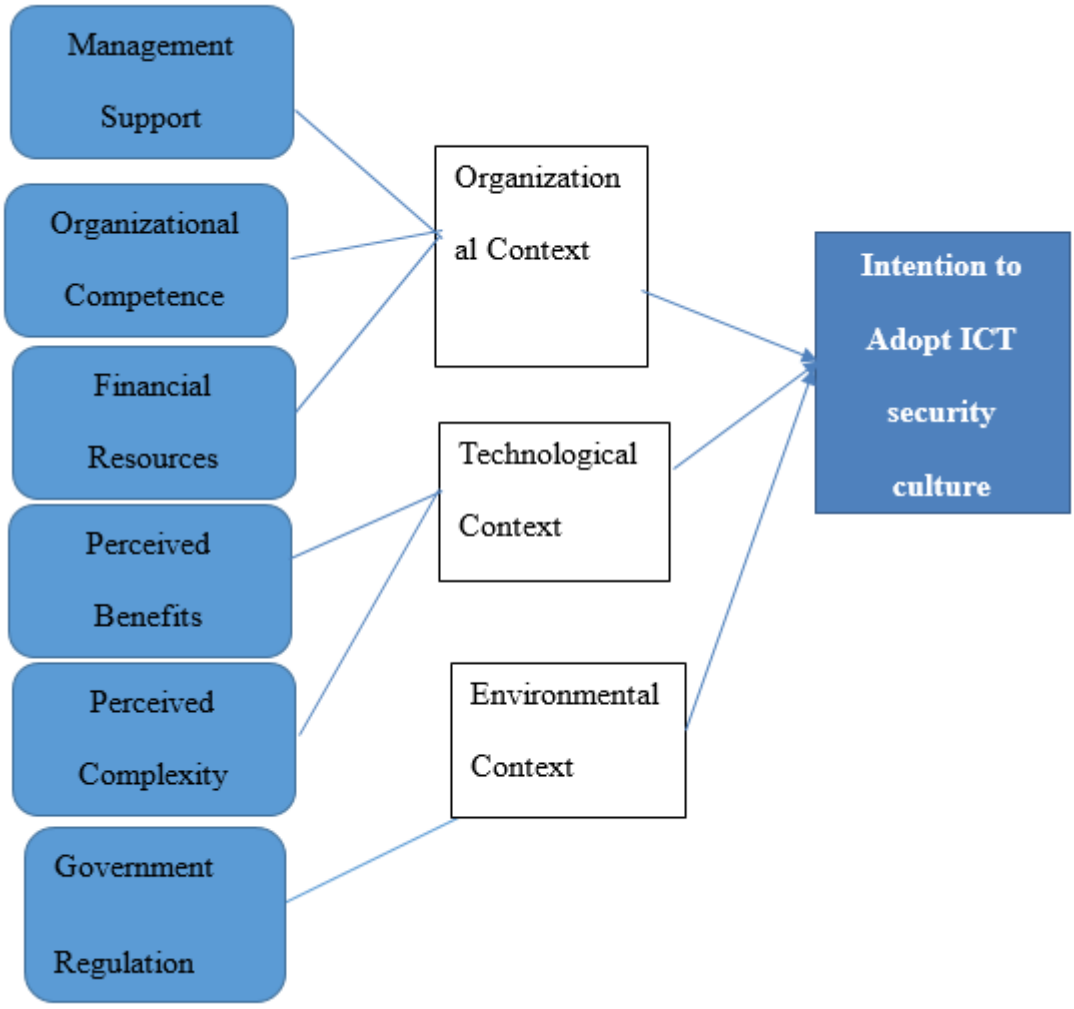


Figure 3-1: Proposed research modelTornatzky and Fleisher (1990)

3.9 Ethical Consideration

The concept of ethical consideration is related to moral standards that should be reflected by the researcher in all of the research phases. Within this research study ethical considerations has been a top priority to adhere to.

All participants in this research were conscious that they do so on voluntary basis. With regards to confidentiality, all correspondences were treated with high confidentiality to guarantee the cooperation of the respondents. To adhere to individual's privacy and anonymity, all the files containing personal identifiable information were password protected. To make sure that all participants understand the objectives and aims of the research study the consent letters were distributed to them in an effort for them to comprehend the outcomes of the research study.

3.10 Data Processing and Analysis Techniques

The captured data was transferred to SPSS version 25 for analysis. To ensure that there was an internal consistency for the concepts of the research, a reliability test was carried out using Cronbach's alphas and composite reliability (CR). A validity test was carried out to assess if the study instrument (survey) definitely measures what it was intended to measure using the following instruments: Kaizer-Meyer-Olkin (KMO), Bartlett's test of sphericity and the Principal Component Analysis (PCA) using the Varimax rotation. And finally, to analyse the hypotheses of the research study the regression analysis technique was conducted, and factor analyses was used to analyse the dataset for the scale construction and operational. Subsequent to that, percentages of the demographic information results, (Section A of the questionnaire) using figures were presented as well as the frequencies and percentages of ICT security culture associated questions results (Section B questionnaire) utilising the tables.

To confirm the technology adoption (ICT security culture) associated questionnaire (Section B questionnaire) consistency, the Cronbach's Alpha and Composite Reliability were analysed, as

discussed before, to confirm that the variables are really measuring the same thing. According to Harfoushi et al., (2016), reliability is based on meticulousness; it is mainly utilised in verifying the uniformity as well as the steadiness of the questionnaire. According to Thope et al., (1991), assessment of reliability should fall under the following questions:

- Will the measurement produce identical results on a different occasion?
- Will comparable reflection be reached by other viewers?
- Is there any visibility on how logic was viewed from row data?

To confirm the steadiness of construct, the Cronbach's results should be above 0.7 to ensure that they are acceptable, any value below that figure is regarded as poor. Reliability of the questionnaires were based on the intention to adopt the ICT security culture in SMMEs. Table 3-4 below highlights the reliability levels.

Table 3-4: Reliability Levels

Reliability	**Ranges**
Poor or unreliable	$\alpha < 0.7$
Acceptable or reliable	$\alpha = 0.7$ and $\alpha < 0.8$
Good or very reliable	$\alpha = 0.8$ and $\alpha < 0.9$
Excellent or strongly reliable	$\alpha = 0.9$ and $\alpha \leq 0.10$

Factor analysis was used within the convergent and discriminant validity to determine if the scales are measuring the construct appropriately. The Principal Components Analysis (PCA) which is a data reduction technique that minimizes a larger set of measures to a smaller and more manageable set was utilized to confirm convergent and discriminant validity. According to Manaf et al., (2013), PCA manages the whole data to be analysed without excluding the fundamental class baseline and looks into the directions that have the widest variations. Shlens

(2014) concur that PCA is a typical instrument used in recent data scrutiny, in varied areas from neuroscience to computer photographs based on its simplistic, non-parametric technique for removing specific details from unclear information sets. Based on the previous statement PCA provided a blueprint on how to minimize a complex data set to minimal dimensions to uncover the concealed and basic structures that periodically motivate it. According to Wang (2014), the PCA is a prejudice transformational process that diagnose an estimate of the covariance matrix of the data. The PCA equation or formula is depicted below in equation 3-1:

Equation 3-1: PCA Formula

$$\bar{y} = \frac{1}{n}\sum_{i=1}^{n} xi$$

The sampling adequacy was conducted utilizing the Kaizer-Meyer-Olkin (KMO). The KMO measures how suited are data sets to factor analysis. According to Abdullah et al., (2016), for the sampling adequacy to be adequate or acceptable its value should be more than 0.5; should the KMO number be below 0.5 the process would be undesirable and factor analysis would not be undertaken. The formula or equation to measure the KMO test is depicted below in equation 3-2 as:

Equation 3-2: KMO Formula

$$KMO_j = \frac{\sum_{i \neq j} r^2{}_{ij}}{\sum_{i \neq j} r^2{}_{ij} + \sum_{i \neq j} u}$$

To assess how the experiential correlation matrix, $R = (ri_j)(p \times p)$ deviate from the identity matrix, the Bartlett's test of sphericity was used. To measure the inclusive relationship amongst the independent and dependent variable we computed the factors of the correlation matrix |R|. UnderH0, |R|=1: if the test results show $|R| \approx 0$, then the variables are highly correlated.

Bartlett's Test of Sphericity highlights to what degree we derivate from the reference situation of |R|=1. The following formula in equation 3-3 was used:

Equation 3-3: Bartlett's Test of Sphericity Equation

$$x^2 = -\left(n - 1 - \frac{2p+5}{6}\right) \times 1n|R|$$

To measure the strength of the relationship between two constructs (see figure 3-2 below), Person's correlation coefficient (r) was conducted. Person correlation coefficient is a procedure for determining the association between two quantitative and continuous variables, it does not try to ascertain if there any dependent and independent variables Thatte and Gogtay (2017). The below formula or equation 3-4 was utilised to analyse the Pearson correlation coefficient:

Equation 3-4: Equation to calculate the Pearson correlation coefficient

$$r = \frac{n\left(\sum xy\right) - \left(\sum x\right)\left(\sum y\right)}{\sqrt{\left[n\sum x^2 - \left(\sum x\right)^2\right]\left[n\sum y^2 - \left(\sum y\right)^2\right]}}$$

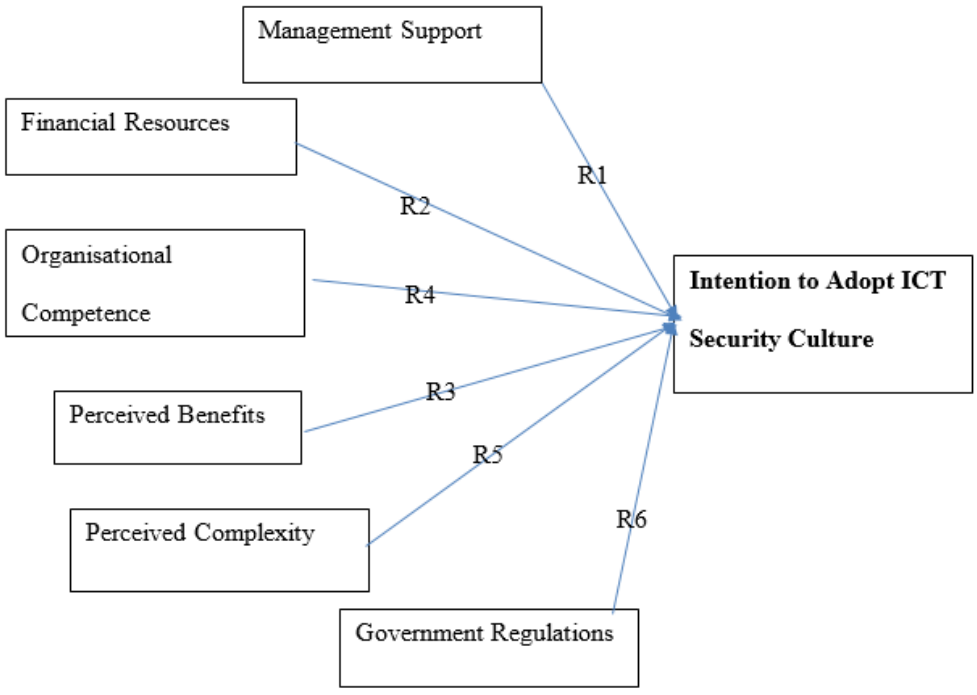


Figure 3-2: Relationship between the independent and dependent variables

After studying the literature reviews, hypothesis development was proposed based on the proposed theoretical framework to measure the association amongst constructs and the adoption of ICT security culture in SMMEs. To ensure that the hypotheses within the research study were measured, the multiple linear regression was conducted. According to Sacla and Angelache (2016a) multiple linear regression is viewed as multiple independent variables utilised to predict the value of a dependent variable, which in this research study is adoption of ICT security culture. In most cases, multiple linear regressions are utilised for demonstrating the association between two or more elucidative constructs by identifying a linear formula or equation between the experimental data.

Regression analysis is an influential statistical method that observe the association amongst multiple variables of interests. According to Kothari (2004) the coefficient of correlation is used to scale the degree of association amongst variables. In this study, multiple regression coefficient of correlation analysis was utilised to analyse the relationship amongst the ICT security culture factors (independent variables) and the intention to adopt ICT security culture (dependent variable). The regression and correlation analyses of the model displays the understanding and confirmation of the suggested relationship between the ICT security culture variables presented and the intention to adopt ICT security culture.

In this research study the independent variables (management support, government regulation, perceived complexity, perceived benefits, organisational competence and financial support) were also used to predict the value of the adoption of the ICT security culture. As the proposed conceptual model had influences towards the adoption of innovation in the previous literature, even in this study it was tested to determine if they have any significant relationship with the adoption of the ICT security culture. Within the research environment, multiple linear regression was utilised for demonstrating the association amongst multiple explanatory

variables and the response variable by recognizing a linear equation between the investigational data. For individual value of the independent construct x it is related to the value of the dependent variable y . According to Sacla and Angelache (2016b) each values of the itemized explanatory construct within the linear regression x_1, $x_2 \ldots x_p$ should be defined based on the equation 3-5 below:

Equation 3-5 Linear Equation $$y = bx + a$$

Subsequent to assessing both the theory reviews and earlier studies, the following hypotheses were consequential (details were represented in figure 3.3 below):

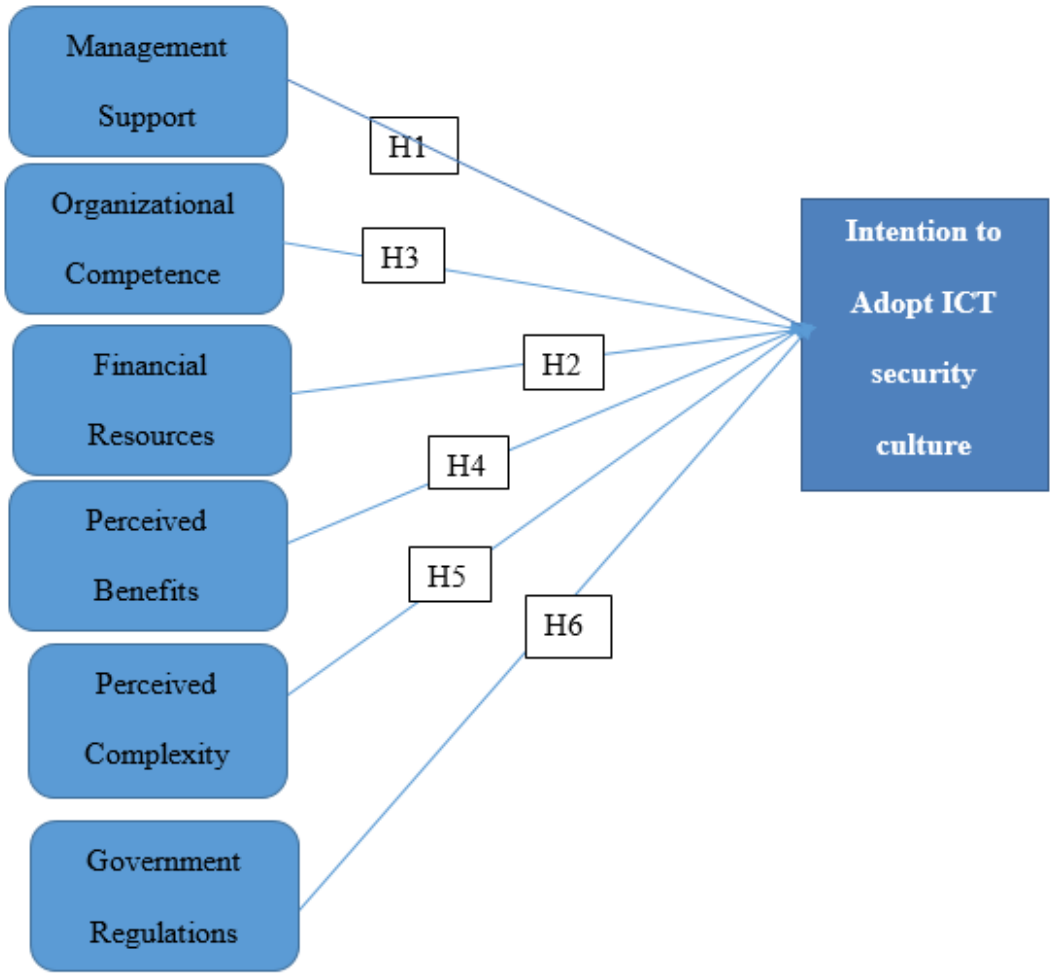


Figure 3-3: Hypotheses Study

i. Management Support

The theory reviews of this study indicated evidence of and substantiate the relevance and the strong positive effect of management support on the intention to adoption ICT security culture in SMMEs. Management support is viewed as the extent to which management support any adoption of internal innovation or processes. According to Walker et al., (2008), management support eagerness to accept technological innovation is one of the main determinants adding more weight to the influence of adopting the e-commerce or any innovation. Motwani and Mirchandani (2001) maintains that the backing from management is critical and undoubtedly distinguish between the adopters and non-adopters in e-commerce adoption process. Hence, this study hypothesises that:

H1: There is strong relationship between management support and the adoption of ICT security culture.

ii. Financial Resources

According to Bagale (2014), financial resources was viewed as one of the substantial aspects influencing the operations of businesses based on the high investment requirements for hardware, software as well as employee training. According to Zhu et al., (2003), financial resource was viewed as the extent to which the resources of the organisation will be used for the innovation adoption. Hence, this study hypothesises that:

H2: There is significant relationship between financial resources and the adoption of ICT security culture.

iii. Organisational competence

Organisational competence is viewed as the extent to which the competency of the organisation is geared towards the adoption or implementation of any technological innovation. The

majority of research studies are in agreement that there is a significant relationship between organisational competence and adoption of innovations (Edgar and Lockwood, 2001; Jabbouri and Zahari, 2014; Clarke, 2001). Hence, this study hypothesises that:

H3: There is strong relationship between organisational competence and the adoption of ICT security culture.

iv. Perceived Benefits

Perceived benefits are viewed as the extent to which the personnel trust that utilizing a specific technology will improve their job accomplishment LIN and CHIN (2016). According to Gerrard and Cunningham (2003) perceived benefits or advantages was recognised as an significant feature impacting the acceptance of internet banking. According to Rogers (1983), perceived benefits is measured in terms of an innovation's commercial viability, time serving, as well as the minimization of discomfort and efforts that will lead to the acceptance of innovation. Hence, this study hypothesises that:

H4: There is strong relationship between perceived benefits and the adoption of ICT security culture.

v. Perceived complexity

Mukhtar and Herzallah (2015), defines perceived complexity as the extent to which technological modernization can be problematic to comprehend and implement. Based on their assertions, intricacy of a structure or innovative technology minimizes the adoption rate. According to Rogers (1995), perceived complexity is viewed as a degree to which the consumers reflects the innovation to be difficult to use and also measured based on the innovation's level of complexity as experienced by potential adopters. So, this study hypothesis that:

H5: There is no significant relationship between perceived complexity and the adoption of ICT security culture.

vi. Government regulations

According to (Zhu et al., 2006a, Liu, 2008, Lin and Lin, 2008, Li, 2008) government regulations and support have a significant influence on innovation adoption. Government regulations is viewed as the extent to which government support innovation is adopted through the implementation and enforcement of laws and/or regulations Zhu et al., (2006a). Hence, this study hypothesises that:

H6: There is a strong relationship between government regulation and the adoption of ICT security culture.

vii. Intention to adopt ICT security culture

The behavioural intention to use signifies a person's eagerness to perform or not to perform an explicit future behaviour Alsamydai (2014). Siringoringo and Guritno (2013) stated that, behavioural intention to use or adopt a specific innovation is motivated by the attitude towards using it.

3.11 Data Validity and Reliability

According to Thornhill and Saunders (2003), to ensure that you reduce the probability of getting incorrect answers, a special consideration need to be given to both data validity and reliability. To determine the usefulness and quality of collected data of the current research study, reliability and validity measures were employed.

3.11.1 Validity

Validity is the instrument that measure the accuracy of what is intended to be measured. The significance of data validation is to ensure that the survey questionnaire is completed, and consistency is maintained towards the key construct of the proposed model.

According to Creswell (2008), the perfect state of a research study occurs if scores are both consistent and valid. Creswell maintains that scores must be both constant and steady (reliable) prior to being expressive (valid). Again, according to Creswell (2008), a research is viewed as effective if scores are eloquent and logical. Creswell maintains that scores will only be valid if the researcher is capable of drawing conclusions from the study samples. The validation technique to be used is construct validity. Construct validity was chosen because it assesses validation using statistical methods or procedures. Construct validity was utilised to ascertain if the scores from the research instrument are significant and also if they can be utilized to make sense of a sample from the community of interest. For the construct validity to meets its objective it had to adhere to the conditions of convergent and discriminant validity. Two subsets of the construct validity (convergent validity and discriminant validity) were employed to measure if the model concept that should be associated are in fact associated and to measure if concepts that are not supposed to be related are indeed unrelated. According to previous research papers the construct validity was used to test or experiment if the instrument does indeed measures what it is supposed to.

According to Babin et al., (2006) convergent validity linked to the process whereby the measured variables within an explicit concept share a major percentage of modification that are in common. According to Larcker and Fornell (1981) convergent validity is acceptable if it meets the following criteria:

- All indicators loading ought to be significant with levels above 0.5.

- Construct composite reliability should be above 0.6.
- Lastly, the average variance extracted based on individual concepts must be above the variance due to the error measurement for the construct. Example is that, Average Variance Extracted (AVE) should be higher than 0.5

According to Teddlie and Tashakkori (1998), the discriminant validity measurement could be tested utilizing Larcker and Fornell (1981) criteria, in which the square root of AVE for the individual concept is thought to be above the square association amongst any concepts within the aspect association matrix. Within this research study, the design of the questionnaire was revised from the questionnaires used by other researchers, as found in the literature review. Thus, the validity of the questionnaire had already established.

3.11.2 Reliability

Reliability pertaining the questionnaire is based on the user's viewpoint to adopt ICT security culture and was conducted using the Cronbach's α as proposed by Cronbach in 1951. Within social science studies, the Cronbach's α efficient is frequently utilised to measure the reliability of questionnaires. According to Harfoushi et al., (2016), reliability is based on meticulousness and is mainly utilised in verifying the uniformity as well as the steadiness of the questionnaire.

3.12 Chapter Summary

Within this chapter, the conceptual research model was adopted based on literature regarding the technological adoption models. All the constructs or variables used were adopted from the related technological adoption frameworks. Subsequent to that, different hypotheses where developed based on the proposed model that was assessed in the subsequent section. Chapter 3 outlined the study approach and explained the method to realize the study purposes. The process of study approach is significant as it assists the researcher to categorize the appropriate methods to apply his/her research based on study design, sample population, questionnaire

design and other associated analysis required. The following chapter dwells more on data analysis and results.

CHAPTER FOUR

4 DATA RESULTS ANALYSIS AND FINDINGS

4.1 Introduction

Chapter four highlighted results analysis and findings consolidated based on the survey questionnaire in relation to the research questions that were presented in chapter one. Survey questionnaires were used for data collection, subsequent to that Statistical Package for the Social Science (SPSS) version 25 was utilised for quantitative breakdown. The survey structure was in two sections. Firstly, the initial portion, Section A, included the demographic information that entails respondents ages, positions, qualification and experience status. The participant's demographic information was not utilised towards the research questions but to highlight the response rate of the participants and their inclusivity in their area of profession.

Section B was used for research purposes and to ensure that the research question was answered, and the objectives met. The research question was based on determining factors affecting the adoption of ICT security culture in SMMEs in the Gauteng province in South Africa. The 5-point Likert scale was used for the participants to choose the correct statement ranging from 1 (strongly disagree) to 5 (strongly agree) in relation to the problems highlighted in the first chapter of this study. Two objectives were used to ensure that the collection of data is aligned and the data analysis is discussed in the next subsections of this document. The key objectives of the research study were to determine the factors or determinants that influence the adoption of ICT security culture in SMMEs and to propose a theoretical model for the adoption of an ICT security culture that will assist in minimizing the human error in SMMEs.

Section 4.2 defines the background information that highlights the rate of responses coupled with the demographical data pertaining to the participants.

4.2 Response Rate

A total number of 665 responses were received of which 18 were non-usable or incomplete and subsequent to that, 647 feedbacks was used for data analysis. The response rate of the research was 83%. The responses were as a result of the estimated 800 feedbacks from participants. A sample size of 647 individuals from different SMMEs in the Gauteng province was used to assess the factors that have constructively impacted on the adoption of ICT security culture. Though the sample does not represent all the SMMEs in the area the size was enough to get a sense of what the population of interest's views were. According to Tsuya et al., (2015), the response rates are significant if the determination of the study is to make generalizations about the lager population of interest. Manfreda et al., (2016) asserts that, if the response rate is below 30 percent of the expected response then the validity, methods used and results will be questionable. In this research study, the percentage of 83% was above the proposed threshold. The sample size of 647 participants made it manageable with regards to time and resource constraints and it also provided critical analysis of the contents under study.

4.3 Reliability Test Results

To determine the internal consistency of multiple variables, the Cronbach's Alpha was utilized to assess construct reliabilities. Cronbach's alpha is frequently utilized by researchers to assess the internal consistency or reliability of a survey when it consists of multiple Likert-type questions. Reliability tests ranges in value from 0 to 1; the closer the value towards 1.0 better the results. Any values that is below baseline of 0.7 towards 0 are regarded as poor (Bougie, 2016). Any numbers above 0.7 means the results are acceptable, and numbers close to 0.8 are good while any number above 0.9 results are excellent and shows a high level of internal reliability. As shown in table 4-1 below all study constructs are above the acceptable reliability levels.

Table 4-1: Reliability levels for research constructs

Construct	No. of items	Cronbach reliability level
Management support	4	0.757
Perceived Benefits	4	0.772
Intention to adopt ICT security culture	4	0.898
Perceived Complexity	4	0.887
Organisational Competency	3	0.757
Financial Resources	4	0.729
Government Regulations	5	0.787

In addition to the outline reliability results in Table 4-1 above, Figure 4-1, 4-2, 4-3, 4-4, 4-5 and 4-6 below displays the outcomes of multiple internal uniformity tests of variables in scales, where the reliability analysis was found to be both acceptable and good as their Cronbach's alpha results were above 0.7.

4.3.1 Perceived Complexity Cronbach's Alpha Reliability Test

Reliability results pertaining perceived complexity show the value in the range of 0.8 (good), and can be seen in Figure 4-1 below. The results show the internal consistency of perceived complexity as reliable with a value of 0.887. Perceived complexity used 4 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1.

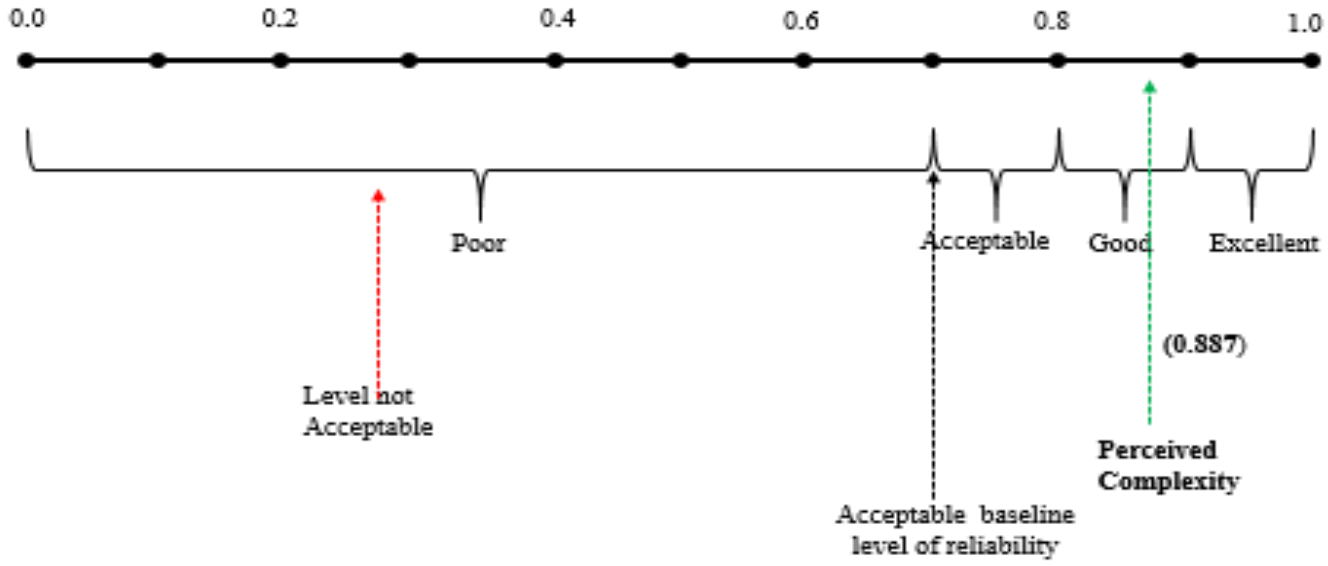


Figure 4-1 : Perceived Complexity Cronbach's Alpha Reliability Test

4.3.2 Perceived Benefits Cronbach's Alpha Reliability Test

Reliability results pertaining perceived benefits shows the value in the range of **0.7** which falls under the acceptable category as per Figure 4-2 below. The results show the internal consistency of perceived benefits as reliable with a value of 0.772. Perceived benefits used 4 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1.

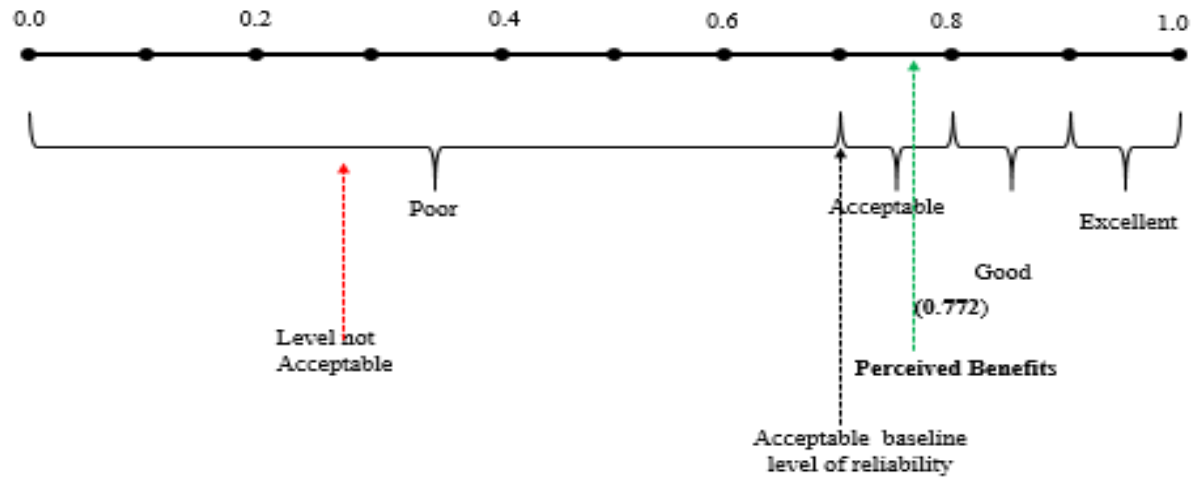


Figure 4-2 : Perceived Benefits Cronbach's Alpha Reliability Test

4.3.3 Management Support Cronbach's Alpha Reliability Test

Reliability results pertaining management support shows the value in the range of **0.7** which falls under the acceptable category as per Figure 4-3 below. The results show the internal consistency of management support as reliable with a value of 0.757. Management support used 4 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1.

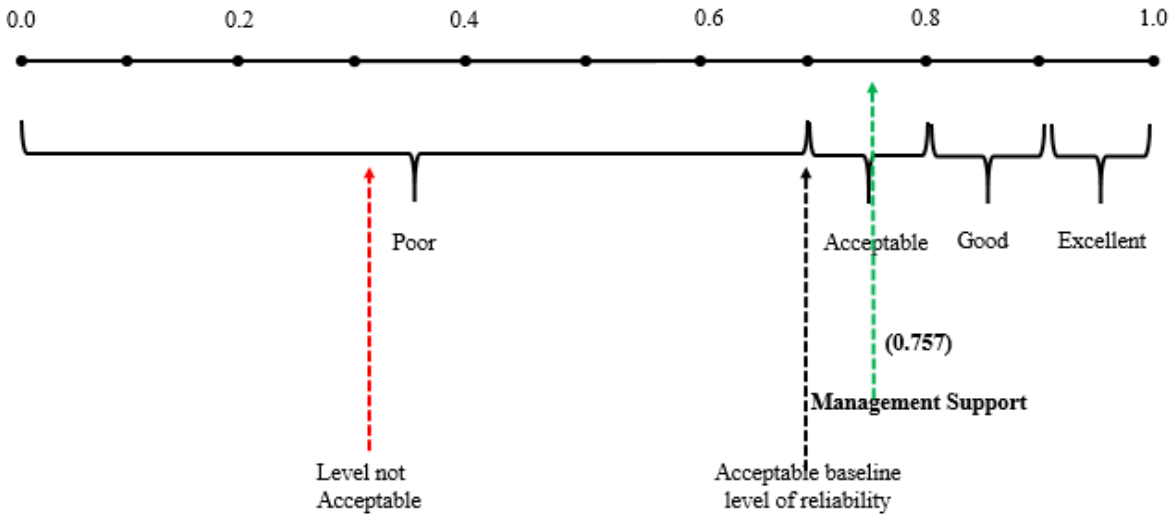


Figure 4-3 : Management Support Cronbach's Alpha Reliability Test

4.3.4 Government Regulations Cronbach's Alpha Reliability Test

Reliability test pertaining government regulations shows the value in the range of **0.7** which falls under the acceptable category as per Figure 4-4 below. The results show the internal consistency of government regulations as reliable with a value of 0.787. Government regulations used 5 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1.

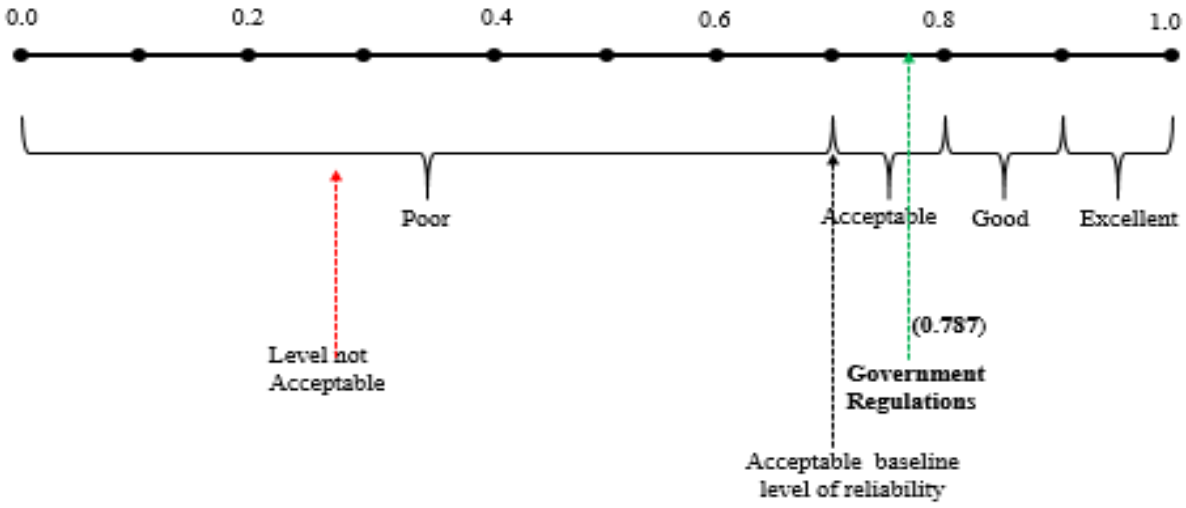


Figure 4-4 : Government Regulations Cronbach's Alpha Reliability Test

4.3.5 Financial Resources Cronbach's Alpha Reliability Test

Reliability results pertaining financial resources shows the value in the range of **0.7** which falls under the acceptable category as per Figure 4-5 below. The results show the internal consistency of financial resources as reliable with a value of 0.729. Financial resources used 4 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1.

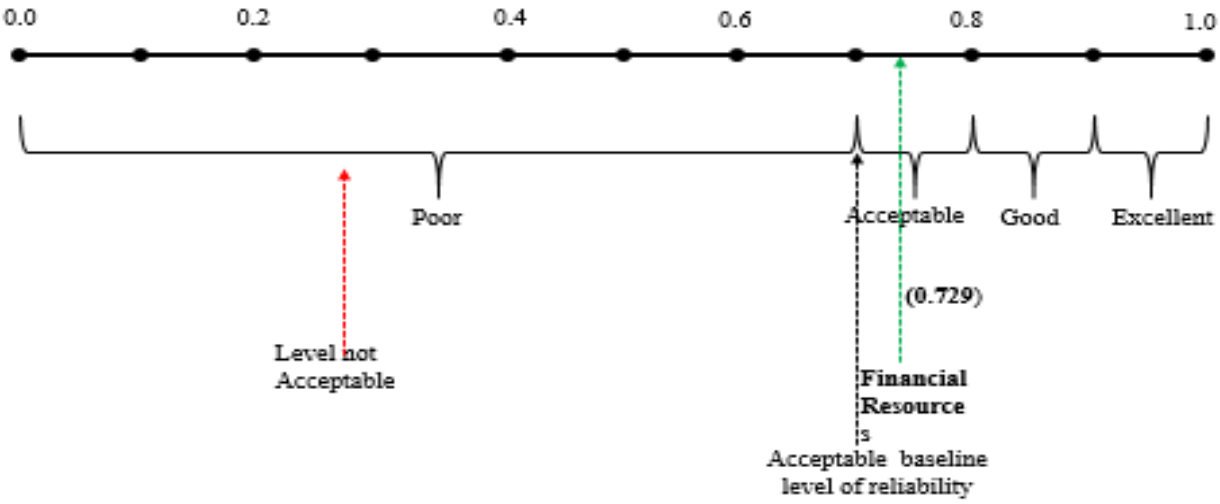


Figure 4-5 : Financial Resources Cronbach's Alpha Reliability Test

4.3.6 Organizational Competence Cronbach's Alpha Reliability Test

Reliability test results of organizational competence shows the value in the range of **0.7** which falls under the acceptable category as per Figure 4-6 below. The results show the internal consistency of organizational competence as reliable with a value of 0.757. Organizational competence used 3 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1.

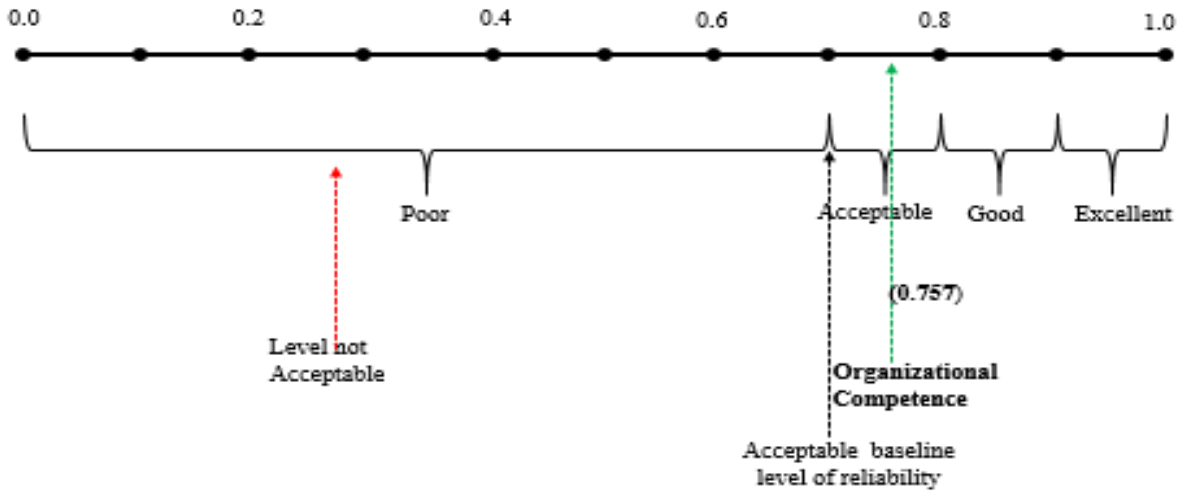


Figure 4-6 : Organizational Competence Cronbach's Alpha Reliability Test

4.3.7 Intention to Adopt

Intention to adopt ICT security culture used 4 items or construct to measure the Cronbach's Alpha reliability as shown in table 4-1. Reliability test results of intention to adopt ICT security culture shows the value in the range of **0.8** which falls under the good category as per Figure 4-7 below. The results show the internal consistency of intention to adopt ICT security culture as reliable with a value of 0.898.

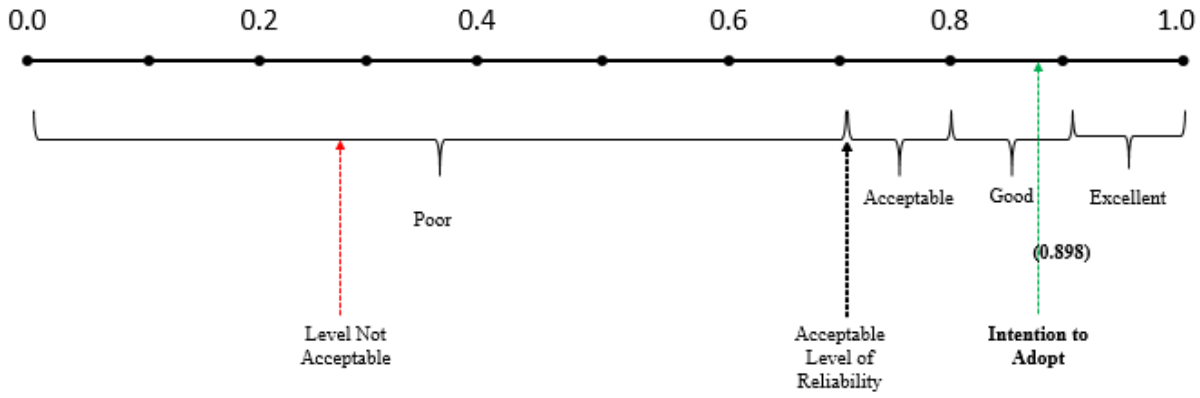


Figure 4-7 : Intention to adopt ICT Security Culture Cronbach's Reliability Test

Summary of Cronbach's reliability

All constructs in this research study are above the set threshold of Cronbach's reliability of 0.7 as asserted by Bougie (2016). Based on the assessment output the reliability of the constructs is acceptable.

4.4 Validity Test Results

To test the validity of each construct, factor analysis was utilised through the principal analysis (PCA) to determine the fundamental variable of the research study. PCA was chosen because it allows for an assessment to both the convergent and discriminant validity. Before conducting the factor analysis, a Kaiser-Meyer-Olkin test of sampling adequacy and a Bartlett test was assessed to make sure that the sample size is acceptable to support factor analysis as a result of the number of variables. As depicted in Table 4-2 below, the chi-square is at 15834.834 with 412 degrees of freedom that is significant at 0.000 level of significance coupled with a Kaiser-Meyer-Olkin of 0.769 that justifies the factor analysis in this research as it is above 0.50. Based on the above breakdown of KMO sampling adequacy and Bartlett's test, the factor analysis for adoption of the ICT security culture questionnaire is regarded as a suitable technique for further data analysis.

Table 4-2: Kaiser-Meyer-Olkin and Bartlett's test

Kaiser-Meyer-Olkin and Bartlett's test	**Results**
KMO measure of sampling adequacy	0.769
Bartlett's Test of sphericity: Approximately Chi-Square	15834.834
: Df	412
: Sig.	0.000

Table 4-3 below depict the factor loading of the principal components. In order to interpret the factor loading, the research followed the recommendation from Anderson et al., (2010). According to these recommendations, any items are viewed as practically significant if their load values are more than 0.5. Based on their recommendations, a cut-off value of less than 0.5 was consequently implemented in this research study. According to Palvia and Aladwani (2002) any value that did not load strongly (any factor less than 0.5) must be eliminated, therefore this principle was applied in this research paper. According to this research studies all factors loaded above the recommended threshold and are therefore all accepted.

Table 4-3: Principal Components Analysis (Factor loading)

Variables	**Questionnaire Construct**	**GR**	**MS**	**OC**	**PC**	**PB**	**FR**	**ITA**
Government Regulations								
GR1	Innovation adoption	0.832						
GR2	environment (business culture) is conducive	0.834						
GR3	policies or regulations (Laws)	0.782						
GR4	Strong commitment	0.697						
GR5	handling of state issues	0.509						
Management Support								

MS1	Management is supportive		0.889					
MS2	Resources availability		0.816					
MS3	Communication capability.		0.788					
MS4	Clear vision		0.587					
Organisational Competence								
OC1	ICT environment			0.941				
OC2	Understanding of business			0.932				
OC3	Competent resources			0.844				
Perceived Complexity								
PC1	Business inconvenience				0.879			
PC2	Learning to adapt				0.869			
PC3	Become skilful				0.814			
PC4	Flexibility of adoption				0.764			
Perceived benefits								
PB1	Improve service productivity.					0.889		
PB2	Minimized issues					0.815		
PB3	Become skilful					0.588		
PB4	Unnecessary down time					0.789		
Financial Resources								
FR1	Availability of resources						0.761	
FR2	Maximize profit						0.866	
FR3	Returns on investment						0.811	
FR4	Cost logistics						0.875	

Intention to Adopt								
ITA1	Intent to use measures in the future							0.682
ITA2	Plan to use measures as soon as possible							0.802
ITA3	Intent to use measures as soon as possible							0.770
ITA4	Plan to use measures in the future							0.615

Legends: GR = Government Regulation; MS = Management Support; OC = Organizational Competence; PC = Perceived Complexity; PB = Perceived Benefits; **Financial Resources, ITA = Intention to Adopt.**

4.4.1.1 Convergent and Discriminant validity assessment

To ensure that the variables have been correctly measured or validated, the construct validity was determined. Construct validity is the extent to which an instrument is actually measuring what it claims to be measuring. Two types of construct validity were used in this research study, namely convergent and discriminant validity, the purpose of which is outlined in the following subsection.

Convergent validity denotes the extent to which scores on a particular test correlate with scores on another test that are intended to measure the same construct. Discriminant validity denotes the extent to which scores on a particular test don't correlate or associate with scores from another test that are not designed to assess the same construct. According to Anderson et al., (2010), for the convergent validity to be acceptable, the composite reliability must be greater than 0.7 and the composite reliability must be greater than the average variance extracted values. As depicted in Table 4-4 both measurements were met.

The convergent validity determines the extent to which procedures of construct are correlating with the average variance extracted (AVE), whereby AVE ought to be greater than 0.5 (Anderson et al., 2010). According to Anderson et al., (2010) the discriminant validity that denotes the extent to which the construct vary from each other should only be established if all constructs share variance individual's items. The above statement can be verified by finding out whether the square root of the AVE is greater than the correlated construct's AVE (Karahanna and Agarwal, 2000). As depicted in Table 4-4 below, all AVE square roots are much higher than the inter-construct correlation. Therefore, the convergent validity and discriminant validity has been met.

Table 4-4: Validity Assessment

Convergent Validity			**Discriminant Validity**						
	CR	**AVE**	**GR**	**MS**	**OC**	**PC**	**PB**	**FR**	**ITA**
GR	.867	.597	**.772**						
MS	.841	.579	.028	**.761**					
OC	.933	.822	.025	.011	**.907**				
PC	.901	.694	-.004	-.002	.016	**.833**			
PB	.841	.579	.007	.019	.000	.025	**.761**		
FR	.898	.688	.022	.038	-.009	015	.003	**.829**	
ITA	.807	.677	.018	.027	.007	0.26	.049	-.003	**.823**

Legends: Composite Reliability (CR), Average Variance Extracted (AVE), Government Regulation (GR), Management Support (MS), Organizational Competence (OC), Perceived Complexity (PC), Perceived Benefits (PB), Financial Resources (FR), Intention to Adopt (ITA)
The numbers that are diagonal (in bolded shape) are the square root of each average variance extracted, whereas the non-diagonal numbers are inter-construct correlations. For discriminant validity to be acceptable the numbers in diagonal as indicated should be greater than the non-diagonal numbers.

4.5 Quantitative Analysis

To ensure that the research objectives were met, the results were analysed and presented in chronological order as per the sample survey questionnaire that are accessible in Appendix B.

4.5.1 Section A: Demographics Information

The demographic details mainly focus on the type of participants who participated in the research study. Characteristics of demographics used in this research study includes: position held, age, experience and qualification.

Position held

As shown in Figure 4-8, the majority of participants hold administrative positions. The figure shows that a total of 48.4% of the 647 participants are in administrative positions, followed by 18.5% in technical positions. 13.3% of participants where engineers, 12.5% in managerial positions and 7.3% was accountants. The results indicated that if the service organisation is occupied by a specific dominant group, they will have either a positive or negative influence on the results.

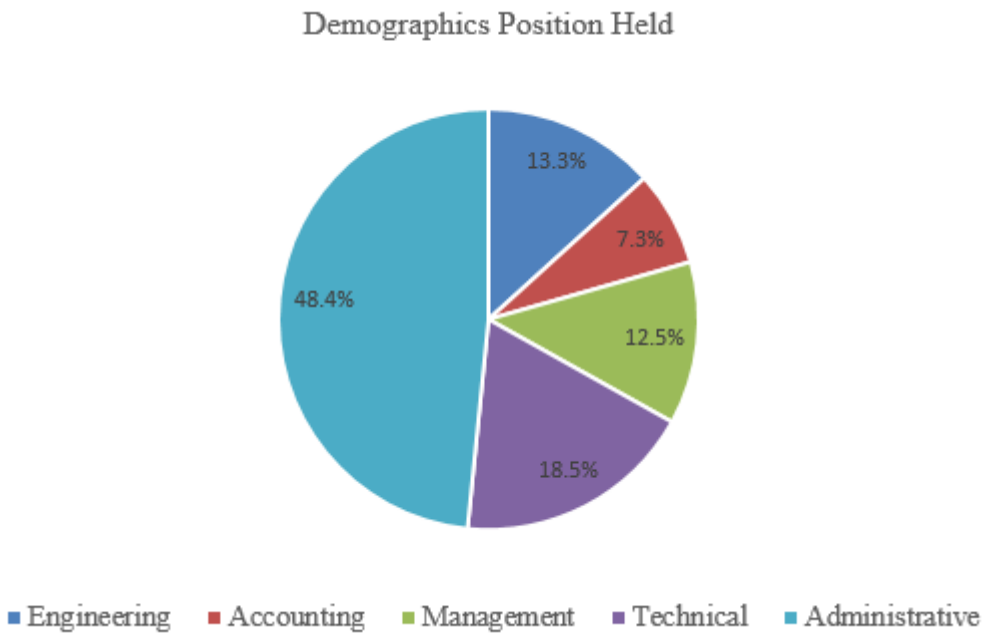


Figure 4-8: Demographical stats for positions

Age

As shown in Figure 4-9 for age statistics, the majority of the respondents have ages between 31 and 35 with 47.0% of the total 647 participants, followed by 19.9 percent of respondents being less than 25 years old. The age group between 41 and 45 are at 12.8% with age group between 25 and 30 being at 6.0%, whereas the age group of over 45 year olds being only 4.3% of the participants. It really demonstrated that the major influencer within the current research study was the age group between 31 and 35.

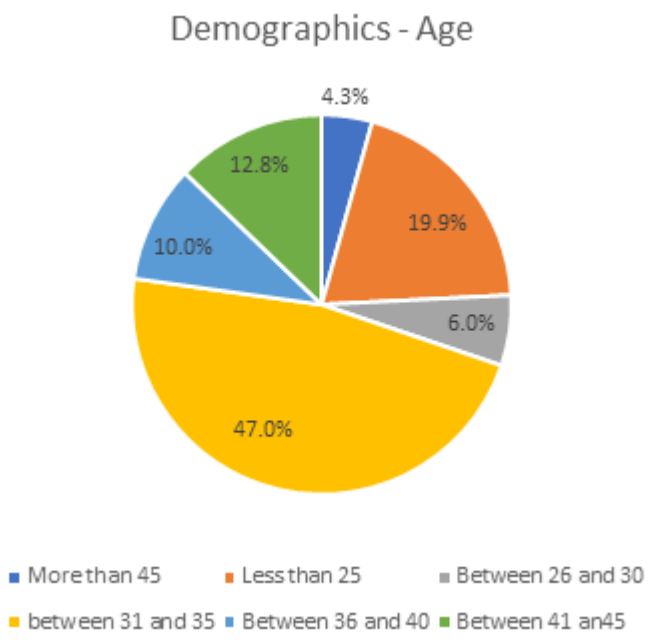


Figure 4-9: Demographical stats for Age

Experience

According to the statistics in Figure 4-10, the group with less than 5 years' experience indicated a positive intention to adopt with 50%, followed by the participants with 6 to 10 years' experience with a 41% of intention to adopt. The category for participants with less than 5

years' experience comprises of 46.8% of the overall 647 participants. Surprisingly the very same group with less than 5 years' experience has a massive 38.8% of the total 647 participants whom are not in support the adoption of the ICT security culture. The statistics again demonstrated that majority of a specific dominant group determine whether the results are positive or negative.

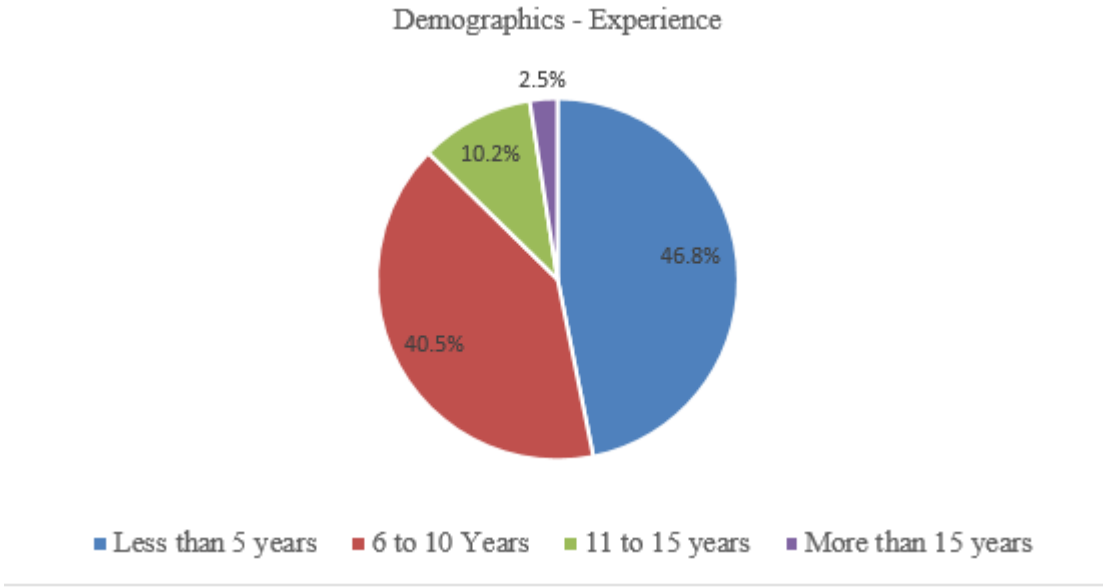


Figure 4-10: Demographical stats for Experience

Qualifications

According to the statistics in Figure 4-11, 41% of the participants in the graduate category indicated positive intention to adopt the ICT security culture followed by 39.9% participants in the diploma category with positive intention to adopt. Out of a total number of 647 participants 39.9% falls into the diploma category while 37.4% are graduates. The statistics indicated the impact of qualification in terms of the intention to adopt the ICT security culture in SMMEs.

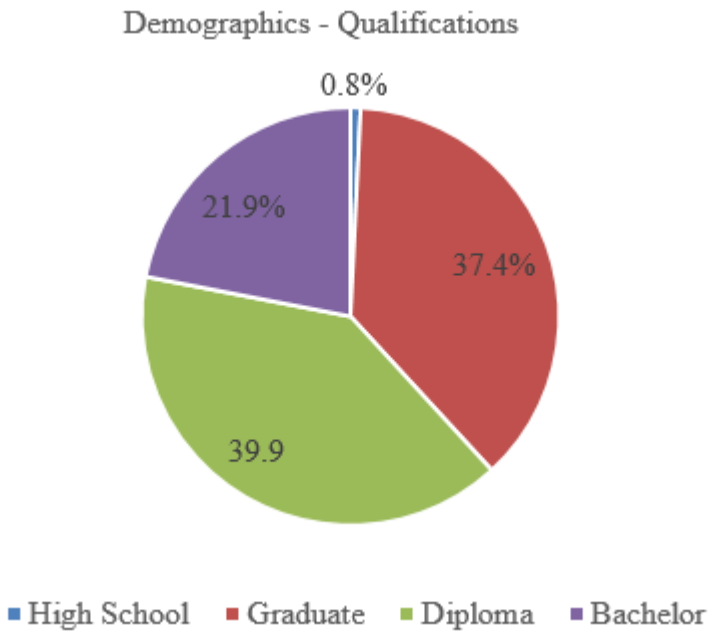


Figure 4-11: Demographical stats for qualifications

4.5.2 Section B: User's Perception on The Adoption of ICT Security Culture in SMMEs

The statements used in section B of the questionnaire of this research study (**refers Appendix B**) seeks to provide input to the research purposes that was outlined in chapter one. The quantitative analysis below used the frequency and percentage tables to highlight the viewpoint of respondents and their interpretations. The reliability and validity of the items in section B were checked in subsections 4.3 and 4.4 respectively.

a) TECHNOLOGICAL CONTEXT

(i) Perceived benefits towards the adoption of the ICT security culture

(a) Adoption of ICT security culture will improve service productivity

As shown in Table 4-5 below, 37 (5.7%) of the participants strongly disagree that adoption of ICT security culture will improve service productivity. Whereas 67 (10.4%) of the respondents disagree that adoption of ICT security culture will improve service productivity. In the same context, 159 (24.6%) of participants neither agree nor disagree that adoption of ICT security

culture will improve service productivity and 278 (42.9) of the participants agree that adoption of ICT security culture will improve service productivity. While 106 (16.4%) of the respondents strongly agree that adoption of ICT security culture will improve service productivity

Table 4-5: Adoption of ICT security culture will improve service productivity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	37	5.7	5.7	5.7
	Disagree	67	10.4	10.4	16.1
	Neither	159	24.6	24.6	40.7
	Agree	278	42.9	42.9	83.6
	Strongly Agree	106	16.4	16.4	100.0
	Total	647	100.0	100.0	

(b) Adoption of information security culture will be minimizing human error

As shown in Table 4-6 below, 19 (3.0%) of the participants strongly disagree that adoption of information security culture will minimize human error. Whereas 106 (16.4%) of the respondents disagree that adoption of information security culture will minimize human error. In the same context of intention, 127 (19.6%) of participants neither agree nor disagree that adoption of information security culture will minimize human error and 303 (46.8%) of the participants agree that adoption of information security culture will minimize human error. 92 (14.2%) of the respondents strongly agree that adoption of information security culture will minimize human error.

Table 4-6: Adoption of information security culture will be minimizing human error

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	3.0	3.0	3.0
	Disagree	106	16.4	16.4	19.4
	Neither	127	19.6	19.6	39.0
	Agree	303	46.8	46.8	85.8
	Strongly Agree	92	14.2	14.2	100.0

	Total	647	100.0	100.0	

(c) It would be easy for me to become skilful to protect information and data assets

As shown in Table 4-7 below, 8 (1.2%) of the participants strongly disagree that it would be easy for them to become skilful to protect information and data assets, whereas 61 (9.4%) of the respondents disagree that it would be easy for them to become skilful to protect information and data assets. In the same context of intention, 187 (29.0%) of participants neither agree nor disagree that it would be easy for them to become skilful to protect information and data assets and 295 (45.6%) of the participants agree that it would be easy for them to become skilful to protect information and data assets. 96 (14.8%) of the respondents strongly agree that it would be easy for them to become skilful to protect information and data assets.

Table 4-7: It would be easy for me to become skilful to protect information and data assets

		Frequency	Percent	Valid Percent	
Valid	Strongly Disagree	8	1.2	1.2	1.2
	Disagree	61	9.4	9.4	10.6
	Neither	187	29.0	29.0	39.6
	Agree	295	45.6	45.6	85.2
	Strongly Agree	96	14.8	14.8	100.0
	Total	647	100.0	100.0	

(d) My interaction with ICT security culture process will minimize data breaches

As shown in Table 4-8 below, 30 (4.6%) of the participants strongly disagree that their interaction with ICT security culture process will minimize data breaches. Whereas 36 (5.6%) of the respondents disagree that their interaction with ICT security culture process will minimize data breaches. In the same context of intention, 177 (27.4%) of participants neither agree nor disagree that their interaction with ICT security culture process will minimize data breaches and 308 (47.6) of the participants agree that their interaction with ICT security culture

process will minimize data breaches. 96 (14.8%) of the respondents strongly agree that their interaction with ICT security culture process will minimize data breaches

Table 4-8: My interaction with ICT security culture process will minimize data breaches

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	30	4.6	4.6	4.6
	Disagree	36	5.6	5.6	10.2
	Neither	177	27.4	27.4	37.6
	Agree	308	47.6	47.6	85.2
	Strongly Agree	96	14.8	14.8	100.0
	Total	647	100.0	100.0	

(ii) Perceived complexity towards the adoption of the ICT security culture

(a) The adoption of the ICT security culture will not inconvenience the way we are doing business.

As shown in Table 4-9 below, 55 (8.5%) of the participants strongly disagree that adoption of the ICT security culture will not inconvenience the way they are doing business. Whereas 98 (15.0%) of the respondents disagree that adoption of the ICT security culture will not inconvenience the way they are doing business. In the same context of intention, 288 (44.5%) of participants neither agree nor disagree that adoption of the ICT security culture will not inconvenience the way they are doing business and 169 (26.0%) of the participants agree that adoption of the ICT security culture will not inconvenience the way they are doing business. 37 (6.0%) of the respondents strongly agree that adoption of the ICT security culture will not inconvenience the way they are doing business.

Table 4-9: The adoption of the ICT security culture will not inconvenience the way we are doing business.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	55	8.5	8.5	8.5
	Disagree	98	15.0	15.0	23.5

	Neither	288	44.5	44.5	68.0
	Agree	169	26.0	26.0	94.0
	Strongly Agree	37	6.0	6.0	100.0
	Total	647	100.0	100.0	

(b) Learning to adapt the adoption of ICT security culture will be easy

As shown in Table 4-10 below, 39 (6.0%) of the participants strongly disagree that learning to adapt the adoption of ICT security culture will be easy, whereas 97 (15.0%) of the respondents disagree that learning to adapt the adoption of ICT security culture will be easy. In the same context of intention, 227 (35.1%) of participants neither agree nor disagree that learning to adapt the adoption of ICT security culture will be easy and 198 (30.6%) of the participants agree that learning to adapt the adoption of ICT security culture will be easy. 86 (13.3%) of the respondents strongly agree that learning to adapt the adoption of ICT security culture will be easy

Table 4-10: Learning to adapt the adoption of ICT security culture will be easy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	39	6.0	6.0	6.0
	Disagree	97	15.0	15.0	21.0
	Neither	227	35.1	35.1	56.1
	Agree	198	30.6	30.6	86.7
	Strongly Agree	86	13.3	13.3	100.0
	Total	647	100.0	100.0	

(c) It is easy for our SMMEs employees to become skilful in using the innovation.

As shown in Table 4-11 below, 21 (3.2%) of the participants strongly disagree that it is easy for our SMMEs employees to become skilful in using the innovation, whereas 87 (13.4%) of the respondents disagree that it is easy for our SMMEs employees to become skilful in using the innovation. In the same context of intention, 260 (40.2%) of participants neither agree nor

disagree that it is easy for our SMMEs employees to become skilful in using the innovation and 189 (29.2%) of the participants agree that it is easy for our SMMEs employees to become skilful in using the innovation. 90 (14.0%) of the respondents strongly agree that it is easy for our SMMEs employees to become skilful in using the innovation.

Table 4-11: It is easy for our SMMEs employees to become skilful in using the innovation.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	21	3.2	3.2	3.2
	Disagree	87	13.4	13.4	16.6
	Neither	260	40.2	24.7	41.3
	Agree	189	29.2	44.7	86.0
	Strongly Agree	90	14.0	14.0	100.0
	Total	647	100.0	100.0	

(d) Interacting or Adoption of ICTs security culture will be flexible.

As shown in Table 4-12 below, 26 (4.0%) of the participants strongly disagree that interacting, or adoption of ICTs security culture will be flexible, whereas 93 (14.4%) of the respondents disagree that interacting, or adoption of ICTs security culture will be flexible. In the same context of intention, 277 (42.8%) of participants neither agree nor disagree that interacting, or adoption of ICTs security culture will be flexible and 196 (30.3%) of the participants agree that interacting or adoption of ICTs security culture will be flexible. 55 (8.5%) of the respondents strongly agree that interacting or adoption of ICTs security culture will be flexible.

Table 4-12: Interacting or Adoption of ICTs security culture will be flexible.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	26	4.0	4.0	4.0
	Disagree	93	14.4	14.4	18.4
	Neither	277	42.8	42.8	61.2
	Agree	196	30.3	30.3	91.5
	Strongly Agree	55	8.5	8.5	100.0
	Total	647	100.0	100.0	

b) ENVIRONMENTAL CONTEXT

(i) Government regulations towards the adoption of the ICT security culture

(a) Government policies allows the adoption of ICT security culture

As shown in Table 4-13 below, 18 (2.8%) of the participants strongly disagree that government policies allow the adoption of ICT security culture, whereas 83 (12.8%) of the respondents disagree that government policies allow the adoption of ICT security culture. In the same context of intention, 177 (27.4%) of participants neither agree nor disagree that government policies allow the adoption of ICT security culture and 293 (45.3) of the participants agree that government policies allow the adoption of ICT security culture. 95 (11.6%) of the respondents strongly agree that government policies allow the adoption of ICT security culture.

Table 4-13: Government policies allows the adoption of ICT security culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	18	2.8	2.8	2.8
	Disagree	83	12.8	12.8	15.6
	Neither	177	27.4	27.4	43.0
	Agree	294	45.4	45.4	88.4
	Strongly Agree	75	11.6	11.6	100.0
	Total	647	100.0	100.0	

(b) We believe that the SMMEs environment (business culture) is conducive enough to adopt ICT security culture

As shown in Table 4-14 below, 36 (5.6%) of the participants strongly disagree that SMMEs environment (business culture) is conducive enough to adopt ICT security culture, whereas 88 (13.6%) of the respondents disagree that SMMEs environment (business culture) is conducive enough to adopt ICT security culture. In the same context of intention, 177 (27.4%) of participants neither agree nor disagree that SMMEs environment (business culture) is conducive enough to adopt ICT security culture and 296 (45.7) of the participants agree that

SMMEs environment (business culture) is conducive enough to adopt ICT security culture. 50 (7.7%) of the respondents strongly agree that SMMEs environment (business culture) is conducive enough to adopt ICT security culture

Table 4-14: We believe that the SMMEs environment (business culture) is conducive enough to adopt ICT security culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	36	5.6	5.6	5.6
	Disagree	88	13.6	13.6	19.2
	Neither	177	27.4	27.4	46.6
	Agree	296	45.7	45.7	92.3
	Strongly Agree	50	7.7	7.7	100.0
	Total	647	100.0	100.0	

(c) We believe that government policies or regulations (Laws) will effectively minimize human error through adoption of ICT security culture

As shown in Table 4-15 below, 36 (5.6%) of the participants strongly disagree that government policies or regulations (Laws) will effectively minimize human error through adoption of ICT security culture, whereas 93 (14.4%) of the respondents disagree that government policies or regulations (Laws) will effectively minimize human error through adoption of ICT security culture. In the same context of intention, 187 (28.9%) of participants neither agree nor disagree that government policies or regulations (Laws) will effectively minimize human error through adoption of ICT security culture and 286 (44.2%) of the participants agree that government policies or regulations (Laws) will effectively minimize human error through adoption of ICT security culture. 45 (6.9%) of the respondents strongly agree that government policies or regulations (Laws) will effectively minimize human error through adoption of ICT security culture.

Table 4-15: We believe that government policies or regulations (Laws) will effective minimize human error through adoption of ICT security culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	36	5.6	5.6	5.6
	Disagree	93	14.4	14.4	20.0
	Neither	187	28.9	28.9	48.9
	Agree	286	44.2	44.2	93.1
	Strongly Agree	45	6.9	6.9	100.0
	Total	647	100.0	100.0	

(d) Proper handling of economic and political instability and human rights issues will allow the adoption of ICT security culture.

As shown in Table 4-16 below, 46 (7.1%) of the participants strongly disagree that proper handling of economic and political instability and human rights issues will allow the adoption of ICT security culture, whereas 78 (12.1%) of the respondents disagree that proper handling of economic and political instability and human rights issues will allow the adoption of ICT security culture. In the same context of intention, 183 (28.3%) of participants neither agree nor disagree that proper handling of economic and political instability and human rights issues will allow the adoption of ICT security culture and 299 (46.2) of the participants agree that proper handling of economic and political instability and human rights issues will allow the adoption of ICT security culture. 41 (6.3%) of the respondents strongly agree that proper handling of economic and political instability and human rights issues will allow the adoption of ICT security culture.

Table 4-16: Proper handling of economic, political instability and human rights issues will allow the adoption of ICT security culture.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	46	7.1	7.1	7.1
	Disagree	78	12.1	12.1	19.2
	Neither	183	28.3	28.3	47.5
	Agree	299	46.2	46.2	93.7
	Strongly Agree	41	6.3	6.3	100.0

	Total	647	100.0	100.0	

(e) We believe that government will demonstrate strong commitment to promote ICT security culture

As shown in Table 4-17 below, 48 (7.4%) of the participants strongly disagree that government will demonstrate strong commitment to promote ICT security culture, whereas 73 (11.3%) of the respondents disagree that government will demonstrate strong commitment to promote ICT security culture. In the same context of intention, 184 (28.4%) of participants neither agree nor disagree that government will demonstrate strong commitment to promote ICT security culture and 307 (47.3) of the participants agree that government will demonstrate strong commitment to promote ICT security culture. 35 (5.5%) of the respondents strongly agree that government will demonstrate strong commitment to promote ICT security culture

Table 4-17: We believe that government will demonstrate strong commitment to promote ICT security culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	48	7.4	7.4	7.4
	Disagree	73	11.3	11.3	18.7
	Neither	184	28.4	28.4	47.1
	Agree	307	47.4	47.4	94.5
	Strongly Agree	35	5.5	5.5	100.0
	Total	647	100.0	100.0	

c) ORGANISATIONAL CONTEXT

(i) Management support towards the adoption of the ICT security culture

(a) Management encourages employees to be ICT security champions.

As depicted in Table 4-18 below, 22 (3.4%) of the participants strongly disagree that management encourages employees to be ICT security champions, whereas 77 (12.0%) of the

respondents disagree that management encourages employees to be ICT security champions. In the same context of intention, 179 (27.6%) of participants neither disagree nor agree that management encourages employees to be ICT security champions and 271 (42.0%) of the participants agree that management encourages employees to be ICT security champions. 98 (15.0%) of the respondents strongly agree that Management encourages employees to be ICT security champions.

Table 4-18: Management encourages employees to be ICT security champions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	22	3.4	3.4	3.4
	Disagree	77	12.0	12.0	15.4
	Neither	179	27.6	27.6	43.0
	Agree	271	42.0	42.0	85.0
	Strongly Agree	98	15.0	15.0	100.0
		647	100	100	

(b) Management will make resources available for the adoption of the ICT security culture

As shown in Table 4-19 below, 26 (4.0%) of the participants strongly disagree that management will make resources available for the adoption of the ICT security culture, whereas 65 (10.0%) of the respondents disagree that management will make resources available for the adoption of the ICT security culture. In the same context of intention, 174 (27.0%) of participants neither agree nor disagree that management will make resources available for the adoption of the ICT security culture and 286 (44.2%) of the participants agree that management will make resources available for the adoption of the ICT security culture. 96 (14.8%) of the respondents strongly agree that management will make resources available for the adoption of the ICT security culture.

Table 4-19: Management will make resources available for the adoption of the ICT security culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	26	4.0	4.0	4.0
	Disagree	65	10.0	10.0	14.0
	Neither	174	27.0	27.0	41.0
	Agree	286	44.2	44.2	85.2
	Strongly Agree	96	14.8	14.8	100.0
		647	100	100	

(c) Adoption of any innovation activities are widely communicated and understood throughout the organisation.

As shown in Table 4-20 below, 42 (6.5%) of the participants strongly disagree that adoption of any innovation activities is widely communicated and understood throughout the organisation, whereas 95 (15.0%) of the respondents disagree that adoption of any innovation activities are widely communicated and understood throughout the organisation. In the same context of intention, 127 (19.5%) of participants neither agree nor disagree that adoption of any innovation activities is widely communicated and understood throughout the organisation and 298 (46.0%) of the participants agree adoption of any innovation activities are widely communicated and understood throughout the organisation. 85 (13.0%) of the respondents strongly agree that Adoption of any innovation activities are widely communicated and understood throughout the organisation.

Table 4-20: Adoption of any innovation activities are widely communicated and understood throughout the organisation.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	42	6.5	6.5	6.5
	Disagree	95	15.0	15.0	21.5
	Neither	127	19.5	19.5	41.0
	Agree	298	46.0	46.0	87.0
	Strongly Agree	85	13.0	13.0	100.0
		647	100	100	

(d) We believe that the SMMEs demonstrate strong commitment to promote information security culture.

As shown in Table 4-21 below, 34 (5.3%) of the participants strongly disagree that SMMEs demonstrate strong commitment to promote information security culture, whereas 109 (16.8%) of the respondents disagree that SMMEs demonstrate strong commitment to promote information security culture. In the same context of intention, 117 (18.1%) of participants neither agree nor disagree that SMMEs demonstrate strong commitment to promote information security culture and 306 (47.3) of the participants agree that SMMEs demonstrate strong commitment to promote information security culture. 81 (12.5%) of the respondents strongly agree that SMMEs demonstrate strong commitment to promote information security culture.

Table 4-21: We believe that the SMMEs demonstrate strong commitment to promote information security culture.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	34	5.3	5.3	5.3
	Disagree	109	16.8	16.8	21.0
	Neither	117	18.1	18.1	40.2
	Agree	306	47.3	47.3	87.5
	Strongly Agree	81	12.5	12.5	100.0
		647	100	100	

(ii) Organizational competence towards the adoption of the ICT security culture

(a) We have a good understanding of the challenges of adopting ICT security culture in our business

As shown in Table 4-22 below, 19 (3.0%) of the participants strongly disagree that they have a good thoughtful of the issues of adopting ICT safekeeping culture in their business, whereas 153 (23.6%) of the respondents disagree that they have a good thoughtful of the problems of

adopting ICT safekeeping culture in their business. In the same context of intention, 207 (32.0%) of participants neither agree nor disagree that they have a good comprehension of the problems of adopting ICT safekeeping culture in our business and 186 (28.7%) of the participants agree that they have a good comprehension of the problems of adopting ICT safekeeping culture in our business. 82 (12.7%) of the respondents strongly agree that they have a good comprehension of the problems of adopting ICT safekeeping culture in our business

Table 4-22: We have a good understanding of the challenges of adopting ICT security culture in our business.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	3.0	3.0	3.0
	Disagree	153	23.6	23.6	26.6
	Neither	207	32.0	32.0	58.6
	Agree	186	28.7	28.7	87.3
	Strongly Agree	82	12.7	12.7	100.0
	Total	647	100.0	100.0	

(b) Our organisation has a good understanding of adoption models that are applicable to our business.

As shown in Table 4-23 below, 36 (5.6%) of the participants strongly disagree that their organisation has a respectable comprehension of adoption frameworks that are applicable to their business, whereas 93 (14.4%) of the respondents disagree that their organisation has a good understanding of adoption frameworks that are applicable to their business. In the same context of intention, 234 (36.2%) of participants neither agree nor disagree that their organisation has a great comprehension of adoption frameworks that are applicable to their business and 188 (29.0%) of the participants agree that their organisation has a great comprehension of adoption frameworks that are applicable to their business. 96 (14.8%) of the

respondents strongly agree that their organisation has a great comprehension of adoption frameworks that are applicable to our business.

Table 4-23: Our organisation has a good understanding of adoption models that are applicable to our business.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	36	5.6	5.6	5.6
	Disagree	93	14.4	14.4	20.0
	Neither	234	36.2	36.2	56.2
	Agree	188	29.0	29.0	85.2
	Strongly Agree	96	14.8	14.8	100.0
	Total	647	100.0	100.0	

(c) The organisation has capable individuals to implement ICT security culture requirements.

As shown in Table 4-24 below, 33 (5.1%) of the participants strongly disagree that their organisation has capable individuals to implement ICT security culture requirements, whereas 160 (24.7%) of the respondents disagree that organisation has capable individuals to implement ICT security culture requirements. In the same context of intention, 137 (21.2%) of participants neither agree not disagree that their organisation has capable individuals to implement ICT security culture requirements and 270 (41.7%) of the participants agree that their organisation has capable individuals to implement ICT security culture requirements. 47 (7.3%) of the respondents strongly agree that their organisation has capable individuals to implement ICT security culture requirements.

Table 4-24: The organisation has capable individuals to implement ICT security culture requirements.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	33	5.1	5.1	5.1
	Disagree	160	24.7	24.7	29.8
	Neither	137	21.2	21.2	51.0

	Agree	270	41.7	41.7	92.7
	Strongly Agree	47	7.3	7.3	100.0
	Total	647	100.0	100.0	

(iii) Financial resources towards the adoption of the ICT security culture

(a) The adoption of ICT security culture will be costly to implement (i.e. initial investments or availability of resources).

As shown in Table 4-25 below, 38 (5.9%) of the participants strongly disagree that the adoption of ICT security culture will be costly to implement (i.e. initial investments or availability of resources). Whereas 93 (14.4%) of the respondents disagree that the adoption of ICT security culture will be costly to implement (i.e. initial investments or availability of resources). In the same context of intention, 174 (26.9%) of participants neither agree nor disagree that the adoption of ICT security culture will be costly to implement (i.e. initial investments or availability of resources) and 297 (45.9%) of the participants agree that the adoption of ICT security culture will be costly to implement (i.e. initial investments or availability of resources). 45 (6.9%) of the respondents strongly agree that the adoption of ICT security culture will be costly to implement (i.e. initial investments or availability of resources).

Table 4-25: The adoption of ICT security culture will be costly to implement. (i.e. initial investments or availability of resources)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	38	5.9	5.9	5.9
	Disagree	93	14.4	14.4	20.3
	Neither	174	26.9	26.9	47.2
	Agree	297	45.9	45.9	93.1
	Strongly Agree	45	6.9	6.9	100.0
	Total	647	100.0	100.0	

(b) The service organisation will maximize profit through the adoption of ICT security culture

As shown in Table 4-26 below, 31 (4.8%) of the participants strongly disagree that the service organisation will maximize profit through the adoption of ICT security culture, whereas 153 (23.6%) of the respondents disagree that the service organisation will maximize profit through the acceptance of ICT security culture. Within the same context of intention, 237 (36.6%) of participants neither agree nor disagree that the service organisation will maximize profit through the adoption of ICT security culture and 186 (29.0%) of the participants agree that the service organisation will maximize profit through the adoption of ICT security culture. 40 (6.0%) of the respondents strongly agree that the service organisation will maximize profit through the adoption of ICT security culture.

Table 4-26: The service organisation will maximize profit through the adoption of ICT security culture

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	31	4.8	4.8	4.8
	Disagree	153	23.6	23.6	28.4
	Neither	237	36.6	36.6	65.0
	Agree	186	29.0	29.0	94.0
	Strongly Agree	40	6.0	6.0	100.0
	Total	647	100.0	100.0	

(c) The adoption of ICT security culture will signify an investment with valuable returns.

As shown in Table 4-27 below, 26 (4.0%) of the participants strongly disagree that the adoption of ICT security culture will signify an investment with valuable returns, whereas 193 (29.8%) of the respondents disagree that the adoption of ICT security culture will signify an investment with valuable returns. In the same context of intention, 177 (27.4%) of participants neither agree nor disagree that the adoption of ICT security culture will signify an investment with

valuable returns and 194 (30.0%) of the participants agree that the adoption of ICT security culture will signify an investment with valuable returns. 57 (8.8%) of the respondents strongly agree that the adoption of ICT security culture will signify an investment with valuable returns.

Table 4-27: The adoption of ICT security culture will signify an investment with valuable returns.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	26	4.0	4.0	4.0
	Disagree	193	29.8	29.8	33.8
	Neither	177	27.4	27.4	61.2
	Agree	194	30.0	30.0	91.2
	Strongly Agree	57	8.8	8.8	100.0
	Total	647	100.0	100.0	

(d) The cost of logistics to support the adoption of the ICT security culture will be high. (i.e. Cost to train employees).

As shown in Table 4-28 below, 46 (7.1%) of the participants strongly disagree that the cost of logistics to support the adoption of the ICT security culture will be high, whereas 143 (22.1%) of the respondents disagree that the cost logistics to support the adoption of the ICT security culture will be high. In the same context of intention, 179 (27.7%) of participants neither agree nor disagree that the cost logistics to support the adoption of the ICT security culture will be high and 239 (36.9%) of the participants agree that the cost logistics to support the adoption of the ICT security culture will be high. 40 (6.2%) of the respondents strongly agree that the cost logistics to support the adoption of the ICT security culture will be high.

Table 4-28: The cost logistics to support the adoption of the ICT security culture will be high. (i.e. Cost to train employees)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	46	7.1	7.1	47.1
	Disagree	143	22.1	22.1	29.2
	Neither	179	27.7	27.7	56.9

	Agree	239	36.9	36.9	93.8
	Strongly Agree	40	6.2	6.2	100.0
	Total	647	100.0	100.0	

d) INTENTION TO ADOPT

(i) Intention to adopt ICT security culture

(Venkatesh, 2003) proposed that the behavioural intent to adopt or use a specific technology or innovation has substantial impact on usage behaviour. At the current moment, SMMEs, is adopting ICT security culture at a snail's pace. Thus, it is impossible to measure the actual usage of the ICT security culture. The current study measures the behavioural intention to adopt the ICT security culture and not the actual usage thereof.

(a) I intent to learn and use all measures of ICT security culture to protect information and data assets in the future.

As shown in Table 4-29 below, 26 (4.0%) of the participants strongly disagree that they intent to learn and use all measures of ICT security culture to protect information and data assets in the future, whereas 83 (12.8%) of the respondents disagree that they intent to learn and use all measures of ICT security culture to protect information and data assets in the future. In the same context of intention, 148 (22.9%) of participants are unsure whether they would learn and use the process or not. 293 (45.3%) of the participants agree that they intent to learn and use all measures of ICT security culture to protect information and data assets in the future, while 97 (15.0%) of the respondents strongly agree that they intent to learn and use all measures of ICT security culture to protect information and data assets in the future.

Table 4-29: I intent to learn and use all measures of ICT security culture to protect information and data assets in the future.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	26	4.0	4.0	4.0

	Disagree	83	12.8	12.8	16.8
	Neither	148	22.9	22.9	39.7
	Agree	293	45.3	45.3	85.0
	Strongly Agree	97	15.0	15.0	100.0
	Total	647	100.0	100.0	

(b) I intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible.

As shown in Table 4-30 below, 29 (4.5%) of the participants strongly disagree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible, whereas 80 (12.4%) of the respondents disagree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible. In the same context of intention, 155 (23.9%) of participants are unsure whether they will learn and use the process or not and 283 (43.7) of the participants agree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible. 100 (15.5%) of the respondents strongly agree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible.

Table 4-30: I intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	29	4.5	4.5	4.5
	Disagree	80	12.4	12.4	16.9
	Neither	155	23.9	23.9	40.8
	Agree	283	43.7	43.7	84.5
	Strongly Agree	100	15.5	15.5	100.0
	Total	647	100.0	100.0	

(c) I plan to learn and use all measures of ICT security culture to protect information and data assets in the future.

As shown in Table 4-31 below, 32 (5.0%) of the participants strongly disagree that they plan to learn and use all measures of ICT security culture to protect information and data assets in the future, whereas 80 (12.4%) of the respondents disagree that they plan to learn and use all measures of ICT security culture to protect information and data assets in the future. In the same context of intention, 151 (23.3%) of participants are unsure to whether they would learn and use the process or not and 290 (44.8) of the participants agree that they plan to learn and use all measures of ICT security culture to protect information and data assets in the future. 94 (14.5%) of the respondents strongly agree that they plan to learn and use all measures of ICT security culture to protect information and data assets in the future.

Table 4-31: I plan to learn and use all measures of ICT security culture to protect information and data assets in the future.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	32	5.0	5.0	5.0
	Disagree	80	12.4	12.4	17.4
	Neither	151	23.3	23.3	40.7
	Agree	290	44.8	44.8	85.5
	Strongly Agree	94	14.5	14.5	100.0
	Total	647	100.0	100.0	

(d) I intent to use all measures towards linking to the ICT security culture to protect information and data assets as soon as possible.

As shown in Table 4-32 below, 19 (3.0%) of the participants strongly disagree that they intent to learn and use all measures of ICT security culture to protect information and data asset as soon as possible, whereas 87 (13.4%) of the respondents disagree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as

possible. In the same context of intention, 160 (24.7%) of participants are unsure to they would learn and use the process or not and 289 (44.7) of the participants agree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible. 92 (14.2%) of the respondents strongly agree that they intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible.

Table 4-32: I intent to use all measures towards linking to ICT security culture to protect information and data assets as soon as possible.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	19	3.0	3.0	3.0
	Disagree	87	13.4	13.4	16.4
	Neither	160	24.7	24.7	41.1
	Agree	289	44.7	44.7	85.8
	Strongly Agree	92	14.2	14.2	100.0
	Total	647	100.0	100.0	

4.6 Relationships Between ICT Security Culture Variables and Intention to Adopt ICT Security Culture Variable

One of the purposes of this study was to evaluate or measure the proposed theoretical framework and determine if there was any association/relationship amongst the aspects to adopt ICT security culture and the intention to adopt factor; to achieve that the Pearson correlation coefficient was used. Based on the findings as per Table 4-33 below, there was a positive correlation coefficient between all independent and dependent variables for the adoption of ICT security culture in SMMEs in the Gauteng province South Africa. As shown in Table 4-33 below, the correlation coefficients (r) of this study ranges from r = 0.504 to r = 0.834.

Table 4-33: Correlation Coefficient

	MS	**PB**	**FR**	**OC**	**GR**	**PC**	**ITA**

Management Support	1						
Perceived Benefits	.785** N = 647	1					
Financial Resources	.585** N = 647	.604** N = 647	1				
Organisational Competence	.766** N = 647	.649** N = 647	.755** N = 647	1			
Government Regulations	.648** N = 647	.656** N = 647	.667** N = 647	.735** N = 647	1		
Perceived Complexity	.667** N = 647	.742** N = 647	.795** N = 647	.834** N = 647	.703** N = 647	1	
Intention to Adopt	.568** N = 647	.570** N = 647	.504** N = 647	.598** N = 647	.612** N = 647	.577** N = 647	1

** Correlation is significant at 0.01 level

The results in Figure 4-12 below show the correlation coefficients that were calculated to measure the strength of the relationship between the independent factors (ICT security culture factors) and the dependent factor (Intention to adopt security culture). Between the variables of management support and intention to adopt ICT security culture there is a moderate relationship based on Pearson's correlation coefficient results ($r = .568^{**}$, $p < .001$). Amongst the variable of financial resources and perceived intention to adopt ICT security culture there is a confirmation of relationship based on Pearson's correlation coefficient results ($r = 504^{**}$, $p < .001$). Between the variable of perceived benefits and intention to adopt ICT security culture there is a relationship as per Pearson's correlation coefficient results in Figure 4-12 ($r = .570^{**}$, $p < .001$). Between the variable organisational competence and intention to adopt ICT security

culture there is also a positive relationship based on Pearson's correlation coefficient results in figure 4-12 (r = .598**, p < .001). The relationship between the variable perceived complexity and intention to adopt ICT security culture is positive (r = .577**, p <.001) according to the results in Figure 4-12. There is significance relationship between the variable of government regulation and variable intention to adopt ICT security culture (r = .612**, p < .001).

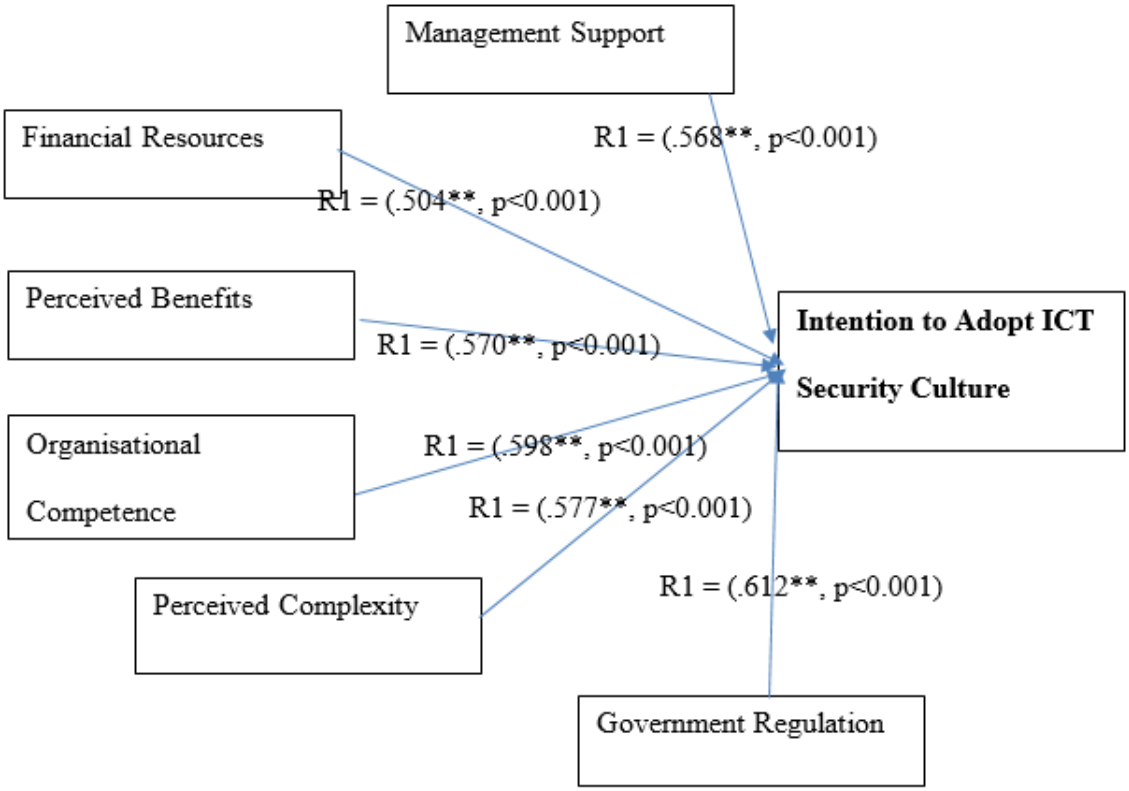


Figure 4-12: Correlation Coefficient

4.7 Hypotheses Test Results

The purpose of the study was to investigate and determine the effect of the TOE conceptual model construct on the adoption of the ICT security culture in SMMEs to minimize data breaches because of the human errors. Following the footsteps of the previous research papers, a multiple regression test was conducted on the model construct to measures if independent construct correlate to the dependent construct (adoption of ICT security culture.)

4.7.1.1 Regression analysis

This segment presents outcomes of the regression analysis of the adoption of ICT security culture in SMMEs in Gauteng province in South Africa as discussed in the preceding sections. To ensure that the proposed model is evaluated, correlation analyses was conducted. Correlation analysis was utilised to measure how strong the association amongst the independent variables and dependent variable are. Factors that have substantial relationship with the adoption of the ICT security culture were also identified. By testing the relationship within the proposed model, objective 2 of the research study, namely developing of a framework of adopting ICT security culture in SMMEs that links to the independent factors in the Gauteng province in South Africa, was accomplished.

To predict the unknown values of a variable (dependent) from the identified multiple variables (independent), multiple regression analysis or predictors was considered. Within this research study, multiple regression analysis was also used to develop a model that can establish the association amongst the independent variables and a dependent variable (ICT security culture) based on collected data of this study. Table 4-34 below presents the model summary of the predictors that are relevant for the R and R-Square. The predictor of intention to adopt ICT security culture in the model include: management support; financial resources; organizational competence; perceived benefits and perceived complexity and government regulations. R is viewed as the Pearson correlation coefficient. The multiple correlation coefficient R that form the square root of R-Square indicate the extent of impact of multiple independent factors associated to the individual dependent variable. R differs from 0 to 1 and within Table 4-34 below, R = 0.691 which suggests that there is a strong relationship between the multiple independent factors and the intention to adopt ICT security culture.

R-Square is viewed as the coefficient of determination because it signifies the amount of variance within the dependent variable (intention to adopt ICT security culture) which is

clarified by the independent variables. R-Square values differ from 0 to 1; the value 0 specify that there is no relationship, 1 indicate a great relationship. If the R-Square values are closer to 1.0, then it indicates a better model and the closer the R-square value to 0, that represent the poorest the model (signalling that knowing one area does not assist one know other areas at all). According to the results below, R-Square is 0.831 and from that it can interpreted that 83% of the variance in intention to adopt ICT security culture can be predicted from independent variables. Another unidentified determinant accounted for the remaining 17%, that is the amount of unexplained variance within the dependent variable (1 – R = 0.523). The adjusted R-Square is at 46.5% while the standard error of estimate (standard deviation) is 0.544. Adoption of ICT security culture is indicated by the F value of 40.015 with the strong significance level of 0.000 ($p<0.05$). The F value is used to check if independent variables are jointly significant or independently insignificant.

Table 4-34: Regression Analysis: Model Summary

Model	**Test**	**F**	**Results**
Regression		40.015	0.000
	R		0.691
	R-Square		0.831
	Adjusted R-Square		0.465
	Std. Error of the Estimate		0.54438

4.7.1.2 Hypotheses regression results

The following factors were discussed to ascertain their impact on the adoption of ICT security culture: Management support; Financial Resources; Organizational competence; Perceived Benefits and Perceived Complexity and Government regulations

Management Support

The first hypothesis H1, management support, was found to have significant positive influence or relationship (beta = 0.527**, p <0.05, N = 647) towards the adoption intentions. As shown in Table 4-35 below, the probability of proportion test validates the significance of the determinants management support that has a significance level of 0.000. The measurement outcome recommends that the intent to adopt is positively impacted by management support, which subsequently substantiates hypotheses one. Position of the result was consistent with earlier studies associated to the adoption of modernization. According to Ramaswany et al. (2015) management support plays a pivotal part in starting, implementing, and supporting, by making the right resources available for the adoption of the innovation. According to Fotoh and Aghaunor (2006) management support have positive impact on the adoption of innovation in the organisation. Management that values the benefit of innovation adoption will probably distribute the necessary resources for the adoption and eventual encourage team members to implement the required change. Should the management view that they will not conceive any benefit of the adoption of innovation they will likely not support the adoption Wu et al., (2011).

This result implied that management support is key in the adoption of ICT security culture in SMMEs. Based on this assessment the construct was supported.

Financial Resources

The second hypothesis H2, financial resource, was found to have less significant impact (beta = -0.064**, p >0.05, N = 647) on the intention to adopt. As shown in Table 4-35, the probability of proportional test indicated that financial resources are insignificant with the test level of 0.529, which is much higher than the 0.05 level. Based on the current assessment the presence of an association amongst financial resources and adoption intentions is not supported. Subsequently, hypotheses 4 is rejected. The above statement was supported by my research,

based on the below references. According to Fintz et al., (2002) SMMEs in the emerging states have tiny or no monetary power to obtain information technology and communication infrastructure or to venture into any innovation that require monetary resources. The same challenge was highlighted in the research by Van Brakel and Mutula (2007) that, financial resources was one of the inhibiting factor to hinder innovation development and adoption in SMMEs.

Organisational Competence

The third hypothesis H3, Organisation competence was found to have a less significant impact (beta = -0.073, p >0.05, N = 647) towards the adoption intentions. As shown in Table 4-35, the probability of proportional test indicated that organisational competence is insignificant with a test level of 0.299, that is much higher than the 0.05 level. Based on the current assessment the presence of an association amongst organisational competence and adoption intentions is not supported. Subsequently, hypotheses 4 is rejected.

Perceived Benefits

The fourth hypothesis H4, perceived benefits were found to have significant positive influence (beta = 0.547**, p <0.05 N = 647) towards the intention to adopt. As shown in Table 4-35, the probability of proportion test validates the significance of the determinants perceived benefits that has a significance level of 0.000. The measurement outcome recommends that the intention to adopt was positively impacted by the perceived benefits, which subsequently substantiates hypotheses one. Subsequently, hypotheses 4 is influential on intention to adopt then it is supported. Preceding theory reviews consistently found that the presence of perceived benefits simplified the adoption of innovation as the service organisation would know what benefits to be derived after their investment (Al-Qirim and Rashid, 2001; Teo et al., 2006).

Perceived Complexity

The fifth hypothesis H5, perceived complexity was found to have a less significant influence (beta = -0.026**, p >0.05, N = 647) towards the adoption intentions. As shown in Table 4-35, the probability of proportional test indicated that perceived complexity is insignificant with a test level of 0.614, that is much higher than the 0.05 level. Based on the current assessment the presence of relationship amongst perceived complexity and adoption intentions was not supported. Subsequently, hypotheses 5 was rejected. More researchers view perceived complexity as problematic during the innovation adoption phases. According to Dexter et al. (2001) perceived complexity is a major inhibitor for innovation adoption as it takes a lot of efforts to understand the solution. In most of the research papers complexity is linked to the technology that is problematic to utilize and comprehend. According to Dexter et al., (2001) a technology that is viewed as complex takes lots of time and energy from the learners to learn. According to Rogers (2003) complexity represents the level whereby invention is hard to comprehend and utilize. If the proposed technological innovation adoption towards the organisation is recognized as compatible towards the existing organisational values and belief, then it is more likely that the organisation will adopt it. According to Rogers (2003) the likelihood of adopting a new technological innovation is less likely to be embraced if it is viewed as more difficult to interact with. According to Otieno (2015), to maximize the probability for innovation adoption accomplishment, innovation should be user friendly, and easy to use.

Government Regulation

The sixth hypothesis H6, Government regulations was found to have significant positive influence (beta = 0.084**, p < 0.05, N = 647) towards the adoption intentions. As shown in Table 4-35, the probability of proportion test validates the significance of the determinant government regulations, which has a significance level of 0.000. The measurement outcome recommended that the intention to adopt is positively impacted by government regulations, that

subsequently substantiates hypotheses one. Hypotheses 6 was influential to the intention to adopt and is therefore supported.

Table 4-35 below displayed the hypotheses regression results for the constructs are actually significance and supported and not supported.

Table 4-35: Hypotheses regression results

Hypotheses	Variables	Beta	Sig.	Remarks
H3	Organisational Competence	-0.073**	0.299	Not Supported
H1	Management Support	0.527**	0.000	Supported
H2	Financial Resources	-0.064**	0.529	Not Supported
H5	Perceived Complexity	-0.026**	0.614	Not Supported
H4	Perceived Benefits	0.547**	0.000	Supported
H6	Government Regulations	0.084**	0.000	Supported
H7	Intention to Adopt	0.461**	0.003	Supported
*Note: Significant level at P <.05 two tailed **				

Source of information: This study

4.8 Final Research Model

Based on the research study results deliberated in chapter 4, Figure 4-13 below depict the final research model that could be used by SMMEs to adopt ICT security culture.

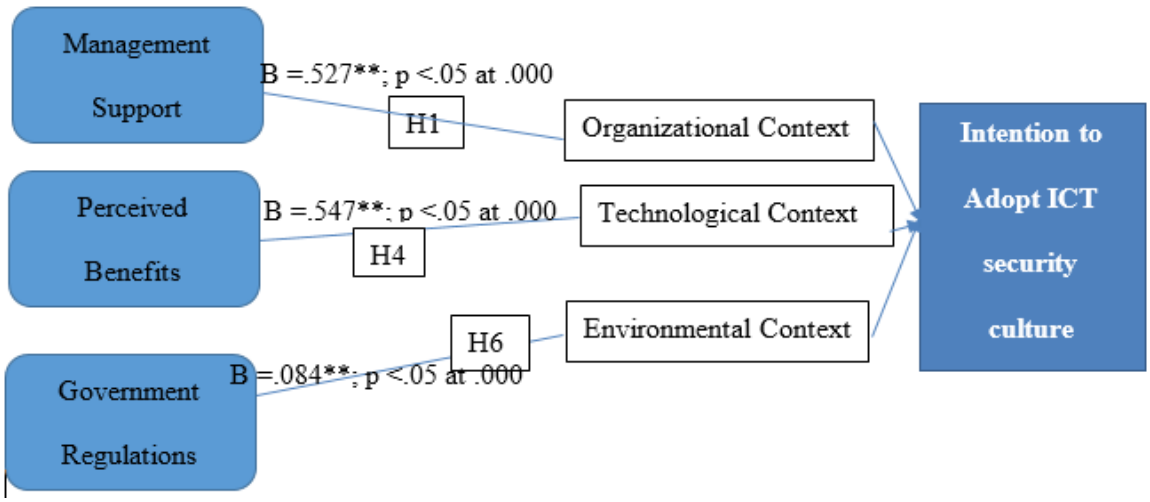


Figure 4-13: Final Research Model for Adoption of ICT Security Culture in SMMEs

4.9 Chapter Summary

Chapter 4 presented and analysed the collected data and highlighted the statistical results of the research. Most of the participants are professional between the age of 31 and 35 years of age and they occupy a stake of 47% in participation inclusively, this indicate what type of age group within the SMMEs have impact on the adoption of the technology innovation. Multiple regression was utilized to measure the association amongst independent and dependent variables. Also, within the current chapter the Cronbach's Alpha was utilised to test the reliability of the construct.

To establish the association between the ICT security culture factors and the intention to adopt ICT security culture, Pearson's correlation analysis process was conducted and the results displayed that all variables are correlated. To determine which factor have influence to adopt ICT security culture, the path coefficient was analysed for the extent of their influence. The confirmed proposed research model was also highlighted.

The following chapter detailed the recommendation and conclusions in-line with the results displayed in chapter 4.

CHAPTER FIVE

5 CONCLUSION AND RECOMMENDATION

The previous chapters dealt with the results of the research study and were displayed both in tabular and figure format. To ensure that there was no ambiguity or misunderstanding of the results, the findings were discussed in detail. The importance of the research study pertaining the adoption of ICT security culture in SMMEs was examined. Contents of this chapter deliberated about the research study conclusions, coupled with recommendation, based on the study results and highlight areas of future research.

5.1 Conclusion

The main determination of this research study was to explore user's perception on the adoption of ICT security culture in SMMEs in Gauteng province in South Africa to minimize data breaches because of the human errors. The research study used the adapted TOE theoretical framework to answer the research questions and achieve the study objectives. The research study was only conducted within the SMMEs sector in Gauteng province in South Africa. The demographic data of the research study was only used to highlight the type of population that completed the research study, they don't have a direct bearing in making the determination on factors that influences the adoption of the ICT security culture. The research questions and the research objectives were outlined as follows:

Research Questions

- ✓ How can the adoption of ICT security culture be supported in SMMEs to minimize human errors?
- ✓ What has been done to minimize security breaches through human error in Information Technology?

- ✓ What are the determinants that influence the adoption of ICT security culture in SMMEs?
- ✓ How to measure the effectiveness of framework for adopting ICT security culture in SMMEs?

Research Objectives were outlined below together with the conclusion reached based on the research results.

Objective 1: To investigate the literature and existing framework on what has been done to minimize security breaches as a result of human error.

The literature review indicated that there is not much research conducted in terms of determining factors influencing the adopting of the ICT security culture in SMMEs to minimize security breaches as a result of human error and the adoption models in this regard are minimal. Most of the research papers focused their attention in explaining what ICT security culture is rather than providing models or determinants that have positive relationship to the adoption of the ICT security culture to minimize security breaches as a result of human errors. According to Pollock (2017), their research study intends to develop a tool that will gather the historical data and apply a Human Factor Analysis and Classification Systems (HFACS) that will analyse the trend in organizations to minimize security breaches as a result of human errors. Output of this research study contributes to the literature on what has been done to minimize security breaches as a result of human errors by proposing the adoption model in that regards.

According to the theory reviews, majority of SMMEs are mainly putting more resources to the technological efforts of protecting their valuable assets than embracing the cultural aspect that form part of the protection value chain. Based on my observation, ICT security culture is still in its early stages and still has to be adopted by many service organisations as it is not viewed as something that will bring return on investment by the management while human errors are putting their reputation posture at risk.

Objective 2: To determine the factors or determinants that influence the adoption of ICT security culture in SMMEs.

Research question 1 and its objective was answered using regression analysis on the hypothesis constructs with regards to the determinants that have positive influence towards the adoption of the ICT security culture in SMMEs. The following factors were found to have positive influence towards the adoption of the ICT security culture in SMMEs: management support, government regulations and perceived benefits.

The research study concludes that management support influences the behaviour of SMMEs to adopt ICT security culture. In addition, the research study also found that majority of SMMEs are likely to adopt the technology innovation if management regards it as a strategic resource. Subsequently to that views management will allocate resources and reward employees for championing the ICT innovation and finally by inspiring employees to become ICT champions.

The research study concluded that, perceived benefits was found having influence on the adoption of ICT security culture in SMMEs. Similar to other research studies, if the users are of the view that technology innovation will improve their bottom line like: improving productivity, positively impacting profitability, improving business processes and improving their communication within their business will influence the adoption of ICT innovation in SMMEs.

Lastly, the research study concluded that government regulation influences the behaviour of SMMEs to adopt ICT security culture. The results suggest that if government enforces their regulation on how to adopt the technology innovation that will not impact on users' confidentiality and privacy the SMMEs will adopt the ICT innovation. However, this notion is problematic as SMMEs must make sure they have security controls in place to mitigate any

threats to user's confidentiality and privacy without relying to the government as it will only provide guidance not implementation of the controls.

Objective 3: To measure the effectiveness of the framework for adopting ICT security culture in SMMEs.

To achieve this objective, Pearson correlation coefficients was employed to measure the correlation or relationships effectiveness amongst the factors to adopt ICT security culture and intention to adopt. The results demonstrate a link between various factors, consequently, it has been affirmed that there is a positive relationship between the perceived factors to adopt ICT security culture and the intention to adopt factor. In addition to the correlation between the factors, the degree of path coefficient between the perceived factors and intention to adopt was conducted. The measurement outcome demonstrates a link between various factors. As a result of that outcome the model or framework was fit for the purposed hence the objective was met.

Objective 4: To propose a theoretical model or framework for the adoption of the ICT security culture that will help in minimizing the human error in SMMEs.

The proposed conceptual model was adapted from Tornatzky and Fleisher (1990) as depicted in Figure 3-1. The proposed model comprised of the following context: technology, environment and organisation that are mostly having an impact to the adoption of ICT security culture to minimize human errors. The relationship of the factors in the context were determined to confirm the supposed relationship with intention to adopt ICT security culture. Based on the above set outcomes the research study achieved the established objective.

Objective 5: To recommend the model for the adoption of the ICT security culture in SMMEs

After assessing the outcome from the research hypothesis, the model or framework was recommended that could be used in SMMEs to adopt ICT security culture that will minimize human error. The final recommended model is shown in Figure 4-13. The final model or

framework comprised of the following variables from the TOE model as outlined from the hypothesis assessment: management support; perceived benefits and government regulations. The research objective has been achieved as the final framework or model was established.

5.2 Limitations of the Study

Like other research studies, this study is not without its limitations. Sample size is one of the limitations as the total participants equates to 647 that excludes generalization to all SMMEs in Gauteng Province however further research is encouraged in this manner to get a wider audience. It would be advisable to increase the sample size to maximize the significance pertaining the exactness and generalization of the study.

The study was conducted in SMMEs in the Gauteng province in South Africa only, as a result it excluded other provinces and countries. The survey questionnaire was in English only; because of the time constraints and selection of the participants, vernacular languages were not considered as they would have prolonged the research study as more resources would been required. According to Delva et al., (2002), surveys that are distributed with time constraints are problematic as people who struggle with real or perceived time constraints are less likely to respond to surveys because these possible respondents feel overworked as they do not have time to complete the survey, hence the number of participants is only 647. Another limitation was that more research study or theory reviews could have been conducted in other languages that were not covered as the researcher only concentrated on literature that was written in English.

5.3 Recommendations / Suggested future works

- According to the literature reviews, not much has been researched to determine the determinant that have effect to the adoption of the ICT security culture to minimize

security breaches because of human errors as more researchers focused on explaining what security culture is than providing factors for adoption. Future works must be undertaken to determine other determinates that have effects to the adoption of ICT security culture.

- According to the theory reviews, adoption of information security culture is not mainly explored by many SMMEs and not viewed as key element towards the establishment of changing users' behaviours towards the information security within their organisation, more study is sought on how to adopt and maintain a reasonable ICT security culture in their establishment.
- More research should be undertaken using a different data collection method like interviews and different environment to ensure that any gab that is identified pertaining the adoption of the ICT security culture to mitigate data breaches is identified and mitigated. It will also improve the current perspective as indicated using the questionnaire instrument.
- To minimize data breaches because of human errors a major information security awareness drive is required within the SMMEs environment. It should not be assumed that since employees know how to access organisational infrastructure they know what to do should something entice them intentionally or unintentionally. Employees should also understand the data classification in their own business unit to ensure that due care is upheld for their protection.
- To minimize data breaches because of human error it is recommended that SMMEs around Gauteng Province in South Africa adopt the framework as outlined in this research study.

REFERENCES

ABDULLAH, N., HADI, N. U. & SENTOSA, I. (2016). An easy approach to exploratory factor analysis: marketing perspective Noor U1 Hadi. *Journal of Educational and Social research,* 6**,** 215-223.

AHMAD, A., MAYNARD, S., CHANG, S. E. & LIM, J. S. (2009). Exploring the relationship between organisational culture and information security culture. *In 7th Australian Information Security Management Confererence***,** 88.

AL-ALAWI, A. I. & AL-ALI, F. M. (2015). Factors affecting e-commerce adoption in SMEs in the GCC: An empirical study of Kuwait. *Research journal of information technology*.

AL-QIRIM, N. A. & RASHID, M. A. (2001). E-Commerce Technology Adoption framework by New Zealand small to medium enterprises. *Research letters information Mathematical Science,* 2**,** 63-70.

Alam, S.S & Noor, M.K.M. (2009). ICT adoption in Small and Medium Enterprises: an Empirical Evidence of Service Sectors in Malaysia. International Journal of Business and Management, 4, 112-125

ALNATHEER, M. & NELSON, K. (2009a). A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Security Research Centre Conferences*.

ALNATHEER, M. & NELSON, K. (2009b). A proposed framework for understanding information security culture and practices in the Saudi context. *Security Research Centre Conferences*.

ALSAMYDAI, M. J. (2014). Adaptation of the technology acceptannce model (TAM) to the use of mobile banking services. *International review of management and business research,* 3**,** 2016 - 2028.

Amrin, N. (2014). The Impact of Cyber Security on SMEs (Master's thesis, University of Twente)

ANDERSON, R. E., BABIN, B. J., BLACK, W. C. & HAIR, J. F. (2010). Multivariate Data Analysis. *7th edition. United States: Pearson*.

ANDRESS, J. & LEARY, M. (2017). Building a practical information security program. Cambridge: Syngress - 2016, 202

AYYAGARI, M., BECK, T. & DEMIRGUC-KUNT. (2005). Small and Medium Enterprises across the Globe. *Small Business Economics 29, 415-434*

BABIN, B. J., ANDERSON, R. E., TATHAM, R. L., HAIR, J. F. & BLACK, W. C. (2006). *Multivariate Data Analysis.* Upper Sadle River, N.J: Pearson Prentice Hall.

BAGALE, G. S. (2014). Determinants of E-commerce in India SMME sector: A conceptual research model based on TOE framework. *Universal Journal Management,* 2**,** 105-115.

BAGOZZI, R. P. (2007). The Legazy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems,* 8**,** 244-254.

BALA, H., BROWN, S. A. & VENKATESH, V. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *Managementd Information Systems,* 10**,** 1-20.

BIRKS, D. F. & MALHOTRA, N. K. (2000). Marketing Research: An Applied Approach, 2nd European edition, Prentice hall.

BOONSIRITOMACHAI, W. (2014). Enablers affecting the adoption of Business intelligence: A study of Thai small and medium-sized enterprises, Melbourne: College of business: Victoria University.

BOUGIE, R. (2016). Research methods for business: A skill building approach. *Research Methods. Cengage Learning.*

BRIDGES, W. (2003). Transition Process Framework. *Management and leadership training, online*

BWALYA, K. J. (2009). Factors Affecting Adoption of e-Government in Zambia. *Electronic Journal of Information Systems in Developing Countries,* 38**,** 1-13.

CAVUSOGLU, H., BULGURCU, A. & BENBASAT, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly,* 34**,** 523-548.

CHAN, M., WOON, I. & KANKANHALLI, A. (2006). Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior *Information privacy and security*.

Chang, S., Ruighaver, A.B., & Maynard, S.B. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security, 26(1), 56-62.

CHAU, P. & TAM, K. (1997). Factors affecting the adoption of open systems: An exploratory Study. *Management information systems quarterly,* 21.

CHAULA, J.A. (2006). A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance. Stockholm University, Stockholm.

CLARKE, G. (2001). Bridging the digital divide: How enterprise ownership and foreign competition affect internet access in Eastern Europe and Central Asia. *The World Bank, Development Research Group Regulation and Competition Policy*.

CORRIS, L. (2010). Information Security Governance: Integrating Security Intothe Organizational Culture. *In proceedings of the 2010 workshop on Governance of Technology, Information and policies - GTIP 10 (p. 35-41)* New York, USA

COSGUN, V. & DOGERLIOGLU, O. (2012). Critical success factors affecting e-commerce activities of small and medium enterprise. *Information and Managament,* 11**,** 1664-1676.

CRESWELL, J. W. (2008). *Educational research: Planning, Conducting, and evaluaing quantitative research.* (3rd edition). New Jersey: Pearson Education.

DA VEIGA, A. (2008). *Cultivating and Assessing Information Security Culture*. *MIS Quarterly, 13, 3, 319-340*

DA VEIGA, A. & ELOFF, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computer and Security,* 29**,** 196-207.

DA VEIGA, A. & MARTIN, A. (2015). Information Security Culture and Information protection culture: A validated assessment instrument. *Computer law and Security Review,* 31**,** 243-256.

DA VEIGA, A., MARTINS, N. & ELOFF, J. H. P. (2007). Information Security Culture - Validation of an assessment instrument. *South African Business Review,* 11**,** 147 - 166.

DANIELS, L. & NGWIRA, A. (1994). Results of a Nation-Wide Assessment on Micro, Small and Medium Enterprises in Malawi. *GEMINI Technical Report No. 53, PACT Publications, New York*.

DAVIS, F. D. (1986). A technology acceptance model for empirical testing new end-user infomration systems: Theory and results. *School of management, Massachusetts Institure of Technology*.

DAVIS, F. D. (1989). Technology Acceptance Model. *MIS Quarterly, 13, 3, 319-340*

DAVIS, F. D., BAGOZZI, R. P. & WARSHAW, P. R. 1989. User acceptance of computer-technology - a comparison of two theoretical-models. *Managment Science,* 35**,** 982-1003.

DELVA MD, K. J., KNAPPER CK, BIRTWHISTLE, R.V. (2002). Postal survey of approaches to learning among Ontario physicians: implications for continuing medical education. *British Medical Jounal,* 325**,** 1218 - 1222.

DEURSEN, N. V. (2015). How to reduce human error in information security incidents. *Computer and Security, vol. 37, 31-45*

DEXTER, A. S., CHWELOS, P. & BENBASAT, I. (2001). Research report:Empirical test of an EDI adoption model. *Information System Journal*.

DHILLON, G. (1995). Interpreting the Management of Information Systems Security. *London School of Economics and Political Science*.

DHILLON, G. (1997). Managing Information System Security; Palgrave Macmillan: London, UK; July;1997.

DILLMAN, D. A., DE LEEUW, E. & HOX, J. (2008). Mixed mode surveys: When and Why. *New York International Handbook of survey methodology*.

DURODOLU, O. (2016). Technology Acceptance Model as a predictor of using information systems to acquire information literacy skills. *Library of Philosophy and Practice 1450: 1-28*

DYERSON, R., HARINDRANATH, G. & BARNES, D. (2008). ICT in small firms: Factors affecting the adoption and use of ICT in Southeast England SMEs.

EDGAR, W. B. & LOCKWOOD, C. A. (2001). Organisational competencies: clarifiying the construct. *Journ Bus.Inqu,* 7**,** 21-23.

ELLINGER, A. E., AUTRY, C. W. & DAUGHERTY, P. J. (2011). Reverse logistics: the relationship between resource commitment and program performance. *Business logistics,* 22**,** 107-123.

ELOFF, J. H. P. & DA VEIGA, A. (2010). A framework and assessment instrument for information security culture. *Computer Security,* 29**,** 196-207.

ELOFF, J. H. P. & MARTINS, A. (2002). Information Security Culture. In proceedings of the IFIP TC11 17th. *International Conference on Information Security (SEC2002), Cairo, Egypt, 7-9 May 2002*.

FARAJI, E., GHAREGOZI, A. & HEYDARI, L. (2011). The study of information technology effect on e-commerce growth. *International conference on advancements in information technology,* 20.

FIDA, B.A. (2008). The importance of Small and Medium Enterprises (SMEs) in Economic Development. *Banking, Finance and Accounting Community.*

FINTZ, J., COURTNEY, S. & CLOETE, E. (2002). Small Business Acceptance and Adoption of e-commerce in western-cape province of South Africa. *The Electronic journal on Information systems in Developing countries,* 10**,** 1-13.

FISHBEIN, M. & AJZEN, I. (1975). The Theory of Reasoned Action as applied to moral behaviour: A confirmatory analysis, *Addison-Wesley Publishing Company, Reading. MA*.

FOTOH, X. & AGHAUNOR, L. (2006). Factors affecting ecommerce adoption in Nigerian banks. *Jonkoping International Business School, IT and Business Renewal*.

FRAMBACH, R. T. (1993). An integrated Model of Organizational Adoption and Diffusion of Innovations. *European Jorunal of Marketing,* 27**,** 22-41.

FURNELL, S. (2007). IFIP workshop - information security culture. *Computer Fraud Security,* 26**,** 35.

GANI, A. & ZAKARIA, O. (2003). A conceptual checklist of information security culture. *European Conference on Information Warfare and Security, University of Reading, Reading, UK, 30 June - 1 july 2003*.

GAVGANI, V. Z., MIRSAEED, S. J., DEHNAD, A. & ABDEKHODA, M. (2016). Factors influencing the adoption of e-learning in Tabriz University of Medical Sciences. *Medical Journal of the Islamic republic of Iran,* 30**,** 1 - 7.

GENNATOU, M., FURNELL, S. M. & DOWLAND, P. S. (2000). Promoting security awareness and training within small organisations. *Infomation security management workshop, Deakin University, Geelong, Australia, 7 November 2000*.

GERRARD, P. & CUNNINGHAM, J. B. (2003). The diffusion of internet banking among Singapore consumers. *The international journal of Banking Marketing.*

GOVERNMENT, W. C. P. (2007). Small, Medium and Micro Enterprises and the Informal Sector. *[Online]. Available:* https://www.westerncape.gov.za/text/2007/8/chapter_6_smme_&_informal_sector_masterfile.pdf *[Accessed 23 June 2017]*.

Greene, G., & D'Arcy, J. (2010). Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In *5th annual symposium on information assurance (ASIA'10)(p.1)*

GUNDU, T. & FLOWERDAY, S. V. (2013). IGNORANCE TO AWARENESS: TOWARDS AN INFORMATION SECURITY AWARENESS PROCESS *SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS,* 104.

GUPTA, A., SINGH, N. & OJHA, A. (2014). Identifying factors of "Organisational Information Security Management". *Journal of Enterprise information Management,* 27**,** 644-667.

HARFOUSHI, O., AKHORSHAIDEH, A. H., AQQAD, N., AL JANINI, M. & OBIEDAT, R. (2016). Factors Affecting the intention of Adopting Cloud Computing in Jordanian Hospitals. *Communication and network,* 8**,** 88-101.

HELOKUNNAS, T. & LIVONEN, L. (2003). Infomation security culture in small and medium size enterprises. *In e-Business Research Forum - eBRF 2003; Tampere University.*

HYLAND, P. & SUKANLAYA, S. (2012). Factors influencing the adoption of information technology in a construction business. *Australasian Journal of Construction Economics and Building,* 12**,** 72-86.

IBM. (2014). Confident and Careful: Insights from the 2014 CISO Assessment. *ISO copyright office3, Geneva, Switerland.*

ILVONEN, I. & KUUSISTO, T. (2003). Information security culture in small and medium size enterprises. *In Frontiers of e-Business Research 2003; Tampere University of Technology and University of Tampere, Finland, 2003*.

ISO. (2005). ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management. *ISO/IEC,2005*

JABBOURI, N. I. & ZAHARI, I. (2014). The role of core competencies on orrganisational performance: An empirical study in the Iraqi private banking sector. *European scientific Journal,* 1st edition.

Jafari, N., Kibbe, W.A., Du, P., Xiao Zhang, Huang, C.C., & Lin, S.M. (2010). Comparison of Beta-value and M-value methods for quantifying methylation levels by microarray analysis. *BMC bioinformatics*, 11(1), 587.

JEDYNAK, P. & BUGDOL, M. (2015). Intergrated Management Systems; Springler: Cham, Switzerland.

KANAAN-JEBNA, A., BAHARUDIN, A. S. & QIAN, L. Y. (2016). Factors affecting the adoption of enterprise resource planning (ERP) on cloud among small and medium enterprises (SMES) in Penang, Malysia. *Theoretical and Applied Information technology,* 88**,** 398-409.

Kankanhalli, A., Teo, H.H., Tan, B.C., & Wei, K.K. (2003). An integrative study of information systems security effectiveness. *International journal of information management,* 23(2), 139-154.

KANUPRIYA, C. (2018). Aligning teaching methods for learing outcomes: a need for educational change in management education using quality function deployment approach. *International journal of Learning and Change,* 10**,** 54-69.

KARAHANNA, E. & AGARWAL, R. (2000). Time Flies when you are having fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS quartely,* 24**,** 665 - 694.

KATSIKAS, S. K. (2000). Health Care Management and Information Systems Security: Awareness, Training. *International Journal of Medical Informatics***,** 129-135.

KHAN, R. (2010). Practical Approaches to Organizational Information Security Management. *SANS institude Reading Room.*

KOTHARI, C. R. (2004). Research methodology, methods and techniques. *India: New Age International Publishers,* (2ed).

KUUSISTO, R. & HELOKUNNAS, T. (2003). Information security culture in a value net. *International Engineering Management Conference (IEMC 2003), Albany, NY, USA, 2-4 November 2003*.

Lacey, D. (2010). Understanding and transforming organisational security culture. *Information management & computer security. 18(1), 4-13.*

LARCKER, D. & FORNELL, C. (1981). Evaluating structural equation models with unoservable variables and measurement erro. *Marketing Research,* 18**,** 39-50.

LEBOEA, S. K. & Ryan, T. (2017). The factors influencing SME failure in South Africa. *Masters dissertation, Cape Town: University of Cape Town.*

LEE, O. K., WANG, M., LIM, K. H. & PENG, Z. (2009). Knowledge management systems diffusion in chinese enterprises: A multistage approach using the technology-organization-environment framework. *Journal of global information management,* 17**,** 70-84.

LERTWONGSATIEN, C. & RAVICHANDRAN, T. (2005). Predicting SME's adoption of enterprises systems. *Enterprise Information Management* 22**,** 10-24.

LI, Y. H. (2008). An empirical investigation on the determinants of e-procurements adoption in chinese manufacturing enterprises. *International conference on management science and engineering* 1 and 2 32-37.

LIN, C. & CHANG, S. E. (2007). Exploring organizational culture for information security management. *Industrial Management and Data systems,* 107.

LIN, C. S. & CHIN, J. (2016). A behavioral model of managerial perspectives regarding technology acceptance in building energy management systems. *8***,** 1 - 13.

LIN, H. F. (2007). Understanding the determinants of electronic supply chain management system adoption: Using the TOE framework. *The Academy of Management Journal,* 86**,** 80-92.

LIN, H. F. & LIN, S. M. (2008). Determinants of e-business diffusion: A test of the technology diffusion perspective.

LIU, M. (2008). Determinants of e-commerce development: An empirical study by firms in shaanxi, China. *4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China,* 1-31**,** 9177-9180.

LOCH, K. & STRAUB, D. (2002). Toward a theory-based measurement of culture. *Global Information Management* 10**,** 13-23.

LONGLEY, S. (2015). Human error remains a big risk for UK SMEs as Employers fail to train staff on how to avoid data breaches. P*roceeding of the 1st International workshop on Socio-Technial Perspective in IS develoment. Stockholm, Sweden*

Louw, L., Thompson, K.L., & Von Solms, R. (2006). Cultivating an organizational information security culture. *Computer fraud & security. 10, 7-11.*

LUCEY, T. (2002). Quantitative Techniques (6th edition) London: Bookpower/ ELST.

MALLAT, N. 2007. Exploring consumer adoption of mobile payments - a qualitative study. *Strategic Information System,* 16**,** 413-432.

MANAF, A. A., HOOMAN, A., ABDULLAH, M. & KARAMIZADEH, S. (2013). An overview of principal component analysis. *Journal of Signal and Information Processing,* 4**,** 173-175.

MANFREDA, K. L., PETRIC, G. & PETROVCIC, A. (2016). The effect of email invitation elements on response rate in a web survey within an onlnine community. *Computers in Human Behaviours,* 56**,** 320 -329.

MARGULIES, J., PFLEEGER, S. L. N. & PFLEEGER, C. P. (2015). Security in Computing. 5th edition. Upper Saddle River, New Jersey: Prentice Hall. p877.

MARTIN, A. & ELOFF, J. H. P. (2002). Information security culture: *Paper presented at the 17th International Conference on Information Security. Boston: Kluwer Academic; 2002: 203 - 214*

MARTINEZ-RUIZ, M. D. P., BARBA-SANCHEZ, V. & JIMENEZ-ZARCO, A. I. (2007). Drivers, benefits and challenges of ICT adoption by Small and Medium Sized Enterprises. 5**,** 104-115.

MAURIEL, A. J., SCHROEDER, R. & DETERT, J. (2000a). A framework for linking culure and improvement initiatives in organisations. *Acad. Manag. Rev. ,* 25**,** 850-863.

MAURIEL, J. J., DETERT, J. R. & SHROEDER, R. C. (2000b). A framework for linking culture and improvement initiatives in organisations. *Academy of management review,* 25**,** 850-863.

MAYNARD, S., RUIGHAVER, A. B. & CHIA, P. (2002). Exploring Orgnisational security culture: developing a comprehensive research model. Paper presented at the Is one world conference, Las Vegas, Nevada USA.

MAYNARD, S. B., RUIGHAVER, A. B. & CHANG, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and security* 26**,** 56-62.

McIvor, R., Shiels, H. and O'Reilly, D. (2003). Understanding the implications of ICT adoption: Insights from SMEs. *Logistics Information Management, 16, 312-326.*

Meyer, C.O. (2005). Convergence towards a European strategic culture? A constructivist framework for explaining changing norms. *European Journal of international relations* 11(4), 523-549.

MILLINUEX, A. W. (1997). The funding of non-financial corporations in EU [1971-1993]: Evidence of convergence. Birmingham: Mimeo.

MIRZA, A. & ALHOGAIL, A. (2014). Information Security Culture: A definition and a literature review. *Proceeding of IEEE world congress on Computer Applications and Information Systems.*

MOHAMMED, A. (2015). Information Security Culture Critical Success Factor. *12th International Conference on Information Techmnology- New Generations*.

MOLLA, A. & LICKER, P. S. (2005). eCommerce adoption in developing countries: A model and instrument. *Information and Management,* 42**,** 877-899.

MOTWANI, J. & MIRCHANDANI, A. (2001). Understanding small business electronic commerce adoption: an empirical evidence analysis. *Journal of Computer Information Systems,* 12**,** 70 - 73.

MUKHTAR, M. & HERZALLAH, F. (2015). The impact of internal organisation factors on the adoption of e-commerce and its effect on organisational performance among palestinian small and medium enterprise. *Proccedings of the International conference on e-commerce***,** 105 - 111.

MURPHY, A. & TAYLOR, M. (2004). SMEs and eBusiness. *Small Business Enterprise Development,* 11**,** 280 - 289.

MYLENKO, N., ARDIC, O. P. & SALTANE, V. (2011). Small and medium enterprises: A cross-country analysis with a new data set. . *Policy research working paper. No 5538, The World Bank, Washington DC.*

NACHMIAS, C. & NACHMIAS, D. (2004). Research methods in the social sciences (5th edition), London: Arnold.

NAENNA, T. & PHICHITCHASOPA, N. (2013). Factors affecting the adoption of healthcare information technology. *EXCLI* Journal, vol. 12, pp. 413-436

NAHLIK, C., MORRIS, D. & ABBAD, M. M. (2009). Looking under the bonnet: Factors Affecting Student Adoption of E-learning System in Jordan. *International Review of Research in Open and Distance Learning,* 10**,** 1-23.

NEL, F. (2017). Determining a standard for information security culture. Thesis Research: North-West University.

NELSON, K., ALFAWAZ, S. & MOHANNAK, K. (2010). Information Security Culture: A behaivour compliance conceptual framework. 8th Australiasian Information Security Conference (AISC 2010), pp. 47 - 55.

NEPAD. (2001). The New Partnership for Africa's Development. Pretoria: NEPAD Secretariat.

NETSHANDAMA, M. J. (2006). The development of Small, Medium, and Micro Enterprises (SMMEs) in the Limpopo Province. *MBA Thesis, Department of Business Administration. South Africa: University of North West.*

NOSWORTHY, J. (2000). Implementing information security culture in the 21st century - Do you have the balancing factors. *Computer and Security,* 19**,** 337-347.

O'BRIEN, J., ISLAM, S., BAO, S., WENG, F., XIONG, W. & MA, A. (2013). Information Security Culture: Literature rewiew. *AISC, vol 105.*

OECD, (2009). The impact of the global crisis on SME and entrepreneurship financing and policy responses. Organisation for ecomomic co-operation and development, Centre for Entrepreneurship.

Ogbonna, E., & Wilkinson, B. (2003). The false promise of organisational culture change: A case of middle managers in grocery retailing. Journal of management studies, 40(5). 1151-1178.

ORODHO, J. A. (2008). Techniques of writing Research Proposals and Reports in Education and Social Sciences. *Masda publishers retrieved @ www.ku.ac.ke/schools/education/images*

OTIENO, A. P. (2015). FACTORS INFLUENCING ICT ADOPTION AND USAGE BY SMALL AND MEDIUM SIZED ENTERPRISES: *THE CASE OF NAIROBI BASED SMEs.*

PAI, J. C., LEE, G. G. & YEH, C. H. (2014). Using a technology-organization -environement framework to investigate the factors influencing e-business information technology capabilities. *Information development,* 31**,** 435-450.

PALVIA, P. C. & ALADWANI, A. M. (2002). Developing and validating an instrument for measuring user-perceived web quality. *Information Management,* 39**,** 467-476.

PELTIER, T. R. (2005). Implementing an information Security Awareness Program. *Information Systems Security,* 14**,** 37-49.

POLLOCK, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classificaion System (HFACS). *Conference on Cybersecurity Education Research and Practice,* 2.

PWC. (2013). Information Security Breaches Survey. Survey conducted by pwc for UK government Business and Innovation Department (2013). http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

QUARTELY, P. & ABOR, J. (2010). Issues in SMME development in Ghana and South Africa. *International Research Journal of Finance and Economics*, 39(6), 215 - 228.

RAHAYU, R. & DAY, J. (2015). Determinat factors of e-commerce adoption by SME in developing country: Evidence from Indonesia. *Social and behavioral sciences*, *195, 142 - 150.*

RAMASWANY, R., GANGWAR, H. & DATE, H. (2015). Understanding Determinants of Cloud Computing Adoption Using an Intergrated TAM-TOE Model. *Journal of Enterprise Information Management,* 28**,** 107-130.

Ren, K., Wang, Q., Wang, C., Li, J., & Lou, W. (2009 September). Enabling public verifiability and data dynamics for storage security in cloud computing. In European symposium on research in computer security. (pp. 355-370). Springer, Berlin, Heidelberg

ROBERTS, M. & PREMKUMAR, G. (1999). Adoption of new information technologies in rural small business. *The International Journal of Management Sciences,* 21**,** 467-484.

ROGERS, E. M. (1983). Diffusion of innovations. *Free Press, New York,* 3.

ROGERS, E. M. (1995). Diffusion of innovations. *3rd edn, Free Press, New York*.

ROGERS, E. M. (2003). Diffusion of innovations. *Free Press, New York,* 5.

ROGERSON, C. M. (2004). The Impact of the South African government SMMEs Programme: a ten - year review (1994 - 2003). . *Development Southern Africa,* 21.

RUIGHAVER, A. B., MAYNARD, S. & CHIA, P. (2002). Understanding organisational security culture. *In Proceedings of the PACIS Security Culture, Tokyo, Japan 2 - 3 September 2002*.

SACLA, C. & ANGELACHE, C. D. (2016a). Multiple linear regression used to analyse the correlation between GDP and some variables. *Romanian statistical review-supplement* 94 - 99.

SACLA, C. & ANGELACHE, C. D. (2016b). Multiple linear regression used to analyse the correlation between GDP and some variales. *Romanian statistical review-supplement nr 9/2016***,** 94-99.

SAINT-GERMAN, R. (2005). Information security management best practice based on international organisation for standardization / international electrotechnical commission 17799. *Information Management,* 39**,** 60-66.

SANCHEZ, L. E., CABALLERO, I., CAMACHO, S., FERNANDEZ-MEDINA, E. & SANTOS-OLMO, A. (2015). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet, 8(30), pp. 1-27.*

Saran, C. (2016). Human error causes more data loss than malicious attacks

Scarrott, G.G. (1985). Information, the life blood of organisation. the Computer Journal, 28(3), 203-205.

SCHEIN, E. H. (1985). *Organisational culture and leadership.* John Wiley & Sons.

SCHINDLER, P. S. & COOPER, D. R. (2011). Business research methods. 10th edition. Boston, MA and Burr Ridge, IL, McGraw-Hill.

Schlienger, T & Teufel, S. (2002). Information security culture - the socio-cultural dimension in information security managagement. In: IFIP TC11 international conference on information security, cairo, Egypt; 7-9 May 2002.

SCHLIENGER, T. & TEUFEL, S. (2003). Information Security Culture from Analysis to change. South African Computer Journal 2003;31: 46-52.

SCHULTZ, E. (2005). The Human Factor in Security. *Computer and Security,* 24**,** 425 - 426.

Seda, (2016). The Small, Medium, and Micro Enterprise Sector of South Africa: Bureau for Economic Research

SHAIN, M. & LONGLEY, S. (1991). Information Security Handbook. First edition. Withire:Macmillan Press Ltd, p 833.

SHLENS, J. (2014). A tutorial on principal components analysis. *Google Researc.* Mountain View, CA 94043.

Reed, R., Lemak, D. & Montgomery, J. (1996). Beyond Process: TQM Contnet and Firm performance. Academy of Management Review, 21, 173-202.

SHOEMAKER, F. F. & ROGERS, E. M. (1971). Communicaiton of Innovation: A Cross-cultural approach. *The Free Press, New York,* 2.

SIPONEN, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management Computer Security,* 8**,** 31-41.

SIRINGORINGO, H. & GURITNO, R. S. (2013). Perceived usefulness, ease of use and attitude towards online shopping airline ticket purchase. *Procedia social and behavioral sciences***,** 81.

StatsSA. Quarter 2: (2015). Quarterly labour Force survey. Pretoria.

Swift, M. (2009). ICT for SMEs - How ICT can be a force of viability. ICT for SMEs Seminar, The Cascadia Hotel & Conference centre Port of Spain, Trinidad & Tobago Wednesday, 25th, March, 2009

TEDDLIE, C. & TASHAKKORI, A. (1998). *Mixed methodology: Combining qualitative and quantitative approaches.* Thousand Oaks, Califonia: Sage Publications.

TEO, T. S. H., RANGANATHAN, C. & DHALIWAL, J. (2006). Key dimensions of inhibitors for the deployment of web-based business-to-business electronic commerce. *IEEE Transactions on Engineering Management* 53**,** 395-411.

THATTE, U. M. & GOGTAY, N. J. (2017). Principles of correlation analysis. *Journal of the association of physicians of India,* 65**,** 78-81.

THOPE, R., LOWE, A. & EASTERBU-SMITH (1991). Management Research: An introduction, Sage Publications, London.

THORNHILL, A. & SAUNDERS, M. (2003). Organisational justice, trust and the management of change an exploration. *Personal review,* 32**,** 360-375.

TORKZADEH, G. & DHILLON, G. (2006). Value-focused assessment of information system security in organisations. *Information Systems,* 16**,** 293-314.

TORNATZKY, L. G. & FLEISCHER, M. (1990). The process of Technological innovation. Lexington Books, Massachutetts.

TSUYA, N. O., TAMAKI, E., BUMBASS, L. L., RINDFUSS, R. R. & CHOE, M. K. (2015). Do low survey respose rates bias? Evidence from Japan. *Demographic Research,* 32**,** 797 - 828.

TUDORACHE, A., CEPTUREANU, S. I., CEPTUREANU, E. G. & ZGUBEA, F. (2012). Knowledge based economy assessment in Romania *Economic Management,* 15**,** 70-87.

VAN BRAKEL, P. & MUTULA, S. M. (2007). E-readiness of SME in the ICT sector in Botswana with respect to information access. *Electronic Library,* 24**,** 402-417.

VAN NIEKERK, J. & VON SOLMS, R. (2010). Information Security Culture: A management perspective. *Computer Security,* 29**,** 476-486.

VELILLA, M. & ROSANAS, J. M. (2005). The Ethics of management control systems: Developing technical and moral values. *Business Ethics,* 53**,** 87-96.

VENKATESH, V., MORRIS, M.G., DAVIS, G.B., DAVIS, F.D (2003). User acceptance of information technology: Towards a unified view. *MIS Quartely,* 27**,** 425-478.

VERIZON. (2012). Data breach investigation report 2012. Verizon RISK Team

VESELI, I. (2011). Measuring the effectiveness of information security awareness program. *Masters Thesis, GJovik University College.*

VON SOLMS, B. & VON SOLMS, R. (2000). From policies to culture. *Computers and security,* 23**,** 275-279.

VON SOLMS, R. & VAN NIEKERK, J. (2003). Establishing an Information Security Culture in Organisations: An Outcome-Based Education Approach. *Paper presented at the ISSA*.

VON SOLMS, R. & VAN NIEKERK, J. (2005). A holistic framework for the fostering of an information security sub-culture in organisation. The paper was presented at the 4th Annual ISSA conference SA.

Von Solms, R. & Van Niekerk, J. (2006). Understanding information security culture: A conceptual framework. in *Information security South Africa (ISSA), Johannesburg, South Africa, 2006, pp. 1-10.*

VON SOLMS, R. & VAN NIEKERK, J. (2010). Information security culture: A management perspective. *Computers Security,* 29**,** 476-486.

VON SOLMS, R. & VON SOLMS, B. (2004). From policies to culture. *Computer and Security,* 23**,** 275-279.

VROOM, C. & VON SOLMS, R. (2004). Towards information security behavioural compliance. *Computer and Security,* 23**,** 191 - 198.

WALKER, J. H., SAFFU, K. & HINSON, R. (2008). Strategic value and electronic commerce adoption among small and medium-sized enterprises in a transitional economy. *Journal of Business and industrial Marketing,* 23**,** 395 - 404.

WANG, Q. (2014). Kernel principal component analysis and its applications in face recognition of mobile reservatiation systems: A technology-organisation-environment framework *Tourism management,* 53.

WARREN, M., ZHOU, W. & NGO, L. (2005). Understanding transition towards information security culture change *In AISM (pp. 67-73)*.

WARREN, M. J. (2003). Australia's agenda for E-security education and research. *In Proceedings of the TC11/WG11.8 Third Annual World Conference on Information Security Education, Naval Post Graduate School, Monterey, CA, USA, 26-28 June 2003*.

WARREN, M. J., LICHTENSTEIN, S. & DOJKOVSKI, S. (2006). Challenges in fostering an information security culture in Australia small and medium sized enterprises. *Information Warfare and Security, Helsinki, Finland 1-2 June.*

Whitman, M.E., (2003). Enemy at the gate: threats to information security. *Communication of the ACM 46(8), p.91.*

WU, M., CHEN, Y. & LOW, C. (2011). Understanding the Determinants of Cloud Computing Adoption. *Industrial Management & Data Systems,* 111**,** 1006-1023.

XIONG, W., MA, A., WENG, F., BAO, S., ISLAM, S. & O'BRIEN. (2013). Information Security Culture: Literature Review. The University of Melbourne.

YIN, R. K. (1994). Case Study Research: Designs and Methods. *Beverly Hills, CA: Sage Publications*

ZHU, K., KRAEMER, K. & XU, S. (2003). Electronic business adoption by european firms: A cross-country assessment of the facilitators and inhibitors. *European Journal of Information Systems,* 12**,** 251-268.

ZHU, K., KRAEMER, K., XU, S. & DONG, S. (2006a). Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems,* 15**,** 601-616.

ZHU, K., KRAEMER, K., XU, S. X. & DONG, S. (2006b). Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems,* 15**,** 601-616.

ZIKMUND, W. G. (2003). Exploring Marketing Research. USA: Thompson Learning.

APPENDIX A: LETTER OF CONSENT

LETTER OF CONSENT FOR:

FRAMEWORK FOR ADOPTIONOF THE ICT SECURITY CULTURE IN THE SMMEs GAUTENG PROVINCE SOUTH AFRICA

RESEACHERS NAME: MORABA MOKWETLI
CONTACT DETAILS: (Mobile) 081 3544 757
(Office) 012 311 2007
E-ADDRESS : MORABAA@GMAIL.COM

SUPERVISORS NAME: T ZUVA
CONTACT DETAILS: 016 950 7587
E-ADDRESS: ZUVAT@VUT.AC.ZA

Dear Participants

You are invited to participate in a research study. The purpose of the study is to determine factor affecting the adoption of ICT security culture in SMMEs in the Gauteng province South Africa. You are welcome to ask any questions pertaining the study or about being a participant by using the above provided contact details.

Your insight of the environment will help in formulating the best framework for the environment. There are no known risks for participation in this study. Information or data collected from this research will be kept under strict security measures and reported only as a collective combined total. The data will be destroyed after the retention of pursuing the study. No one other that the researcher will know your individual answers to this questionnaire.

Your participation in this research study is voluntary; you are under no obligation to participate. By returning the completed questionnaire implies consent for participating in the study. Your personalised information will remain confidential and anonymous.

Any participation and cooperation in getting the insight of the environment by completing the questionnaires would be highly appreciated and will eventually help me in achieving my Information Technology Master's degree at Vaal University of Technology.

Thank you for your assistance in this important endeavour.

Sincerely yours,

Moraba Mokwetli

APPENDIX B: SURVEY QUESTIONNAIRES

Factors affecting adoption of the ICT security culture in SMMEs in the Gauteng province South Africa

Section A: **Demographic Information**

Please choose the appropriate option based on the following questions in line with your demographics.

1. Which position are you holding at your current employment?
    - Management
    - Administrative
    - Technical
    - Accounting
    - Engineering
2. How many years of experience do you have in the current employment?
    - Less than 5 years.
    - 6-10 years
    - 11 – 15 years
    - More than 15
3. Which is the highest degree or level of school you have completed?
    - Graduate
    - Bachelor
    - Diploma
    - High School
4. How old are you? Please indicate if you are:

- Less than 25 years
- 25-30 years
- 31-35
- 36-40
- 41-45
- More than 45 years

Section B: SMMEs Perception towards adoption of ICT security culture

Kindly read each statement and select the relevant choice by clicking within the square options that shows how strongly you either agree or disagree with the set statement

Rating scale: 1=Strongly Disagree, 2=Disagree, 3=Neither agree or disagree, 4=Agree, 5=Strongly agree

	Statements	**Strongly Disagree**	**Disagree**	**Neither agree or disagree**	**Agree**	**Strongly Agree**
Question 1 to 4: Management support towards the adoption of ICT security culture						
1	Management encourages employees to be ICT security champions.	1	2	3	4	5
2	Management will make resources available for the adoption of the ICT security culture	1	2	3	4	5
3	Adoption of any innovation activities are widely	1	2	3	4	5

	Statements	Strongly Disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree
	communicated and understood throughout the organisation					
4	We believe that the SMMEs demonstrate strong commitment to promote information security culture.	1	2	3	4	5
Question 5 to 8: Government Regulations						
5	Government policies allows the adoption of ICT security culture	1	2	3	4	5
6	We believe that the SMMEs environment (business culture) is conducive enough to adopt ICT security culture	1	2	3	4	5
7	We believe that government policies or regulations (Laws) will effective minimize human error through adoption of ICT security culture	1	2	3	4	5
8	Proper handling of economic, political instability and human rights issues will allow the	1	2	3	4	5

	Statements	Strongly Disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree
	adoption of ICT security culture.					
9	We believe that government will demonstrate strong commitment to promote ICT security culture	1	2	3	4	5
Organisational Competence						
10	We have a good understanding of the challenges of adopting ICT security culture in our business	1	2	3	4	5
11	Our organisation has a good understanding of adoption models that are applicable to our business.	1	2	3	4	5
12	The organisation has capable individuals to implement ICT security culture requirements.	1	2	3	4	5
Perceived Complexity towards adopting ICT security culture						
13	The adoption of ICT security culture will improve customer service	1	2	3	4	5

	Statements	Strongly Disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree
14	The adoption of ICT security culture will reduce cost of business operations	1	2	3	4	5
15	The adoption of the ICT security culture will enable the business to reap operational benefits.	1	2	3	4	5
16	The adoption of ICT security culture will help in improving distribution channels	1	2	3	4	5
Question 17 to 20: Perceived benefits towards adopting ICT security culture						
17	Adoption of ICT security culture will improve service productivity	1	2	3	4	5
18	Adoption of information security culture will be minimizing human error	1	2	3	4	5
19	It would be easy for me to become skilful to protect information and data assets	1	2	3	4	5

	Statements	Strongly Disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree
20	My interaction with ICT security culture process will minimize data breaches	1	2	3	4	5
Question 21 to 24: Financial Resources to adopt ICT security culture						
21	The adoption of ICT security culture will be costly to implement. (i.e. initial investments or availability of resources)	1	2	3	4	5
22	The service organisation will maximize profit through the adoption of ICT security culture	1	2	3	4	5
23	The adoption of ICT security culture will signify an investment with valuable returns.	1	2	3	4	5
24	The cost logistics to support the adoption of the ICT security culture will be high. (i.e. Cost to train employees)	1	2	3	4	5
Questions 25 to 28: Intention to use ICT security culture						

	Statements	Strongly Disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree
25	I intent to learn and use all measures of ICT security culture to protect information and data assets in the future.	1	2	3	4	5
26	I intent to learn and use all measures of ICT security culture to protect information and data assets as soon as possible.	1	2	3	4	5
27	I plan to learn and use all measures of ICT security culture to protect information and data assets in the future.	1	2	3	4	5
28	I plan to learn and use all measures of ICT security culture to protect information and data assets as soon as possible.	1	2	3	4	5

THANK YOU