Information security awareness in small information technology-dependent business organisations

Dissertation Presented as part of partial fulfilment of degree:

MASTERS of BUSINESS MANAGEMENT (INFORMATION TECHNOLOGY)

In the Department of Business Management

UNIVERSITY OF JOHANNESBURG

May 2014

By

Name: Pierre Jordaan

Student Number: 200802828

Dedication

TO MY FAMILY

FOR YOUR LOVE, GUIDANCE AND SUPPORT.

THIS DISSERTATION IS DEDICATED TO YOU

Acknowledgments

Firstly, I would like to acknowledge my supervisor Dr Kennedy Njenga of the University of Johannesburg. His patience, thoughts, ideas, and the lessons given to me on the research process and the structuring of this dissertation were invaluable. His advice was always and continues to be useful and this work would not have been possible without him.

Thank you, Kennedy, for your guidance and patience that kept me on track during my writings and research. I have learned so much as a researcher and it has been a personal and unforgettable experience.

Finally, I would like to thank my family and friends, and, above all, my God for the wisdom and energy to complete this dissertation. I could not have completed this dissertation without their understanding, patience, encouragement and support.

Abstract

Small businesses thrive in the developing economy of South Africa and address the important issue of unemployment and poverty that exist in the country. A large number of these business organisations can be found in the province of Gauteng because of the large and diverse economic contribution the province delivers to the economy of South Africa.

With the increased use of technology in the small businesses of Gauteng and South Africa, the risks around cyber-security, information security and other IT-related threats that can harm the businesses increase. As part of the related IT risks comes the information security awareness of the businesses. Research findings show that little to no information security awareness exists in the small IT-dependent business organisations of Gauteng, South Africa.

New knowledge has been gained from the information technology uses and information security awareness that exists in small business organisations. This knowledge is specific to the small business organisations of South Africa which places an African context to a global debate of information security awareness.

Keywords

Small business organisations, information security, information security awareness, personal and sensitive information.

Contents

Chapter 1

`

Small business organisations form part of a country's economy and can operate in the same or different markets as larger organisations. Information technology is used by small business organisations to do business and to form part of the digital economy. In Chapter 1 these two statements will be elaborated upon and will lead to a research problem that is deemed to be studied.

Chapter 1

Background

1.1 Small business organisations in South Africa

The South African National Small Business Act 102 of 1996 identifies a 'small business organisation' as an "entity" that can either be legally registered or not registered and that is mainly focused on conducting "small business matters." If a small business is formally registered it usually employs more than 5 people but less than 100, will have "fixed business premises," forms part of the "formal" economy and is often registered as a "proprietorship or closed corporation" (Gauteng provincial government, 2010:7-8). Small businesses thrive in the developing economy of South Africa and address the important issue of unemployment and poverty that exist in the country. The National Small Business Act of 1996 classifies small businesses in a "schedule" where eleven different types of operating industries are identified. The Act classifies each operating industry according to the "full-time paid employees" the organisation needs to have to be classified as a small business organisation in South Africa.

1.2 Small business organisations operating in the Gauteng province of South Africa

Gauteng currently represents only "*1.4%*" of South Africa's surface area but hosts around "*23.7%*" of the country's population, which amounts to "*12.2*" million people (SouthAfrica.info, 2012). A large number of small business organisations can be found in the province of Gauteng owing to the large and diverse economic contribution the province delivers to the economy of South Africa.

Small business organisations that existis in Gauteng and South Africa can take on many forms and operate in different industries. One form is generally refered to as a '*Spaza shop*' and has been included as part of the South Afirican legislation since "1982". A *Spaza shop* is usually defined as a "*small family business in a township*" and they have been documented as having made use of information technology (Scheers, 2010).

1.3 Unemployment in Gauteng province and Small Business Development

In the census of 2011 it was reported that 26.3% of Gauteng's population was unemployed according to the "official unemployment" definition (Stats SA, 2012). Unemployment is measured using the strict definition referring to people "*actively searching for work"* and the broad definition of unemployment referring to people not actively searching for employment (Nattrass, Wakeford, & Muradzikwa, 2003). Unemployment types can further be seen as "structural unemployment (market imperfections), frictional unemployment (new market entrants and movements), cyclical unemployment (demand and supply) and seasonal unemployment (change in demand over periods") (Mafiri, 2002:p7-12.) These unemployment types also occur in the South African marketplace and affect the small business organisations. Unemployment stretches across the different cultures and age groups of the country and one of the approaches used to solve this problem is the encouragement of local, small and informal business in South Africa (Ladzani & Netswera, 2009).

The development of small businesses in South Africa is deemed to be extremely important as it forms part of the country's strategy of reducing unemployment. The "Small Enterprise Development Agency (SEDA)" that is operated from the "Department of Trade and Industry" is one government initiative that is used to support the development of small businesses in South Africa (SEDA, n.d.).

For the period "1985-2005, only around 10% of the employment opportunities created" was done by "large established firms", showing the need to focus on the small business environment (SBP, 2009).

1.4 Diffusion of and dependency of IT into small business organisations

In a study conducted on small businesses in the USA, it was found that information technology could have a big impact on the success of a business, whether it involves delivering a better service to the customer or executing business processes more efficiently (Beheshti, 2004). Within the small business environment, Information Technology has been known to "*increase business efficiency and benefits as well as to make the organisation more competitive towards the outside business environment*" (Baard & van den Berg, 2004).

Because of the increased availability as well as affordability of information and communications technologies (ICT), many small South African business organisations are incorporating the use of information technology as part of their business processes. A business process can be defined in a simple manner as the "way that work is performed" in the organisation (Carkenord, 2009). A critical business process can then be said to be business processes or functions that the business organisation simply cannot survive without. The use of information technology has helped organisations in creating new opportunities and business processes that contribute to the mission of the business. Many small South African businesses are increasingly being information technology-dependant and are making use of ICT as part of their core or critical business function. These functions have included practices such as online banking, bookkeeping, tax returns and numerous other tools for conducting e-commerce and making the trade of the business more effective.

The use of IT can be related to any of the above mentioned business activities and should this component fail, the business would suffer a halt in operations & production. This can be problematic for small businesses that have no form of business continuity planning or disaster recovery plans, especially if they are dependent on a fragile component such as IT. From the defined critical business process one can suggest that if a critical IT component in a small business of Gauteng fails, the business could suffer damage such as financial or reputational damage.

1.5 Risks in the small business environment of Gauteng and South Africa: Cybercrimes and the need for awareness

With the increased use of technology in the small businesses of Gauteng and South Africa, the risks also increase around cyber-security, information security and other IT-related threats that can harm a business. To control these risks, governing structures and policies are usually adopted by larger organisations where knowledge and skills are more abundant. However, governance and security resources are not always available and implemented by smaller organisations that also make use of information technology as part of the business.

The increased use of information technology services can also be fuelled by the “increased availability of broadband services” to the South African consumer, creating more “opportunity for cybercrimes to take place” (Grobler & Jansen van Vuuren, 2010). Grobler *et al (2011:113)* further describe the digital space as a “dangerous place that poses a threat to the local community” of South Africa. The encouragement of entrepreneurship and new businesses within the South African market has been a long-time top priority for government. This and the described need to reduce unemployment in the country all contribute to the increased usage of IT in the small business sector.

Without the necessary support and awareness around cybercrimes, the small-business sector could become another target for criminals and an opportunity to commit cybercrimes. Owing to the critical role that information technology plays in some organisations, threats such as cybercrimes can affect the organisation severely and can even cause the organisation to discontinue operations. (Mejias, 2012).

Small business organisations in South Africa do not have high future prosperity expectations as a big reason for business failure is due to owners not having enough "management competencies" (Urban & Naidoo, 2012). Managerial decision-making is critical to the business organisation regardless of the size of the business. It is also known that small businesses in South Africa often lack the proper managerial skills with a "lack of experience" in the management of these shortcoming management requirements (Mbonyane & Ladzani, 2011).

Urban and Naidoo (2012:146-163) further conclude that owing to a shortage of "skills" in the small business sector, a need for awareness and awareness initiatives exists against threats that can harm the organisations. Some of the other factors that can contribute to the failure of small business organisations include the "internal market in which it operates, problems with employees, operational problems and financial problems" (Scheers, 2010). These factors can easily relate to the use of information technology that is utilised to gain market competitiveness as well as the overall business processes that are supported by information technology.

Cybercrimes can be defined as "any illegal activities" such as the abuse of personal information that takes place through the use of "internet components" and which have to be carefully managed due to its unique nature and continually growing risks (Salifu, 2008:433). Crime affects the lives of all South Africans, which make it essential to have the necessary tools and initiatives in place that can benefit everyone affected – directly or indirectly. The problem of cyber-security is further escalated by the low literacy rates in South Africa and a lack of information security awareness in the business environment (Grobler & Jansen van Vuuren, 2010).

Not all employees are educated in the workplace to be aware of the threats that involve the sharing of personal information or are taught to show due diligence when providing personal information to others. Not all business organisations in South Africa follow guidelines or best practices such as the King Reports or COBIT to govern their ICT use or to protect personal information that is stored by the business (Kyobe, 2010). The protection of personal information thus forms a critical part of cyber-security, which, as explained, has a definite influence on the South African business community.

People are still implicated as being one of the biggest "weaknesses" in the "security of systems" used in organisations and this emphasises the importance of educating the users around the secure use of these systems (Boucher & Flowerday, 2011) & (Harnesk & Lindstrom, 2011: 262). IT systems in the business environment in this case include both the use of information and technology in the organisation.

Without the necessary knowledge or level of awareness, businesses will not be able to fully protect their sensitive information and the personally stored information of its clients, business partners and other stakeholders. In a recent study on small businesses in South Africa it was again stated that management experience is mostly learned by business owners through "a trial and error process", which can be extremely risky to the business especially when dealing with critical IT components (Perks, 2010).

The "Protection of Personal Information Act of 2013" defines "personal information as any information that can identify a living person or legal person" and can contain any of the following and even more:

- "Information relating to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, health, disability, beliefs and culture, religion, date of birth"
- "Information on any personal records such as medical, financial, criminal or employment history"
- "Contact numbers, addresses and e-mails" or any other information directly referring to a person including "biometrical information".
- "Information on opinions including about other people, private correspondence and the disclosure of a person's names against the information relating to a person such as a phone number or address"

  (Protection of Personal Information Act, 2013)

This definition of personal information is extensively stated in the Protection of Personal Information Act and also applies to small business organisations and individuals in these organisations. Information security awareness constitutes one of the protection mechanisms against the threats that exist for business organisations. It is for these reasons that awareness should be created in the small business organisations of Gauteng so that cybercrimes and other information security threats can be minimised.

1.6 Background to the research problem

The outline of this study will be to gain an understanding of the level of information security awareness in information technology-dependant business organisations of Gauteng, South Africa. In gathering an understanding of this a qualitative study shall be done that will make use of a broad scope in terms of cyber-security threats as well as how sensitive and private information has to be protected in the business organisation. This information and knowledge gained can then be further used to build a framework that will help increase the level of information security awareness in these IT-dependant companies.

The study is limited in that it will only focus on gaining an in-depth understanding of how information security awareness is perceived in these small business organisations that rely on the use of information technology. Before any influences can be made to the object of study a clear and in-depth understanding has to be formed on the type of IT-dependant components the business organisation has as well as the potential threats these business processes face in the described world of information technology.

1.7 Problem Statement and Objective

Research Aim: The aim of this research study is to identify the level of information security awareness espoused in small information technology-dependant businesses around the Gauteng province of South Africa.

Research Objectives:

- Identify the information and cyber security awareness espoused regarding use of personal and sensitive information
- Identify how the use of information and technology forms part of a critical process in small organisations.
- Identify how personal and sensitive information collected by small organisations is stored and used.

Research Question:

What is the current information security awareness in small information technology-dependant business organisations in Gauteng, South Africa?

Secondary Research Questions:

a) What is the information and cyber security awareness exposure regarding use of personal and sensitive information in the small information technology-dependant business organisations in Gauteng, South Africa?

b) How does information technology form part of a critical process in small organisations?

c) What personal and sensitive information is collected, stored and used by small organisations?

1.8 Research Design

The study will be an empirical study in which primary data is to be gathered using a qualitative research approach following the interpretivism research philosophy. This will be clearly explained in Chapter 3 where the research methods are discussed.

Interpretivism is selected as a research philosophy due to its wide acceptance as a business research philosophy. It will be used to "*understand the behaviour*" of information security awareness as espoused by small businesses in Gauteng. By distinguishing between human subjects and computer related objects the use of information technology and information security awareness can be studied (Saunders, *et al*., 2009:116). Interpretivism will help explain information security awareness as a social phenomenon, which can then be used to further develop the framework using a "subjective interpretation" by seeing the culture of the organisation as a "variable" following an inductive approach (Blumberg, *et al*., 2008:21 & Saunders, *et al*., 2009:111). In Chapter 3 of this study the philosophical theory of interpretivism and subjective interpretation will be elaborated upon and described in more detail. Support for the research methods selected for the study will also be given.

Gauteng is specifically selected owing to its high representativeness of population, housing approximately "22.39% or 11 328 203 people" of the South African population (SouthAfrica.info, 2011). It has been mentioned earlier in the chapter that the unemployment rate in the Gauteng province was measured in the 2011 census to be 26.3%. The province of Gauteng has "three metropolitan municipalities, namely: City of Johannesburg, City of Tshwane and Ekurhuleni Metro, as well as two district municipalities, namely: Sedibeng and the West Rand" (Government Communication and Information System, 2012). The census survey delivered the following unemployment statistics for each of the local municipalities:

Municipality	**Unemployment Rate 2011 census report Gauteng, South Africa**
Sedibeng	32% Unemployed
West Ra**nd**	26.7 Unemployed
Ekurhuleni Metro	28.8% Unemployed
City of Johannesburg	24.7 Unemployed
City of Tshwane	24.2 Unemployed

(Table 1 - Stats SA, 2012)

Calculating the number of small businesses by definition in Gauteng is extremely difficult, as, according to the National Small Business Act of 1996, not all small businesses have to be formally registered. During a small business survey of Gauteng in 2006, the "population for small business owners or people involved in small businesses was estimated to be 1 053 818 individuals" (FinScope, 2006:20). This is an extremely large number and is reduced into the following population that will be used for the study: From the survey 64% of the population where deemed to be from the "infomal" business sector, "18% unregistered indivuduals operating businesses" and "17% or 184 992" people owners of very small and small registered business organisations as per definition in section 1 (FinScope, 2006:20). The selected population of small business owners in Gauteng will thus be based on the number of 184 992 registered owners from which a sample size of 25 shall be drawn. The sample drawn from this population will be done by making use of the 'purposive sampling' technique that will be fully discussed in Chapter 3 of the research.

A mono method research approach was used in the study to help solve the set objectives and overall research aim. A qualitative research approach is adopted to better explain and understand the concept of information security awareness within a small South African business context (Migiro & Magangi, 2011). The study was an exploratory study that made use of semi-structured interviews from a qualitative perspective to understand and explain how information security and awareness is perceived in small business organisations of Gauteng (Blumberg, *et al.*, 2008:201). The use of most methods in the study are not standardised because of the lack of research on the small-business environment of Gauteng and information security awareness.

This study is largely motivated by the previously discussed impact that the small-business community has in South Africa along with the increased use of technology within these businesses. These can be from operational use through to management and even strategic planning. Further motivation for the study is the "lack" of research that has been done on the small-business community of South Africa, including its use of technology (Mbonyane & Ladzani, 2011).

Chapter 2

`

This chapter takes a holistic look at the supporting literature for the introduction of the small business organisations of Gauteng and the information security awareness of these business organisations. Chapter 1 introduced these concepts along with how the use of information technology in the daily operations of small business organisations in Gauteng can be affected. In Chapter 2 an in-depth discussion with supporting literature will be made to understand the research problem that is presented.

Chapter 2

Literature Review

2.1 Introduction

Chapter 1 describes the small business environment of Gauteng and South Africa as well as the daily challenges they face. These challenges include the tough economic environment, the shortage of skills and the problem of information security and cyber threats. Chapter 2 will explore these areas in detail to form a clear picture of the current small-business environment. This will be done in such a manner to support the research question and objectives set out at the end of Chapter 1.

2.1 Cybersecurity and Information Security

Chapter 1 explained the security problems and concerns that can influence information and technology in the business. The following sections will describe what cybersecurity is and how it influences the use of information technology. This will be followed by a discussion of information security and how it is different from cybersecurity. The purpose of the discussion in this section, section 2.1, is to describe the relationship between these two concepts so that further discussions can be clear and placed within the correct context.

Cybercrimes can be defined as “any illegal activities” that take place through the use of “internet components”, such as the abuse of personal information, and which have to be carefully managed owing to their unique nature and continually growing risk (Salifu, 2008:433). Mainelli describes cybercrimes by “contrasting [them] to normal crimes from an insurance viewpoint” and concludes that it cannot be seen as a “normal crime” as businesses cannot always buy securities such as “burglary or fire cover”, making it a whole new and complex business risk (Mainelli, 2013).

From the two definitions it can be seen that cybercrimes can involve illegal activities, but these are not always as simply defined as ordinary crimes owing to their complex nature and difficulty in understanding. It can also be said that cybercrimes are not only caused by the use of information technology but also through a number of other factors. Using the two definitions discussed above, the reality of crime in the cyber world can be analysed to determine its impact on society.

Crime that takes place in the cyber world is nothing new and can affect anyone who makes use of information technology. Implications can also indirectly affect people through the means of services and consumable products that make use of information technology components. Without making direct use of information technology, people can still become victims of cybercrimes and other cybersecurity threats. Possibilities such as identity theft that can happen when personal information is provided to a third-party, who then misuses this information through the use of information and communication technologies.

Cybercrimes are mainly the result of the actions of cybercriminals who have the specific intent of finding “vulnerabilities and shortages” within an organisations information systems and by doing so, exploiting the system and services offered by the company (Bhattacharya, 2011:300). These crimes are not only aimed at businesses but can also affect home and indirect-users, as previously stated.

Cybercrimes are described as a modern problem where actions are taken mostly from a “reactive” approach against threats rather than a “proactive” approach (Broadhurst, 2006:3). This provides reason for concern and creates a need for protection against the cyber threats that exist. Section 2.2 will focus on the impact that cyber and information security threats have on small business organisations, however, this section will continue with a discussion that will help support the above statements made about cyber threats and their influence on society.

It has been mentioned that owing to the existence and rapid increase of cyber security, a number of risks exist. One of these risks is that of information security. The ISO27002 defines information as an “asset that can be used by businesses” to form part of the business and is sometimes considered as a critical business process (ISO/IEC 27002:2005, 2005). This has been mentioned in Chapter 1 as to where and how information can play a role in the day-to-day activities of a business. The ISO27002 report further defines information security as the “protection of information by means of various methods that will help build business continuity, minimise risk and grow the return on investment (ROI) and future prosperity (ISO/IEC 27002:2005, 2005).

2.2 Small businesses and Cybersecurity

Cybercrimes have a greater impact on developing countries, which is commonly seen as the result of a lack of "law enforcement and expertise" (Salifu, 2008:440). In Chapter 1 this influence of small businesses and cybersecurity was stated when unpacking the research problem, which was supported by the literature and literature findings from Chapter 2.

An environment that provides opportunity for the threat of cybercrimes to take place and which does not have sufficient protection is good cause for a research study to be made. Along with the threats that exists within the cyber world comes the challenge of keeping information secure. Information security is affected by the security of information technology and should be treated in a common manner, as explained in section 2.1.

Furnell, Gennatou & Dowland (2002:352) emphasise that **information security** is "critical" to "organisations that [have] a technology dependency" and conclude that there is a current "lack in small business organisations". This is a global problem that also affects the small business community of Gauteng and South Africa, as mentioned in Chapter 1. Information security concerns affect organisations that make use of information technology and information systems in a direct or indirect manner.

Security and security awareness is mainly derived from the need for protection against cybercrimes. This includes the protection of information and technology that is used in the business organisations. Throughout the business environment numerous tools, techniques, standards, methodologies and best-practices exist that can be used to combat the risk of cybercrimes. These tools are tailored according to the intended business environment, though are mostly intended for large-size organisations. Focusing on the small-business sector, including that of Gauteng, one has to carefully consider which approach to follow that will deliver the most secure environment possible for the specific IT-dependant organisations.

The types of cyber security measures that can be followed by small business organisations include using a personal and work-related computer that uses commercial products like "antivirus or firewall software" without having any specific knowledge of the possible cyber threats that exist, to employ someone that has a "professional knowledge on cyber security" or, finally, to "outsource all of their security needs" (Bhattacharya, 2011:302). For the purposes of this study it will be assumed that most small information technology-dependant businesses of Gauteng make use of a blind approach to combat cyber threats or have no countermeasures in place. Although the assumption is not scientifically sound, it can still be used to guide the design of measuring instruments. This is, however, supported by the literature and discussions thus far from Chapter 1 and 2.

2.3 Personal and sensitive information in the business organisation

Personal and sensitive information, as defined in the introduction, can include anything from identity numbers, addresses, medical records, patents/formulas and protected financials. The Protection of Personal Information Act defines "personal information as information relating to a living natural person" and can include information relating to "race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, health, disability, beliefs and culture" (Protection of Personal Information Act, 2013). Chapter 1 explained how the Protection of Personal Information (POPI) Act defines personal information and how it affects the use of information in business organisations. A further link was drawn between the use of personal information in the business and how it is supported by information security awareness.

The POPI Act defines what personal information can include and how it relates to a person or legal use of such personal information in business, including small business organisations. The use of information and technology in small business organisations have been defined and included in the research objectives in Chapter 1. It further includes use of information as part of the research question looking at the information security awareness in the small business organisations of Gauteng, South Africa.

2.4 Small businesses and Information Security

Cybersecurity has many aspects including the management of information security as well as the awareness level regarding the safe use of personal information. Privacy is a security concern, making it important to ensure that information is kept secure in the organisation. Chapter 1 describes how important the management and awareness of information security is to any business, including the small business organisations in Gauteng, South Africa.

It has also been explained in section 2.2 and 2.4 how important it is for organisations to keep their information and communication systems secure. Information security management and information security awareness are two critical components of cybersecurity and the governance of information and communications usage in the business environment. **Information security management** is differentiated among the "prevention paradigm", which focuses on preventing past security threats, and the "response paradigm", which looks at preventing future threats, including those that have not yet been identified (Baskerville, Spagnoletti & Kim, 2012).

Information security management forms part of the bigger picture of IT Governance, which also forms part of corporate governance and is noted to be mostly absent or incomplete in small and informal businesses (Coertze, van Niekerk, von Solms , 2011:1). Coertze et al. (2011:2) further highlights that information security not only exists within the body of IT Governance but can also be found elsewhere within the bigger corporate governance framework, including legal and social responsibilities. The lack of information security governance in small business organisations supports the research problem, which is to investigate the awareness of protecting information in the small business organisations of Gauteng.

The 2012 “Kaspersky Lab Global IT Security Risks Report” highlights that two of the biggest “concerns IT Professionals” in business have is “IT Security and […] data security” (Kaspersky Lab, 2012). This survey was mostly concerned with larger business organisations but its findings cannot be excluded from the operations of small business organisations. Part of the research question specifically states that the subject of study is small IT-business organisations in Gauteng. Although the population is somewhat different, the research objective of the above mentioned study closely relates to the research question in this study. This close relationship, and the obvious use of technology as part of the business in its everyday processes or any other manner in which technology affects the business, should be considered when planning and executing the research. This will provide support that the results from the study’s report can be applied when preparing the research tools and collecting the empirical evidence.

When similar reports that have common populations or similar research objectives are studied, further observations on the current research and real-world trends can be observed. For example, in a global study conducted in 2012 specifically focussing on small business organisations, the following 5 overall findings were found to be a business risk:

a) Lack of employee knowledge
b) Lack of protection
c) Growth in the use of mobile products
d) Data not being “backed-up”
e) Lack of “security policies”
(Trend Micro, 2012)

The stated focus of the study as described will be to measure information security awareness in the small information technology-dependant business organisations of Gauteng. It has been further said the results as well as the procedures followed by other business organisations should be consulted as guidance and then used to support the research results. Before this research problem can be further unpacked, 'awareness' and the contextual meaning of 'awareness' has to be defined and explained.

2.5 Awareness as a social phenomena

From the discussion in the previous section, as well as in Chapter 1, it was suggested that the 'awareness' of small businesses in Gauteng has to be studied. Awareness was specifically defined in the context of information security awareness that exists in the particular small IT using business organisations. It is necessary to clearly distinguish between the different security, information and awareness concepts to ensure that they are fully understood and placed within the correct context of the research study.

The first approach will define 'awareness' from a social study perspective to understand where this phenomenon fits within society. By defining awareness it can more easily be placed into context for the purpose of this study, which will benefit both the researcher and reader. The discussion will be expanded towards what 'information security' is and how this social occurrence is applied to information and communication technologies. As information security awareness is defined, it has to be compared to cyber and IT-security as a research object to highlight similarities as well as key differences.

Once the discussion of awareness, information security awareness and the comparison with IT-Security has been completed, its relevance can be discussed in terms of how it fits in with the purpose and specific research question of the study. This discussion will help put the explained concepts in to context by highlighting how it forms part of the study and its purpose.

As has already been stated, 'awareness' firstly has to be defined and placed into context before it can be mapped into information security and the intended research study. According to the Oxford Dictionary, the word 'awareness' means to have some form of "knowledge or perception over a situation or fact" (Oxford Dictionaries, n.d.). This definition shows how awareness is not always factual and correct but can also be viewed according to a person's own perception or understanding. This has been previously mentioned and is partly responsible for the need to understand the awareness of small technology businesses, which forms part of the solutions towards understanding the research question.

This definition is supported by numerous other similar describing definitions comparing it to a "psychological state of consciousness" regardless of being factually correct or not (Arp, 2007:101-102). This being said, it is clear that awareness is a psychological state in which a purposeful decision has to be made by reffering to past experiences, knowledge or perception. Once the term awareness is understood, it can be correlated with the meaning of information security awareness and how it is in line with the above descriptions of 'awareness' and its applicability. These definitions are not specific to a certain environment, landscape or audience, making it important to look at how the term is placed into the relevant study context, as has been mentioned.

2.6 Awareness and the different types of knowledge

Awareness has been described in different ways that include understandings that do not always see awareness in terms of facts, but also in terms of "assumption or perception" that forms part of the "tacit knowledge" that is owned by the "people" in the organisation (Smith, 2001:314). Tacit knowledge is mostly controlled by the employees within an organisation and is often lost when people leave the business. It is important to make a clear distinction between tacit knowledge and explict knowledge and to place it into the context of a small IT-business of Gauteng. Tacit knowledge will "remain tacit knowledge" as long as it stays in the individuals "mind" and does not get captured in some manner (Alony, Whymark & Jones, 2007:55). Tacit knowledge is thus closely related to awareness and the discussion made on how 'awareness' can be interpreted.

"Explicit knowledge" is defined as knowledge that has been obtained by the employees of an organisation "through education or structured" study and which is of "high quality" (Smith, 2001:315). Explicit knowledge also forms part of awareness and is more closely related to the definitions of awareness as having 'factual and correct' knowledge. Chapter 1 described how the small-business environment of Gauteng is structured and also looked at the lack of education and formal business practices in the region. From the explanations above, it can be said that the assumed knowledge in small information technology businesses would mostly be tacit knowledge. Literature supports the understanding that that tacit knowledge is "taught and shared" by people, including employees in the organisation, through "stories, work discussions" and other ways of interacting (Smith, 2001:317).

2.7 Information Security Awareness

Information security *awareness* differs from information security *management* as it describes a condition where all stakeholders in the business know the importance of information security as well as the role they play in ensuring that personal information is kept safe (Boucher & Flowerday, 2011:2). The Management of information security has been described as a formal process that is adopted by the organisation and where all the stakeholders are actively involved. Information security awareness, on the other hand, was described as something different but placed into the same context of a business organisation. The clear explanation and distinction between the two concepts helps to highlight the purpose and goal of the set research question and objectives. By distinguishing between what management and awareness of cyber and information security awareness is, it will be easier to apply the intended research approaches.

Being 'aware' can be influenced by the business organisation through a number of management techniques. Information security management in business organisations has been highlighted in section 2.1 and 2.2 by making use of various examples. These include the formal processes that can be implemented by business organisations as well as the governing bodies in place. However, referring back to the definitions of awareness and information security awareness, it can be concluded that awareness does not necessarily have to come from formal management initiatives, such as educational sessions, but can be transferred in a tacit form through stories, experiences and other methods of informal communication.

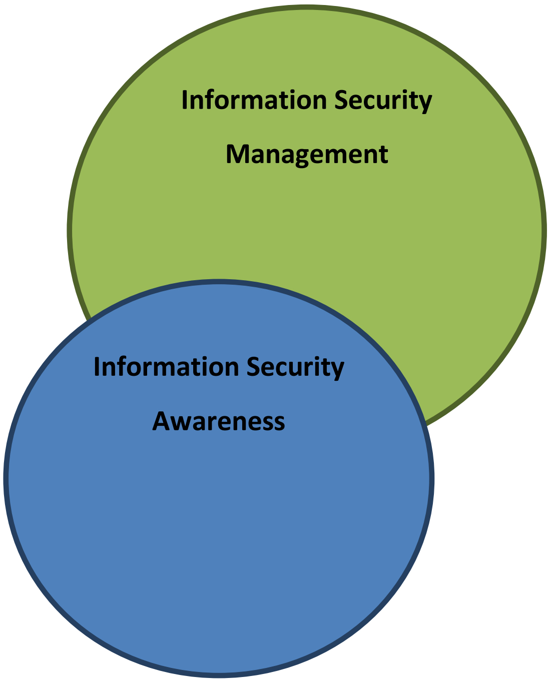

Information Security Management
Information Security Awareness

Figure 1: Information Security Mapping

One can see from the highlighted definitions and explanations that there are key differences between Information security awareness and information security management. It has also been mentioned that although there are clear differences between the two concepts, they can also be related to one another. For the scope and purpose of the study it has further been highlighted that the interest of the study lies in awareness in small IT-businesses, rather than in the management of information security awareness.

Figure 1 illustrates how these two concepts affect one another but also indicates how they can be independently studied within an organisations environment. The management of information security, thus, cannot be disregarded, but a greater focus can be placed on how 'awareness' exists in the business organisation. The illustration of information security and information security awareness in Figure 1 is not proportionally displayed. Referring to the definitions and studied literature, it is difficult to identify whether the management or awareness of information security is larger, smaller or consistently the same within business organisations. This is owed to the different sizes, cultures and other demographics found in different business organisations.

Figure 1 illustrates the researcher's views of how Information Security Awareness and Information Security Management relate to one another and how it was studied within the context of the identified research problem.

To conclude the above discussion, it is difficult and nearly impossible to generalise on the occurrence of information security management or awareness in all business organisations. This is why the research question needs to be carefully followed according to the selected population towards which the research is aimed. The beginning of Chapter 2 describes Gauteng as one of the economic hubs of South Africa with large and diverse small business organisations. This will make it easier to apply the research findings to the rest of South Africa, which will be done in the analysis (Chapter 5) chapter of the research study.

The chosen object of study, namely the small IT-dependant businesses in Gauteng, will make it easier to narrow down and study information, security and awareness in business organisations. As mentioned, Figure 1 does not illustrate the size or relevance of the awareness or management that takes place in the business organisation, but rather the relationship between the two. Literature has suggested that the management of information security is lacking in small businesses, however, until the empirical evidence has been gathered and analysed it will be impossible to assume any facts or make suggestions.

2.8 Information Security Awareness as part of the everyday business operations

"Security Awareness programs in general give users the knowledge to identify security problems" and to act accordingly in order to prevent security threats (Chen, Medlin & Shaw, 2008). This suggests that security awareness includes the obtainment of knowledge that will help people identify possible security concerns as well as the use of the right tools to prevent these security threats. In this case the 'right tools' can refer to the explanation of information security awareness and to having the correct knowledge, perceptions and other previously mentioned characteristics to be able to act appropriately against the highlighted areas. The second observation to make is that the process of transferring knowledge, which results in learning, is referred to as awareness, and in particular security awareness. This part of the definition speaks to the way in which the awareness levels are created: through the transfer of knowledge by teaching and learning in the business organisation.

2.9 The need for Information Security Awareness in business organisations

There are also criticisms in research around the current ways and methods of creating information security awareness in business organisations. One of these describes the current methods for creating information security awareness in businesses as old and outdated by comparing it to general "public security" (Stewart & Lacey, 2012:30). Traditional methods like these have been studied in the past by the researcher includes 'scare' techniques such as signs that make users aware of the risks involving the use of technology. This situation is often the result of the organisation itself not knowing what the current awareness levels are or how to use the correct methods of educating its employees.

Organisations sometimes know that there are security concerns around the use of information and technology, but do not "understand exactly what" these risks and concerns are (Furnell et al., 2002:352). This creates the problem that organisations, such as the small business organisations in Gauteng, do not know how to protect themselves or do not show any form of due diligence.

From the provided discussions it can be concluded that information security awareness includes the knowledge and type of knowledge as well as ability of the users to identify security threats and the necessarily skills needed to act accordingly in preventing these security threats.

The above statement is extremely broad and can be interpreted in several manners. This can be from the user identifying the actual threat and responding to the specific threat as compared to the user's ability to identify possible threats and to take possible precautions. This refers to section 2.1 & 2.2 where cyber security in the business environment is discussed. From this technical level a user may not always possess the skill to identify and combat the specific IT threats, but may at least have the knowledge available to know that harm can potentially be caused and that certain actions for protection have to be taken.

2.10 Information Security Awareness in small information technology-dependant business organisations of Gauteng

As described in Chapter 1 and in the research problem, the significance of the study resides within the increased use of information and communications technology (ICT) in small business organisations and the lack of information security awareness in the South African business environment. Information security awareness is seen as the knowledge that exists in the small businesses of Gauteng and also includes the IT-users' ability to show due diligence when working with information that has to be kept secured.

Knowledge and the two different forms of knowledge, 'tacit and explicit', have been defined and placed into context in section 2.2. When referring to information security awareness as the 'knowledge that exists within the business organisation, it is also important to determine what the knowledge type is as well as where it resides, before it can be measured. The measurement of the phenomena of information security awareness will be discussed further in Chapter 3: Research Methodology.

Information security awareness in small businesses, including those of South Africa, is just as important as in large enterprises because they make use of the same "markets" and take advantage of the same "benefits" that come from the use of information technology (Upfold & Sewry, 2005). This is just one of the reasons for the importance of information security awareness in small business organisation and why it is not only important to large organisations.

2.11 How is information security awareness created in the small IT-dependant business organisations?

The research question has to be answered by gathering evidence to determine what types of cyber and, specifically, information security awareness knowledge exists in the small technology-dependant businesses of Gauteng. Empirical evidence is also needed to help understand how the selected population of businesses perceive and approach the highlighted cyber and information security threats and concerns. The following section will be used to explain the understanding of information security awareness and how it forms part of awareness as a psychological and technological concept.

From this high-level approach, Chapter 3 will present a clear conceptual approach as to how the research question will be answered. Before the research question can be answered or evidence collected, it is important to understand how information security exists in the business organisation. It is also important to understand where it exists and how it is transferred, as is mentioned in section 2.6 on the various knowledge types. The creation and transfer of information security awareness will help one to understand the research problem and research questions.

One of the approaches towards creating information security awareness in small businesses is to help the business and its employees "understand" the risks involved and by doing so creating better awareness, as opposed to the usual risk awareness method (Stephanou & Dagada, 2008). This method, as Stephanou and Dagada (2008) show, explains that through the process of learning the business one can come to know how the threat works and can how it can negatively affect the business. Organisational learning has always formed part of maturity developments and conforms to what was described about where and what awareness exists in small business organisations.

Referring to the users level of 'awareness' should thus also include the users understanding of what the information security risk is and their ability to take appropriate action to minimise the risk. Being aware is only one part of the awareness component and can also be to understand the related risks. As part of the research tools that will be formulated, the level of understanding regarding information security awareness should also be observed and documented.

In another study done on small business organisations that have technology dependencies, it was observed that a good method for creating awareness was through "an environment where mistakes can be made and lessons learned", without leaving the organisation with serious reputational or financial damage (Furnell et al., 2002:354). Methods such as these should be considered when the study is conducted and an understanding has to be gained around the information security awareness in the small IT-dependant business organisations of Gauteng.

Further studies on the small business environment of South Africa indicated the lack of formal information security and awareness "frameworks" as well as how "sensitive information" is persistently used without the necessary protection (Upfold & Sewry, 2005).

2.12 Legal implications for the business: Information Security

Section 2.3 described the Protection of Personal Information Act and how it affects the business organisations in Gauteng and South Africa. It was further mentioned how this act affects the small business organisations and the way they use information on a daily basis.

Now that information security awareness and the implicating business risks have been discussed, the legal implications need to be defined. These legal implications are specifically those that can affect the small business organisations of Gauteng and South Africa. These implications will have a great impact on the study and when writing up findings for the small technology dependant businesses and information security awareness. The legal implications, no matter how significant, will have an impact on the population and should thus be included as part of the study.

Not only do policies to protect personal and sensitive information exist in organisations, but also as part of the law of countries such as South Africa. These national and international laws are set in place as protection mechanisms against the cyber and privacy threats mentioned in Chapter 1.

Information security and the protection of personal information are becoming more of a concern in South Africa and are currently forming part of the national agenda. This is mainly because of privacy concerns and the mandate for information security to adhere to these privacy concerns. In March 2009, government proposed a controversial "Protection of Personal Information Bill (POPI)" with the aim of protecting personal information of South Africans (Protection of Personal Information Bill, 2009). Although sometimes criticized by the public and the media, the bill aims at ensuring the protection of personal information as well as the establishment of "protection principals" through the implementation of an "Information Protection Regulator" (Protection of Personal Information Bill, 2009).

On 26 November 2013, the Protection of Personal Information bill became an act after being signed by the president, giving business organisations "a one year compliance period" (KPMG South Africa, 2013). The purpose of the POPI Act is to support the "constitution of 1996 regarding the right to privacy" through a number of actions: protecting personal information, regulating the processing of personal information by establishing an information regulator and introducing rights towards the protection of personal information" (Protection of Personal Information Act, 2013:16).

The definition of personal and sensitive information was given in section 2.3 of this dissertation, where the POPI Act was introduced. The understanding of personal and sensitive information was also given with relation to information security awareness that forms part of the research study. It was also mentioned that business organisations have a "one year grace period to comply with the act" (KPMG South Africa, 2013).

An alternative approach that has seen less resistance is the acceptance of a "National Cyber Security Policy Framework" in March 2012 that is intended to help assist national security against "cybercrimes" through the 'alignment of existing laws', which will ultimately create a safe ICT-environment in South Africa (Department of State Security, 2012). Although cabinet has already accepted the cyber security policy framework for South Africa, no further action has been taken to mature the defined purpose of this law to protect South African consumers from cyber risks.

The enforcement of the abovementioned also impacts the small business community of Gauteng, South Africa. Compliance towards the mentioned acts should be included in the research objective of identifying the information security awareness in the small business organisations of Gauteng.

Information security awareness has been defined and set in the context of the operating small business environment in Gauteng. It is important to look at the different models, frameworks and governing bodies that can assist with the information security awareness in the small business organisations. The investigation of these tools will form part of the evidence to answer the research question and achieve the set research objectives.

2.13 Governing bodies and best practises

The first tool to assist with the promotion and measurement of information security awareness in the small business organisations of Gauteng and South Africa is the governing bodies or best practices that exist.

Cobit 4, a best practice document on IT governance suggests in its "DS7 Control Objective" that all stakeholders in the organisation who make use of IT within the organisation "should be effectively educated" and also specifically refers to security concerns in the organisation (Cobit 4.0, 2006). In the updated version, Cobit 5, a new section namely "Manage Security" has been added to the "Align, Plan & Organise Process", which specifically refers to information security on a management level, indicating the importance of this concern to any business that has to manage their IT components according to a governing framework (ISACA - Cobit 5, 2012).

Although formal governance or management practices are not always applied in small business organisations, the risks and concerns highlighted in these governing bodies can still affect the company. This also does not cancel out the need for security measurements and mitigation capabilities as indicated in Chapter 1 and 2. Cobit 5’s “[d]efining and managing of the companies information security risk treatment plan (APO13.02)” specifically indicates that there should be “training and awareness programmes” in place in the organisation (ISACA - Cobit 5, 2012). The suggestions made in this governing framework can be tailored and applied to almost any business organisation, indicating the possibility of the risks raised in the document on businesses, which will include the small IT-dependant business organisations of Gauteng.

It has been mentioned that governance frameworks can be used in organisations for managing and controlling, realising benefits and managing risks. Part of the governing and risk management objectives of the framework should be focused on the local laws and best practices that are used in operating the market of the organisation. Such laws will be specific to which types of business organisations are affected as well as what is expected from the particular organisation in terms of legal compliance.

In a study focusing on some of the “Information and Communications Technology challenges that are faced in Africa today,” it was suggested that if the development of IT wants to be used as a tool to create jobs, the correct “national priorities and policies should be in place (Edoho, n.d.). The following section will describe some of the local initiatives, laws and practices set to protect South Africans and South African businesses from the cyber and information security risks that exist. This will include the protection of personal and sensitive information that is used in the business organisations. The applicability of these influencing mechanisms will also be described for the small business organisations of Gauteng.

2.14 Frameworks for creating information security awareness in small information technology-dependent business organisations

In this section some of the methods that can be used to create information security awareness will be explained. This will help support the definitions of information security awareness and how it occurs in the business environment. There are several options available when cyber and information security awareness wants to be created in small business organisations. Methods selected are the most appropriate for use in the small business organisations of Gauteng according to the studied literature thus far. It is therefore important to ensure the correct techniques are studied in line with the population of the research and that will help achieve the research objectives.

It has been mentioned that there are various methods that can be used to create information security awareness in the work environment. It has also been explained that there is a need for cybersecurity in any organisation that makes use of information technology. As suggested in the introduction, a tool specifically designed for the South African small business environment is needed to increase and measure awareness concerning the use and protection of sensitive and personal information. By investigating some of the current tools used to increase awareness and applying them to local awareness initiatives, businesses will be able to increase their awareness level of information security among their employees and other stakeholders.

Information security awareness in the organisation can be applied using various methods and can also be classified in very different ways. Security awareness can be applied to the organisation on an "individual level" or on a group level, each using distinct techniques that can include "presentations, e-mail, posters and individual [and] group activities" (Albrechtsen & Hovden, 2010).

Siponen describes information security awareness among people as being influenced through two categories, namely the "framework" category and the "content" category. The "framework category" focuses on scientific methods that should be "quantitatively" analysed whereas the "content category" is focused on a less-scientific approach and should be "qualitatively" analysed (Siponen, 2000). For the scope and purpose of this study a qualitative research approach was selected as explained in Chapter 1, section 1.9: research design. Chapter 3 will elaborate on how a qualitative conceptual approach will be followed for gathering and interpreting evidence.

A basic "Information Security Awareness Program" is described to have "four stages namely the identification of the security awareness need, selecting the key topics to cover", assigning ownership and executing the program (Tsohou, Kokolakis & Karyda, 2008:280). This traditional approach is easy to implement but sometimes has little value to offer, especially if the audience is diverse. Through this, several local and tailored methods have been developed for businesses in South Africa. To study the information security awareness in these small business organisations it is important to understand the source of information security awareness and where it resides in the business and its employees.

Coertze et al., (2011:2) suggest that existing methods like the “Information Security Management Toolbox” can be adapted for an online environment and its scope broadened specifically for “managing information securely in small-to-medium-sized businesses of South Africa.” The “Information Security and Awareness Model (ISRA,)” was built as a tool to increase information security awareness and can be tailored to a *specific* industry where not only IT-related employees, but *all* stakeholders, are included in the awareness campaign (Kritzinger & Smith, 2009:521). From the ISRA model, Labuschagne and Eloff (2012) built a “Shared Public Security Awareness (SPSA) system” that can be applied to small business organisations with multiple users on a “shared computer”. This system is used to create awareness, assess the awareness level of the user as well as to provide the user with an Internet connection. The use of this model is aimed at the individuals who make use of the shared service and is suggested for organisations such as “internet cafes and schools” (Labuschagne & Eloff, 2012). The level of information security awareness is thus measured through a single domain that is used by multiple users in the business organisation.

These two models have tailored the science of increasing the information security awareness of the users in the particular small business organisations. The use of these two frameworks will also assist with the understanding of the information security awareness in the small business organisations of Gauteng.

Another model used to create awareness in the workplace is the “Informational Privacy Model” that is built on the popular “McCumber INFOSEC Model” (Boucher & Flowerday, 2011) and which focuses on four principals concerning the storage of personal information:

- Data owner’s responsibility
- Data ‘requestors’ responsibility
- Data handling ‘consistency’
- Legislation regarding the storage of personal information
  (Boucher & Flowerday, 2011).

These principles of the INFOSEC model are also in line with the requirements of the POPI act described in section 2.12. They clearly identify the legal impacts and the responsibilities of the business and individuals that make use of personal and sensitive information.

The INFOSEC model emphasises the importance of educating the user against the threats of abusing personal information and the 'Information Privacy Model' focuses on delivering the proposed education to the user. This model is used to create security and privacy awareness among the users of the information system including those in the small business organisations of Gauteng.

Tools like the ISRA model, Toolbox or Information Privacy Model can be used as part of the development of a framework that will help create information security awareness in the small business organisations of Gauteng. Another approach for creating awareness would be to focus on the user's attitude towards information security awareness. The classic "attitude system" includes the "intended behaviour of the user, the actual behaviour of the user, ideas and suggestions and the emotional response of the user" (Thomson & von Solms, 1998:169). This model suggests that the behaviour of individuals in the organisation can be influenced through "directly changing the individuals behaviour, influencing the individuals attitude once his/her behaviour has changed and, lastly, through persuasion", which is achieved through the use of various tools (Karyda, Kokolakis, Kiountouzis, & Tsohou, 2012).

The "Information Security Culture Framework (ISCF)" makes use of three "levels" through which the framework can be applied to the business and its "information security tools", namely the "organisational level, group level and individual level" (Veiga & Eloff, 2010). These are used to positively influence employees and to ultimately create an "Information Security Culture" (Veiga & Eloff, 2010). Information security awareness forms part of the organisational culture and the organisations information security strategy.

Another interpretation of information security awareness suggests that a "strong correlation" exists between the "Risk Assessment of Information Security Systems" and the following three areas: "Technical Knowledge of information security threats, impact of these threats on the organisation [and] the motive of an attacker" (Mejias, 2012). Meijas suggests that these three factors form the underlying principles of information security awareness in an organisation, which can then be used for assessing the related risks. The three principals are also applicable to small information technology-dependant business organisations in Gauteng. When the user of a system is aware of the types of IT and information security related threats that exist, as well as the potential impact of these threats on the organisation, the user of the system will have a better understanding of information security threats. The third factor that contributes to the user's knowledge of information security awareness is the understanding that the user has of a cyber attacker, which includes the motives of such an attacker. The final suggestion made is that the risk assessment of information security awareness can be done from the three mentioned areas that constitute what information security awareness is in the business organisation (Mejias, 2012).

The Microsoft Corporation suggests that a “public health model” can be used on devices connected to the internet, creating a “collective defence” protection against information security threats through the “identification of infected devices and by improving user awareness on the “health of the device” (Charney, 2010). The use of this model can thus be approached from a service providing side to monitor the user’s device and to create sufficient awareness for the user. “Health Certificates” are used as protection mechanisms in this model and serve as part of the user security awareness creation mechanism (Charney, 2010).

Although this model is intended for users in a closed network who are accessing the internet and not for small-business users, the awareness component of keeping the users informed on the ‘health’ of their systems can still be valuable. If users are actively informed on the condition of their system and the security around the sensitive information held, a more effective and secure environment can be created for the small IT-dependant business users of Gauteng.

Other techniques for learning and awareness measurement include tools that are specifically tailored for the particular business environment. Such tools can help business organisations “learn about security, test their understanding of security” and apply what they have learned to the everyday business environment when working with information and technology (Furnell et al., 2002:354).

Models and frameworks will be studied with the aim of finding the optimal tool for measuring the level of information security awareness in the small-business organisations of Gauteng. The findings can also then be used to build a new framework that can support the small-business environment of Gauteng and the rest of South Africa, so as to protect information in the organisations.

A recent study on the use of mobile banking in South Africa revealed that technologies with high perceived value may cause consumers to overlook the related “privacy and security concerns” (Njenga & Ndlovu, 2012), supporting the need for research into the use of ICT in the small business environment of Gauteng. The creation of an “information security culture as part of the business culture” is necessary for the small business environment of Gauteng, as it forms part of the awareness component that will help protect the business organisations against the mentioned risks (Okere, van Niekerk & Carroll, 2012).

From the above discussions it is clear that the best approaches have to be selected for assisting with the research and specifically with the awareness problems that need to be studied. It has been mentioned that a tailored approach has to be created that will support the research needs when applied to the small technology businesses in Gauteng.

2.15 Conceptual model for Information Security Awareness in Small information technology-dependant business organisations of Gauteng, South Africa

It is suggested that owing to the diverse learning culture in South Africa, a model or framework has to be specifically tailored and localised to fit and benefit the selected population. Cultural differences such as the "different mother tongue languages" can have an impact on information security awareness in business communities (Kruger, Flowerday, Drevin & Steyn, 2011). The need for an information security awareness conceptual model is important for the small-business environment of Gauteng. This need is explained in detail throughout Chapter 2 as the importance of information security awareness and how it affects the small businesses of Gauteng is highlighted.

One of the major contributing factors is that not all small business organisations are able to manage the information security threats that exist within and around their business. Additionally, many of the business organisations may not even be aware that these threats exist and can harmful effects on the business (Perks, 2010:221).

Information security awareness is also "argued to be part of organisational change" and it has to influence the "quality and state" of the organisations operations in terms of the previously discussed risks and concerns (Tsohou, Kokolakis & Karyda, 2008:272). This again emphasises that informtion security and awarenss is not a sole encapsulated concept and as explaind in the previous section, impacts on a number of other business activities. The severe risk that can affect critical business components and that may have legal impacts has also been highlighted.

2.16 Bounded Rationality

One tool that can be used to help the researcher understand where the stakeholders in small businesses have a lack of knowledge when it comes to cyber and information security awareness is the “psychological concept of bounded rationality” (Stewart & Lacey, 2012:30). Bounded rationality occurs when people want to make a decision “but cannot always do” so because of the lack of understanding and knowledge of their “internal and external environments” (Jones, 1999:298). As long as the reasoning behind bounded rationality is kept in mind, the researcher will be guided by not asking biased questions or by making biased decisions. This theory also supports the categories of tacit and explicit knowledge, which relates to the two different types of knowledge a person may posess and how the person uses it to make decisions.

In the approach of bounded rationality the researcher will be able to study the current information security awarness of the small businesses organisations. Steward and Lacey, 2012 describe “rationality as the best or value maximising choice users will make” when confronted with the risks of information security. The term is referred to as “bounded rationality” because the users are not fully aware of the risks and are only making decisions based on the best of their understanding and capabilities (Robbins, Judge, Odendaal & Roodt, 2009:124). As the literature has already helped the researcher understand that people do not make perfectly rational decisions because of their limited knowledge, it will be important to try and determine what actions and decisions they might take.

It is suggested that “conceptual frameworks” such as “bounded rationality” should be used when studying information security awareness in the small business organisations of Gauteng (Stewart & Lacey, 2012:37). As such, the use of frameworks will help to study and support the phenomena of information security awareness.

The theory of bounded rationality will be the first approach adopted in the interview sessions to help understand what the small business organisations know and understand around cyber and information security. Not only will the organisations’ knowledge of the specific threats that exist be understood, but also the understanding they have of the impact these risk can have on the business. As explained in the research objective, holistic information such as this can help with future research and implementations towards the cause of the research problem.

The theory of bounded rationality displays numerous characteristics that can help with the research problem. The theory explains how “users make decisions based on their existing beliefs, attitudes, limited knowledge, time, available resources as well as level of satisfaction” (Stewart & Lacey, 2012:33). Figure 2.1 illustrates how the theory of bounded rationality will be used in this research study.

In the formulation of the interview questions that will be described in the next chapter, the above-mentioned focus points will be used. Probing questions will be formulated in such a manner that will help understand the user's current beliefs around a certain subject as well as their attitude towards this identified point.

Chapter 3 will refer to the conceptual model and discuss how the view of bounded rationality can be incorporated into the design of the research instruments. Along with the theory of bounded rationality comes the theory of planned behaviour.

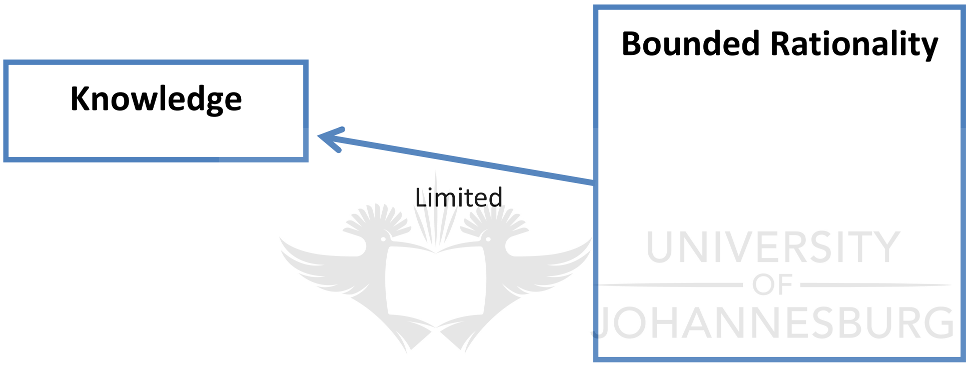


Figure 2.1: Bounded Rationality (Adapted and illustrated from figure 2.2 and 2.3)

2.17 Planned behaviour

The theory of planned behaviour from Icek Ajzen will be used to develop the research instrument along with the model that was used by Kruger and Kearney to measure information security awareness at a South African "university in the Eastern Cape" (Ngoqo & Flowerday, n.d. and Ajzen, 1991). In the theory, Kruger and Kearney suggest that awareness can be measured using "three dimensions which are scaled as follows: knowledge, attitude and behaviour" (Ngoqo & Flowerday, n.d.). The selected psychological theory is known as the "theory of planned behaviour", which determines the participants "behavioural *intentions or actual* behaviour" against the set topics and research problem (Ajzen, 1991:179). Kruger and Kearney link *actual behaviour* to the approach for measuring information security awareness in the organisation. Actual behaviour is what the author uses to describe awareness and as the approach for understanding awareness.

A number of researchers have used the approach of measuring information security awareness through knowledge, attitude and behaviour, as has been described in chapter 2 where some of the local and international approaches for measuring information security awareness have been mentioned. Authors adapt their research approaches to measuring information security awareness according to their research needs. Another "*five step ladder model* uses knowledge, attitude and behaviour and refers to it as the (KAB) model", which also includes the users "intention and belief" to measure information security behaviour (Khan, Alghathbar, Nabi & Khan, 2011: 10864).

Another author used the "knowledge, attitude and behaviour" model along with more specific organisational statistics to measure the information security awareness of an organisation (Mugo, 2012:55-56). By using more specific data from the organisation, the author was able to accurately determine the behaviour element on data such as "actual passwords used in the company and analytics on the security of the passwords, security incidents reported" and other security related information (Mugo, 2012: 56-57). By combining this actual behaviour with the research conducted, the awareness of the individual or organisation can be measured.

The following approach will be adhered to when formulating the questions per category, and keeping them in line with the selected mode and psychological theory: 'knowledge' will be tested by asking the participant a specific question; 'attitude' will be taken as the participants "thoughts" on the subject; while a behavioural response question will test the third "dimension" in measuring awareness (Ngoqo & Flowerday, n.d.). The selection and formulation of the questions according to the above mentioned model is supported with literature in the category selection of Chapter 2.

The scale suggested by Ngoqo and Flowerday of knowledge 30%, attitude 20% and behaviour 50% will not be used to quantify the qualitative results. The "theory of planned behaviour", which measures actual behaviour or awareness, will be used to categorise the intended questions and analyse the responses (Ajzen, 1991:179). Chapter 3 will illustrate how the research instruments were designed using the conceptual framework that includes the theory of planned behaviour that will help determine information security awareness or actual behaviour.

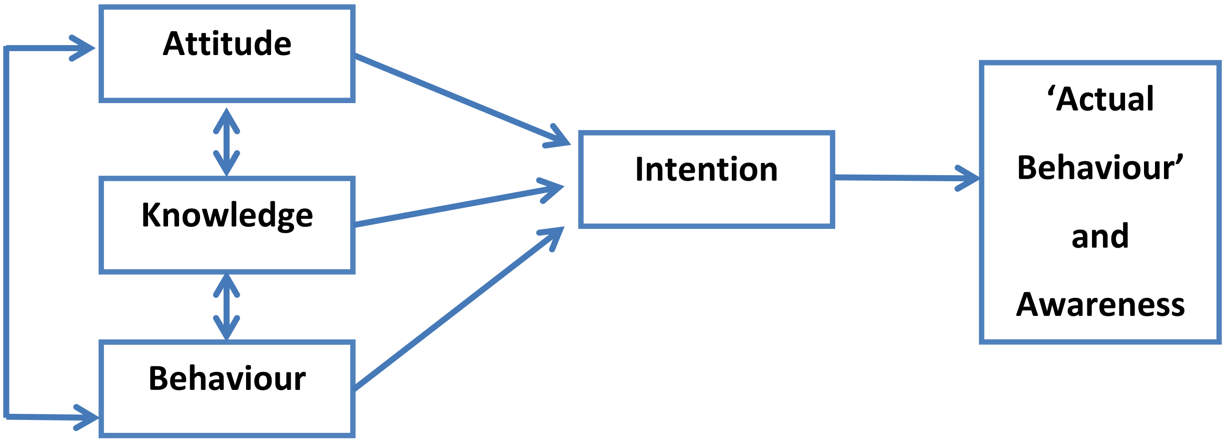
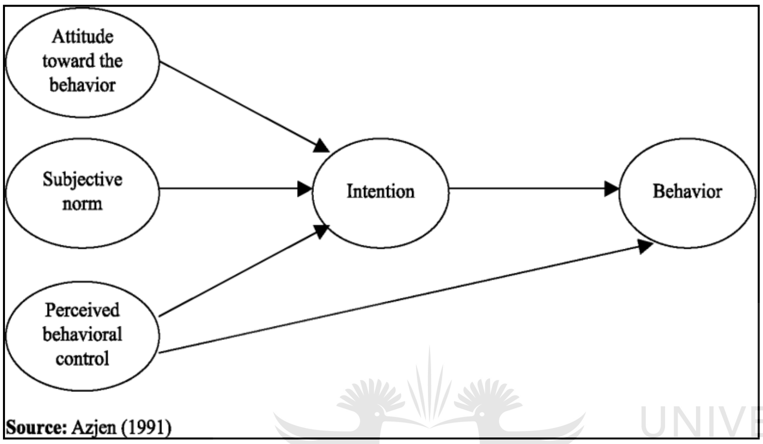


Figure 2.2: The Theory of Planned Behaviour (Adapted from Icek Ajzen, 1991)



Source: Azjen (1991)

Figure 2.3: The Theory of Planned Behaviour (Azjen, 1991)

Figure 2.2 and 2.3 shows how the theory of planned behaviour was studied and adapted by researchers to measure information security awareness. This model of the theory was originally designed by the developer of the theory, Icek Ajzen, and adapted to show how it will be used as part of the research. In Ajzen's original model of planned behaviour, knowledge is referred to as a "subjective norm" that describes how "a perceived perception is performed around the behaviour" (Ajzen, 1991:188). Researchers have elaborated upon this by referring to subjective norms as the '**knowledge'** a person has on which to apply this perceived perception. The three factors are further described by Ajzen to give way to 'intention', which equals 'actual behaviour' (figure 2.2 and 2.3). Actual behaviour has been used in the research discussed to understand the awareness of a person or organisation.

2.18 Self-categorising of elements

Planned behaviour and bounded rationality have been described as theories or viewpoints to support information security awareness and how it can be studied for the particular population of small businesses in Gauteng, South Africa. Along with these two theories, a number of factors have been identified to form part of information security awareness. It has been shown that information security, cybersecurity and the use of IT in businesses all form part of information security awareness. To study these factors that build towards information security awareness, 'self-categories' of elements have to be defined in the design of the research instrument. Key themes or topics in the literature, which will help to understand information security awareness in the small business organisations, have to be identified.

These key themes or topics will be used when designing the research instrument that will gather evidence on the information security awareness of these businesses. The need for self-categories of elements will be further explained in Chapter 3 where the research instruments are designated to help solve the research question and meet the research objectives.

2.19 Understanding the conceptual approach

To understand the business problems described above, the conceptual model can be followed, which will help in solving the problem. Semantics should always be used when discussing/describing occurrences, especially if deemed important to the relevance of this study. "Semantics" is used in the "adjectival" form to give "meaning" to terminologies and is commonly defined as the "study of meaning" (Dictionary.com Unabridged, 2009). The conceptual model is applied to give outcome to a "conscious/unconscious understanding through definitions", as well as the necessary semantics that will give meaning to the underlying problems (Duan & Cruz, 2011).

In simpler terms, the "conceptual model" can be seen as a "high-level description" of a system and how it functions" (Johnson & Henderson, 2002:26). This refers back to the proposed research question and what it means to gain a better understanding of the small business environment in Gauteng. A better understanding, in particular, is the use of information technology and the level of user awareness in the business when it comes to the use of information.

The conceptual model has many definitions and viewpoints and should be interpreted in a different manner for every situation. The viewpoint of a conceptual model through the representation of the intended measurements of this study will also be different from any other study. This makes the understanding of the conceptual model through the set research questions an important part of the research objectives and research findings.

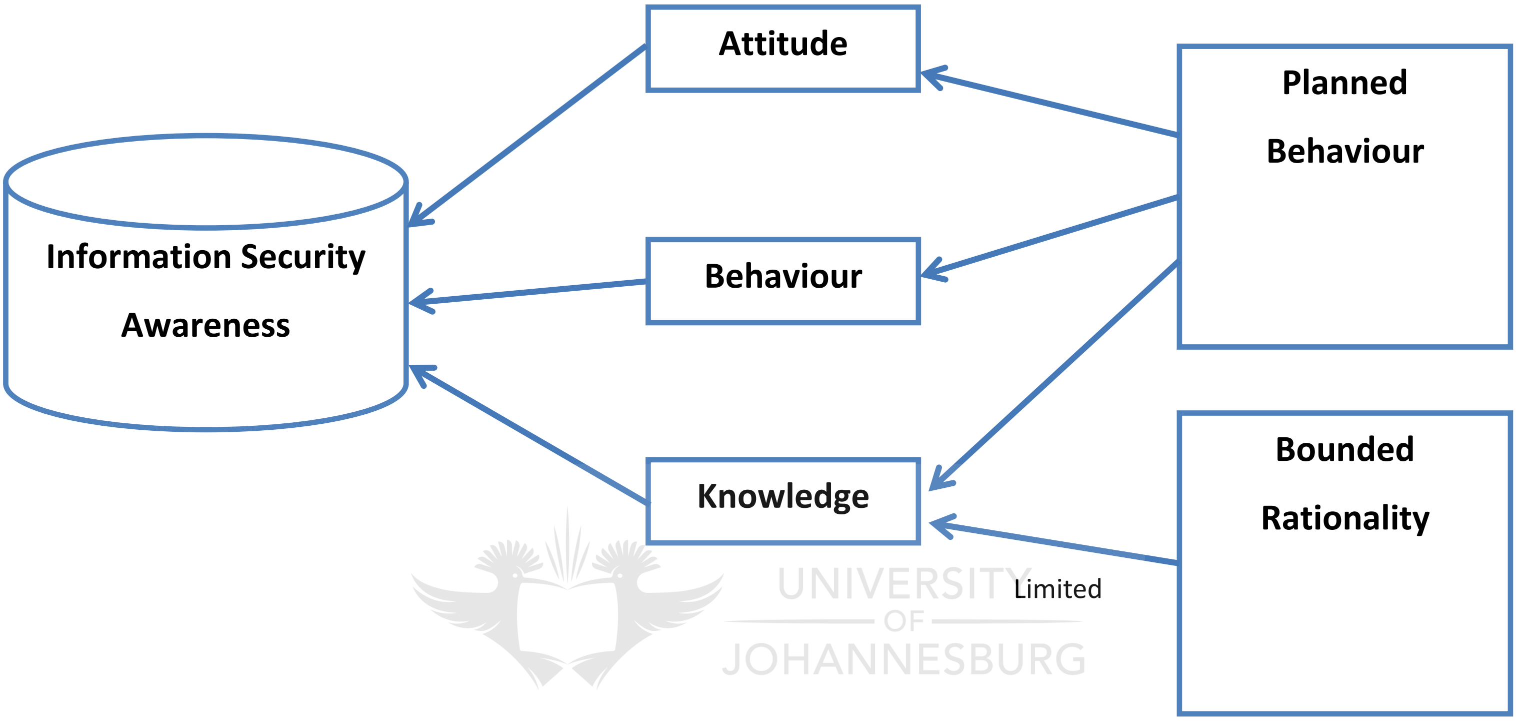


Figure 2.4 Conceptual Model: Information Security Awareness in small business organisations

Figure 2.4 illustrates the conceptual approach and tools that have been highlighted in Chapter 2, which will assist with the measurement of information security awareness in the small business organisations of Gauteng. Section 2.19 defined how a conceptual viewpoint can be followed for the purpose of this study and how it will assist in answering the research question.

Through the guiding concepts of planned behaviour and bounded rationality, the knowledge, attitude and behaviour of the small business organisations can be understood. These viewpoints will help in understanding the awareness of the self-categories that will ultimately build an understanding of the information security awareness of the participants.

The research and design of the research instruments will be guided by the conceptual model and referred to often as guidance for the understanding of information security awareness. The conceptual model will also assist with the interpretation of the research results and findings in the chapters to follow.

The need to understand information security awareness in the business environment has now been explained along with the importance and significance of the impact it can have on business organisations. Before the research methods and tools can be defined in Chapter 3, the conceptual model has to be logically applied to the understanding of the research question and what is expected from the research. Chapter 3 will explain how the above conceptual viewpoint should be followed as a research methodology.

Chapter 3

An in-depth understanding of the proposed research topic was made in the previous chapter giving a good understanding of the research problem and research objectives that have to be achieved. In describing the gap in knowledge that has to be understood, a picture was formed of what needs to be studied to help solve this problem. The current chapter will give meaning to how this research problem is to be studied using a formal research approach. The conceptual model defined at the end of Chapter 2 helps to guide the reasoning behind the need for Chapter 3 as part of the research problem.

Chapter 3

Methodology

3.1 Introduction

Chapter 3 is dedicated towards explaining how the study is to be executed and how the data will be collected. It will start by explaining the philosophical views that will be followed when selecting an appropriate research approach. A qualitative research approach was mentioned in the previous two chapters along with motivations for following this research route. This was also explained through a conceptual model in Chapter 2, section 2.19, where the understanding of the research problem was unpacked.

3.2 Research Philosophy: Phenomenology

After the research philosophies, qualitative research shall again be described in detail to explain the relevance and the context to the research problems. The qualitative research approach then has to be analysed according to the selected methodologies and tools.

The second part of the chapter will discuss the analytical approaches taken, which will then, together with the evidence that is gathered, help support and answer the research problem. As previously mentioned, a qualitative analysis approach has to be taken, which is most sufficient for the selected gathering tools.

Soshana Zuboff wrote a book titled: "In the age of the smart machine: The future of work and power" where she describes the "use of information technology in organisations" (Kallinikos, 2011:1). In her studies, Zuboff describes how information technology can be used to "automate" business processes and also describes how information technology can be used as an "informative tool" for business decisions (Zuboff, 1985). "Informated" is a process described by Zuboff to explain where a business organisation uses "knowledge and information" through the use of technology to make business decisions (Kaiserlidis & Lindvall, n.d.).

Phenomenology and phenomenological research is described by literature through a number of philosophical manners and viewpoints. “Phenomenology is a philosophical discipline” that can be used as a research “framework to provide a contextual view” of what is researched by collecting data on the “environment, past experience, knowledge and interactions” (Frauenberger, Good & Keay-Bright, 2010). The Phenomenological approach will also be used as “guidance” when the research tools are designed (Frauenberger et al., 2010:188). The use of this approach is in line with what was discussed in the literature and as a guiding view for collecting and analysing research data.

There are several ways of looking at what phenomenology is and how it can be used to guide research. In an in-depth literature synthesis of Thomas Groenewald, descriptions of phenomenology as a “research paradigm” include “studying the environment people live in” as well as “how they think”, and then writing up the understandings of the research evidence gathered (Groenewald, 2004). Key terminologies are highlighted in these studies, such as “personal experience, personal knowledge, personal perspective and personal interpretations”; in order to describe how phenomenological research is conducted (Lester, 1999).

This thorough description of the philosophical viewpoint and how it can be used to do research is applicable towards the previously described research problems and research question of this study. The object of study, namely small IT-dependant business organisations in Gauteng, has a specific nature that needs to be understood to confirm the current research suggestions and to add a valuable discussion on the impact of the research results.

It is important to understand how people in the small IT-business organisations of Gauteng use and understand information technology, their knowledge on specific subjects and their decision making capabilities using their personal knowledge and perceptions. When questions around this can be asked and answers provided, it will be possible to gain a better understanding and write research findings. The phenomenological viewpoint goes along with qualitative research that was primarily selected because of the lack in current research and the need for and in-depth study on information security awareness. Owing to the ‘in-depth’ nature of this study, the mentioned characteristics of the phenomenological viewpoint have to be measured according to the research tools and instruments that will be used. The reasoning behind the decision making of individuals in the business has also been highlighted as a key question that has to be investigated, especially when looking at the understanding or awareness of these individuals.

3.3 Ontological Viewpoint: Relativism

The ontological view followed in this study shall be the view of "Relativism", which states that there is "no consistency in moral beliefs and principals as people are individuals", meaning there are no "standard morals" (McDonald, 2010). This was explained in chapter 2 where it was discussed that there is no consistent model, framework or best practice currently being followed by the small business organisations of Gauteng. The lack of information security awareness in these small business organisations was explained, as well as the possible associated risks that have to be studied and understood. This is also in line with the guidance of the phenomenological view that will guide the analysis of the data in Chapter 4. In this Chapter the qualitative data gathered has to be analysed according to the selected conceptual framework and other described research approaches.

Relativism is "not the opposite", but rather a mutual philosophy for "idealism", which states that individuals can sometimes make "ethical decisions based on a framework" (Al-Khatib, Malshe & Sailors, 2009). The selected population of the study can be described as 'irrational' thinkers with minimal-to-no framework of reference for information security awareness in organisations. This theory should not cloud the research results or outcomes with bias, making it necessary to understand where these individuals get their knowledge from and how they use it for rational decision-making.

3.4 Understanding the small business environment: Interpretivism

After the ontological view of relativism has been described, the epistemology, or area of "acceptable knowledge", has to be defined, which will form part of the core research in this study (Saunders et al., 2009:240). As mentioned in the research design of Chapter 1, the philosophy of interpretivism shall be used to understand the social behaviour of people in the small-business environment of Gauteng and the information security awareness in their organisations. This can be gained by understanding the knowledge of these individuals as well as their decision-making processes. This is consistent with the phenomenological research theory and the described characteristics and purpose for the study.

Interpretivism has been selected as the research philosophy as it helps to understand the "complexity of the social environment", which then gives way to the researchers own interpretation or frame of reference (Blumberg et al., 2008:253). The epistemological research approach will thus be used to guide the study, while interpretivism will be used as reference towards how the research approach has to be followed.

To summarise, the mentioned philosophical views that are accepted for this study are used to develop a clear understanding of the information security awareness in the small businesses of Gauteng, without any standard moral principal and through the researchers own framework or viewpoint. This approach will help answer the research question and achieve the set research objectives.

3.5 A qualitative research approach for the study

Chapter 4, section 4.1 will discuss the selected qualitative research approach that is followed for this research study. In both of the previous two chapters it was explained why a qualitative research approach is best for the research problem presented. The research philosophy and viewpoint form part of the qualitative interpretation that will be followed.

Quantitative Research is mostly focused on numbers, especially when an exact number can be calculated using a certain method that can be explained and documented (Saint Mary's University of Minnesota, 2003). Qualitative Research, on the other hand, works towards “describing the quality of something or the how much”, instead of necessarily answering it statistically and numerically (Blumberg et al., 2008:192). “Qualitative management research” is difficult to define in a single manner and has to be specifically tailored to its intended research environment (Johnson, Buehring, Cassell & Symon, 2007:37). The rest of Chapter 3 will elaborate on the intended tools and methods that will be used to help answer the research question and objectives.

The use of a qualitative research approach conforms to the previously mentioned research philosophies as well as to the purpose of this research study. It has been motivated and explained that an in-depth study has to be done on the small information technology-dependant business organisations of Gauteng. It can further be noted that the selected philosophy of ‘interpretivism’ and the viewpoint of ‘relativism,’ are both in line with following a qualitative research approach. The use of a qualitative research approach is beneficial to this study in a number of ways as stated in the research purposes.

There are two other reasons for the selection of the qualitative research approach: It is common for business studies to be of a qualitative nature, firstly, if there is a “sociological and psychological” influence, and, secondly, if the phenomenon is relatively new with minimal research already conducted in the specific research area (Blumberg et al., 2008:192). The businesses in focus in this study are the small IT-dependant business organisations of Gauteng and the sociological impact is the threat that exists in the use of information and communication technologies in the businesses. The psychological influence includes the awareness that the employees in the organisations have towards the factors highlighted in Chapter 1 and 2. A qualitative research approach is deemed correct for the purpose of this research paper, as this new phenomenon needs to be described before it can be quantified. As little current frameworks for the measurement of the particular object of study exist, it will be important to draw themes and conclusions for the proposed fieldwork to ensure that adequate and suitable conclusions can be made. Following the selection of the qualitative path for the research, a supporting set of philosophical views will be included to describe how the research will be conducted.

A secondary ontological view, namely 'subjectivism', shall be followed to support the philosophy of 'interpretivism' by accepting that the research findings will be viewed through the researchers "perception or viewpoint" (Saunders et al., 2009:240). The use of this philosophy thus makes the assumption that the research findings will be from the researcher's point of view. The use of subjectivism and interpretivism fit well with the qualitative research study that will be followed and has been described in the research design so far.

The first research method used in the study has been an extensive review of the literature around the research topic. The literature was unpacked in Chapter 2 where the need for the research and suggested research approach was explained. The literature is used throughout the research including the research design and data gathering and interpretation. This will help the research process to stay on track and to keep the researcher informed of the tools and techniques that can be used to assist the study. Academic journals, conference proceedings and trusted media sources will mostly be used along with other significant material to synthesise the research problems and first three chapters of the study.

3.6 Sampling technique and sampling criteria: Information Technology-Dependency Tool

The second research instrument will be an 'Information-Technology-Dependency tool' that will be conducted telephonically or face-to-face to draw the sample from the selected population. This sampling method is known as "criterion based sampling, critical case sampling" or the purposive sampling technique that will be used to select the correct small businesses in Gauteng (Turner, 2010:757). The following will describe the reason for the selection of the sampling technique, including why it is the suggested tool for the selected research population.

The technique is a non-probability sampling technique and is also referred to as "purposive sampling", by which the sample has to "adhere to a specific criteria" before being further included in the study (Blumberg et al., 2008:253). The 'specific criteria' will be used to determine if the selected organisation is dependent on information and communication technologies or has any critical business processes related to ICT. This will help to reduce time when conducting the interviews as all the subjects will be valid for the study. The specific non-probability purposive sampling technique used in the study is seen as “homogeneous sampling”, which will draw 5 samples from the population that will adhere to the set criteria of being an IT-dependant business organisation (Saunders et al., 2009:240). These five samples are then regarded as part of the population for the study as it represents the information technology-dependent small business organisations of Gauteng. The sampling criteria will be explained in the next section along with the method for sampling.

3.7 Semi-structured interviews and sample selection

Non-standardised, semi-structured interviews shall be used to gather the primary empirical data and is selected because of the relatively large population and lack of existing research on the specific topic (section 3.1). This will be discussed in the next section where the second research instrument will be applied to the selected sample.

The time frame for the study will be a cross-sectional study where the current information security awareness of small business organisations in Gauteng, South Africa is to be determined. The selected sample will be drawn from the technology owners or representatives of the small businesses in Gauteng that make use of information technology as one of their core business or supporting business functions.

Non-standardised, semi-structured interviews shall be conducted from a qualitative approach with the owners or IT representatives of the small businesses in Gauteng. A selected sample of 5 in-depth, semi-structured interviews will be conducted, transcribed and analysed. Semi-structured interviews are selected because respondents have to be guided along the topic of information security related risks that exist in the business environment (Blumberg et al., 2008:385). Section 3.1.2 will expand on the selection and motivation for the interviewing technique as a research tool for this study.

Owing to the selection of a semi-structured interview, an interview-administered-questionnaire will form part of the study to help guide the topic and determine the current information security awareness that exists in the studied organisations (Saunders et al., 2009:360-371). Standardised tools will be adapted and tailored to fit the profile for measuring the information security awareness that exists in the small business environment of Gauteng. The questionnaire will be given to the respondents during an interview and will make use of techniques such as the Kruger, Drevin & Steyn, 2001 “vocabulary test” or “consensus ranking”, which can be used to measure the understanding of information security awareness of the respondents. These techniques mentioned in the literature review have to be in line with the conceptual model's approach that will guide the research.

Results gathered from the previous methods will be used along with existing techniques like the "consensus ranking approach", which will categorise and prioritise the different aspects of information security awareness in the small-businesses (Kruger & Kearney, 2008:255). The "attitude behavioural system" described in the literature and the conceptual model will finally be used to ensure that the information security awareness is measured as intended for the research and purpose. This is in line with the philosophical approach of the regulatory perspective to support the current business infrastructure rather than to re-engineer it. The next section of the research design section shall expand on the suggested research tools and how they will be formulated and executed as part of the research data collection.

3.8 IT-Dependency and Tool as sampling criteria

Following the discussion in the Literature review and the beginning of Chapter 3, the focus of the study is on the small IT-dependent businesses of Gauteng. A tool has to be composed and tailored that can be used to determine if the selected small businesses have an information technology dependency or not.

In big organisations it is not uncommon to find formal models, policies and procedures that deal with the management of cyber security and information security threats; And from these formal plans that help to protect the business's information assets, backup plans will be made in case these security measures fail. A scenario like this is sometimes referred to in the business environment as a "disaster where formal contingency plans" have to be made from an already established set of "business continuity plans" that will help recover the business form its disaster state (Arduini & Morabito, 2010:122).

The reviewed literature has already indicated that this is not the case for small businesses in Gauteng and that a lack of cyber and information security awareness exists. Both Chapter 2 and the Research questions indicate that the purpose of the study is to identify the level of cyber and, specifically, 'information security awareness' in these business organisations. Part of the focus of this requirement is to identify the small business organisations of Gauteng that are information technology-dependant. The meaning of an IT-dependency has also been defined in Chapter 2 and as part of the research objectives.

Further research stipulates the different types of IT-Dependencies that a business organisation may have. One of these divides IT-dependencies in the business environment into two categories: “The first type” is when the business organisation is dependent on an improvement in a business process created by IT alone, while the second type is when a business process is improved by IT but could still be done manually although it would be at a loss to the business (Nordströma, Söderströmb & Hansethc, 2000).

Chapter 2 discussed how the small business environment, and in particular that of Gauteng, has a lack of these formal business procedures and it was argued that the rationale for this is often owed to the lack of user awareness that these incidences can cripple a small business. To measure how vulnerable a business is against theses technology risks, the IT-dependency of the business has to be measured. This will need to be done in such a manner that the size of the business organisation is carefully brought into consideration before evaluating how it uses information technology as part of its business operations.

At the end of Chapter 2 the conceptual model was described as the preferred representative model to articulate the collection of tools and methods that will be used to achieve the research objectives of the study. The use of the conceptual approach to guide the research will be further explained in Chapter 4 where the data is analysed and findings noted.

One of these will be the formulation of an ‘IT-Dependency Tool or Checklist’ that has to be applied to the business organisation before including it in the sample as specified in the research objectives. This will not only help with the sample selection process of the study but will also give a better description and understanding of the business and its daily use of information and technology.

3.9 Information Technology Dependency and Critical Business Process Identifier

It was explained in Chapter 2 what information technology-dependency is in a business organisation, as well as how it will be included for the purpose of this study. When a technology dependency occurs the business makes use of IT as part of a critical business process that has to be maintained for the business to operate. Research recognises the increasing need for “planning and risk management” that has to be undertaken because of the increased IT-dependency (Business Roundtable, 2007). The selected population of business organisations with technology as a critical business process, thus those that are IT-dependent, are the target for this measurement tool.

A tool is needed that will help with the sampling and that will understand how the small business organisation is dependent on the use of information technology as well as the business components that are dependent.

3.10 Planning for Information Technology-Dependency measurement

The approach identified in the previous section will focus on the IT-dependant small business organisations in Gauteng, South Africa to execute the interview research instruments. Following from the discussion made earlier in this chapter, an information-technology-dependency tool, needs to be designed and guidelines need to be established on how it will support answering the research question. The research approach to this requirement will be through a short telephonic or face-face interview incorporating a small set of questions. All the questions asked are close-ended questions mostly requiring a ‘yes’ or ‘no’ answer, which will be fully described in the following section. Probing techniques may be used to give the interviewee a better understanding of the question that is being asked with all precautions taken to avoid influencing the participant with the researcher’s own bias.

The use of this approach was also identified in Chapter 2 as purposive sampling, where a sample is drawn after it meets a certain criteria. The questions are formulated around the discussion of what a dependency is to the business as well as how this is applied to the use of technology in the small business.

Each question will be scored or given a ‘yes’ or ‘no’ indicator, which will then ultimately be used to determine if the small business-organisation has an information technology dependency or not. As the IT-dependency in the business is tested it will be aligned to the described phenomena of a ‘critical business process’ and how the organisation is dependent on this process for the business to be operational, as explained. This will be performed on the selected small businesses of Gauteng that are believed to make use of information technology on a regular basis. By applying this research technique, the necessary samples can be drawn for analysis by the suggested qualitative and conceptual approach.

The successful answering of the questions will indicate that the business organisation makes use of information technology and has an IT-dependant business process. Lastly, it has to be established if the organisation makes use of personal and sensitive information as part of the business operations, as described in Chapter 2. By conducting the interview, the researcher can also get a brief insight into the current business activities that are taking place and how they make use of information and technology. This will give the researcher an understanding of the types of information used and how the information flows within the business. By taking this tailored research approach, the sample can be prepared for the second analysis techniques, which are the non-standardised, semi-structured in-depth interviews. This research instrument will be discussed in the following section, but referenced throughout to display the overall research approach that will answer the research question.

3.11 Design of the IT-dependency tool

This section will start with the IT-dependency tool and how it will be used for selecting the sample (criteria sampling). The selected questions will be given to the participant organisations that must adhere to the set criteria to be deemed part of the population of the study, which are the IT-dependant small business organisations of Gauteng, South Africa.

Along with the formulation of the questions, a clear supporting reason will be given to indicate its relevance to the study and to draw a sample according to the set criteria of the tool, which will be done by referring to the literature or any other similar tools that have been discussed. The literature already indicated the need to make use of a specific sampling technique by which the sample must adhere to a certain criteria before being deemed part of the research population. After the questions have been formulated the tool can be used for selecting the sample of the research study.

Probing questions can also be used when telephonically or face-to-face administering the questionnaire to determine if the business has an IT-Dependency or not. The importance of using probing techniques and a tailored instrument is because of the diverse culture and language barriers that exist in Gauteng. This will help the researcher who is also gathering the empirical evidence in assuring that the participant understands the question and answers as accurately and truthfully as possible.

To place reliance on this tool, the follow-up in-depth semi-structured interview can be used to confirm and elaborate on the organisations use of information technology as a critical business processes. This interview will make use of similar and more in-depth questions with the intention of evaluating and confirming IT-dependency. Along with the confirmation of IT-dependencies, the remaining questions, according to the instruments design, will investigate the organisation’s information security awareness.

The questions set out below will be administered verbally, either through face-to-face meetings or telephone conversations, which will then identify the selected sample for the study. The questions are set in such a way that all must be answered ‘yes’ for the organisations to be classified as information technology-dependant. Thus, if all questions are answered yes, the organisations will be seen to have an IT-dependency and will be a valid member of the population that was identified for the purpose of this research study. After the successful administration of these questions and the gathering of the necessary samples, the following step can be taken, which is to conduct the interviews.

3.12 Questions for the information technology-dependency tool

Refer to 'Addendum A' for the IT-dependency tool and questions.

1: Small business organisation: South Africa

The purpose of the first question is to make accurate judgements on the size of the selected business organisation. In Chapter 1 it was stipulated that according to the 'South African small business act', a small business organisation has more than 5 employees but less than 50 employees. Answers to this question must be accurate, as it determines, according to the guidelines of the Small Business Act of 1996, if the participant organisation is a small business organisation of South Africa (according to size of business). According to the information provided by the respondent, the small business organisation will then be classified as an official small business or not.

2: Technology use in the small business organisation

The second question is simply to confirm and have the identified technology representative of the organisation state that he/she is aware of information technology that forms part of the business organisation. The person to be interviewed, as explained in Chapter 2, should be the key IT-person or owner of the small business organisation.

3: Dependency on information technology

It is important to determine if the business is aware of their IT-dependencies, such as business process that cannot function without the organisation making use of IT. Therefore, this will have to be a probing question so that the interviewee can comfortably identify if any business processes cannot be executed without the use of information technology. The interviewer can also confirm the response by asking follow-up questions to ensure the response is as accurate as possible.

To ensure the question is answered accurately, the interviewer will need to listen to the described 'critical business process' to identify the following:

- If the process that is described by the participant is a business process that is actually used within the business organisation and that makes use of information as well as technology.
- Secondly, if the described business process involving the use of information technology makes the organisation IT-dependant according to the set criteria of the instrument.

4: Information Technology-dependant business processes

The purpose of this category is to give the interviewer a good understanding of the types of information that is used by the business organisation and for what this information is used. The understanding of information can be compared to the set definitions and criteria in Chapter 2, to ensure that the information adheres to the specified criteria of being personal or sensitive.

By verifying the above questions, the researcher can determine if the organisation falls within the set criteria of the selected population for the study, as identified in this section and described in Chapter 2. This includes:

- The organisation is a small business organisation (Small Business Development Act 1996 Definition) and that the business resides within the province of Gauteng, South Africa.
- The organisation has an information technology-dependency, as defined in Chapter 2 and Chapter 3.
- The organisation makes use of information as defined in Chapter 2, which makes it relevant to the research problem.

The final questions formulated for the IT-dependency tool that is going to be used for this study can be found in Addendum A. Each question is in the order as the above-described factors and will determine the IT-dependency of the business organisation. For the small business organisation to be seen as an 'information technology-dependant' business organisation, the questions have to be answered according to the following (Table 1 below):

Table 1	Yes	No
Question 1	✓	
Question 2	✓	
Question 3	✓	
Question 4	✓	

This outcome was described in Chapter 2 as the "Purposive Sampling Technique" by which the sample will be tested beforehand and has to "adhere to specific criteria" to form part of the population. In the case of the defined research tool, all questions have to be answered 'yes' for the organisation to be seen as part of the population of the information technology-dependant small business organisations of Gauteng.

The main purpose of the IT-dependency instrument is to determine if the small business organisation of Gauteng has an information technology-dependency or not. It further sets the scene for the in-depth interview where the information and technology use of the business has to be understood in detail.

Research suggests that when studying 'information security awareness' in the business it is critical to "identify the key stakeholders" that take part in studied activity (Tsohou et al., 2008:333). This statement is strongly supported by the suggestions made in Chapter 2 around the diverse demographics of the studied object. It is important to define who the relevant stakeholders in the businesses are, as well as to motivate why the selected interviewee is best to answer the questions on the organisations information and technology uses.

Addendum A of the research document includes the questions selected to determine if the small business organisation has an information technology-dependency or not. Following the execution of the IT-dependency tool and the selection of the research samples, the next research instrument can be applied. The planning and designing of the interview questions will be done in the next section.

3.13 Providing context to 'information security awareness' and the small business sector of Gauteng: Self-Categorisation

The understanding of information security awareness has been clearly explained by various definitions and examples. This was done in Chapter 2 along with the larger context of information security management and cyber security management, as well as cyber security awareness. Information security was also applied to the small business organisations of Gauteng.

To understand the information security awareness of the small IT-dependant business organisations in Gauteng, a clear understanding has been obtained on the discussion made in Chapter 2. Key themes from the literature shall be used to construct the self-categories of the research instrument. These themes or topics relate to all the various factors discussed in Chapter 2 around small business organisation in Gauteng and South Africa, information and cyber security and information security awareness.

The themes drawn from the literature will help answer the information security awareness and what is required to understand the information security awareness of the business. In Chapter 2 the proposed self-categories for the research study were identified.

3.14 Definitions and understanding of interviews as instrument

This section is dedicated to describing the second research tool that is to be used for empirical data gathering in the study. Sections are separated to, firstly, give an understanding of the selected tool, followed by the motivations for applicability to the research problems.

An interview can be broadly defined as “a meaningful conversation” that is used as a research technique to “collect descriptive data through the subjects own words”, which can then be analysed to gain further understandings (Carruthers, 1990:64). As explained in the previous section of this chapter, the interviewing method selected for this study shall be the semi-structured, in-depth and face-to-face interview approach. This approach has several suitable qualities for the qualitative research approach of the study as well as the research question. The three types of interviews include “structured interviews, semi-structured interviews and unstructured interviews” (Fox, 2009).

Fox describes ‘structured’ interviews as interviews “that are mostly used for quantitative data analysis” where questions are all pre-defined and where the “possible answers” to the questions might also be pre-defined. An ‘unstructured’ interview has “a smaller number of flexible questions around a certain theme which are selected with the aim of getting the participant to talk around them to obtain a broader understanding” of the research objectives (Rowley, 2012:262).

From the literature reviewed it was observed that semi-structured interviews do not always lie exactly between structured and unstructured interviews but definitely contain attributes from both of these two main types of interviews. Semi-structured interviews can be seen as interviews that involve the “preparation of questions that are guided around themes” and can also include other interviewing techniques, such as “probing” (Qu & Dumay, 2011:246).

From the above explanations, as well as from the discussion for the selection of a qualitative research study, the semi-structured interviewing technique is deemed to be the best approach to help answer the research questions. To ensure that this research tool is well designed, various sources on ‘semi-structured interviews’ and the understanding of information and technology in business were studied.

In this situation the tool had to be tailored for small, IT-dependant business organisations in Gauteng and is seen as the best tool for solving the research question.

3.15 Motivating: Semi-structured, in-depth face-to-face interviews

Chapter 2 gave a clear explanation of exactly where the research problem resides, as well as the current research that has already been conducted. It was concluded that little published evidence exists, creating a need for the proposed research questions to be answered through an in-depth study. The literature suggests that one of the best methods for gaining an insight into a person's understanding and "experience of something would be to ask them" through the process of a semi-structured interview (Reid, Petocz & Gordon, 2008:47).

A major advantage of the interviewing method is that it keeps its "objectivity", but still captures the subjects "opinions" as well as the "reasons they have for them" (Carruthers, 1990). This statement was clearly highlighted in Chapter 2, where the lack of current research into the object of study was described. It was concluded that an extremely objective tool should be used to capture the correct information that will help gain a better understanding into the 'information security awareness' that exists in small business organisations.

Semi-structured interviews "relate to structured interviews" in the sense that questions are pre-defined but differ as the "questions are not close-ended but rather open-ended" (Fox, 2009). This is what is needed for the purpose of this study as not enough research has been done so that a standardised questionnaire or structured interviewing technique can be used to answer the research questions. The need for both objectivity and open-ended questions is critical to the object of study because of its current lack of research.

An "elite or expert" is defined within a business environment as the person in an organisation who is "considered" the most "important" or has the best "knowledge" in that environment; a specific research technique called "Elite or Expert Interviewing" exists (Moore & Stokes, 2012:439-440 and Harvey, 2011:432). This interviewing technique best supports the need for the selection of the participant in the organisation that is most qualified to discuss the use of information and technology.

"Elite or expert interviewing" will form part of the qualitative approach of this study because it focuses on the people that have a clear understanding of the business processes that exist within the studied environment (Blumberg et al., 2008:202). This technique is specifically chosen to complement the research instruments, which state that the owners or IT-representatives of the small business organisations have to be interviewed because of their understanding and knowledge of the different information and technology used in the organisation.

3.16 Using theory and research methodology to plan the interview and design the interview questions

As mentioned in the first two sections of this chapter, it is important that the research tools are able to provide "answers" to the research question (Rowley, 2012:263). The design of the interview instrument has to be carefully done to ensure that sufficient information is collected for answering the research question and achieving the research objectives. One of the simplest ways in which this planning process can take place is "preparing for the interview, the construction of the correct research questions and then to conduct the interview" (Turner, 2010:756).

To ensure that the participant has an overall understanding of the intended interview, the research questions shall be explained in a simple and understandable manner. It is important that before the interview is conducted, the participant is fully aware of the specific terminologies that will be used during the interview (Rowley, 2012:263).The next sections will expand on the various techniques that will be used to achieve these objectives, which will help ensure the accuracy and efficiency of the research instrument.

3.17 Elite/expert interviewing: information technology representative of the business organisation

The key 'information technology' contact or business owner in the organisation has to be found for elite or expert interviewing to take place. It is important to identify the correct person that has knowledge around the overall business operations and how this process is supported by information and technology. These elite or expert people in the small business organisations will likely be the owner of the business or an IT-representative. The selected representative for the participant organisation has to have knowledge of the following:

- Information use in the business
- Information technology use in the business
- IT and information security in the business (no technical knowledge but an understanding on the business actions towards these areas is required)

The first IT-dependency research instrument will help assist with ensuring the representative for the participant business will be able to answer the questions relating to the above mentioned criteria.

3.18 Bounded Rationality for designing interview questions

One of the first tools that can be used is the "*psychological concept of bounded rationality*" that can help the researcher to understand where the stakeholders in small businesses have a lack of knowledge when it comes to cyber and information security awareness (Stewart & Lacey, 2012:30). Bounded rationality can occur when people want to make a decision "but cannot always do" so because of a lack of understanding and knowledge on their "internal and external environments" (Jones, 1999:298). As long as the reasoning behind bounded rationality is kept in mind, the researcher can be guided by not asking biased questions or making biased decisions or assumptions.

Using the approach of bounded rationality the researcher will be able to identify the current awareness levels in the self-categories of the studied small businesses organisations in Gauteng. "Rationality" in this instance is described "as the best or value maximising choice" users will make when confronted with the risks of information security. The term is referred to as "bounded rationality" because the users are not fully aware of the risks and are only making decisions based on the best of their understanding and capability (Robbins, Judge, Odendaal & Roodt, 2009:124). As the literature has already identified that people do not always make perfectly rational decisions, because of their limited knowledge, it will be important to determine what actions and decisions they will take.

The literature suggests that "conceptual frameworks", like that of "bounded rationality", should be used when studying information security awareness in small business organisations, including those of Gauteng (Stewart & Lacey, 2012:37). Chapter 2 unpacked the concept of bounded rationality and how it can be used for studying information security awareness in business organisations.

Bounded rationality will be the first approach utilised in the interviews so as to help identify what the small business understands about cyber and information security. These self-categories will not only include the specific threats that exist, but also the understanding of their impact on the business. As explained in the research objective, holistic information such as this can help with future research and implementations with regards to the cause of the research problem.

Bounded rationality also explains how "users make decisions based on their existing beliefs, attitudes, limited knowledge, time, available resources as well as level of satisfaction" (Stewart & Lacey, 2012:33). The conceptual model identified in Chapter 2 illustrates how bounded rationality relates to knowledge in the business and how knowledge forms part of the components for understanding information security awareness.

3.19 Supporting the interview questions with theory

The interviews will make use of probing techniques such as 'open-ended questions' to understand the nature of the business, its dependency on information technology and if any current awareness methods are in place for cyber and information security threats (Saunders et al., 2009:338). Structured questions will be designed according to the required purpose, using techniques such as "introductory questions" for setting the scene; "follow-up or probing questions" to clarify the required information and informal questions to further explore the proposed problem (Blumberg et al., 2008:288).

Saunders et al describes probing as "follow-up questions or suggestions" that will help the participant deliver more accurate and in-depth responses that will be analysed to answer the research questions.

It was explained how the participant will be prepared for the interview through a series of opening questions and explanations as to the objective of the study, as well as to give the participant a better understanding of what is required from him/her. These will all be in line with the identified set of research questions and research objectives, and with the evidence that is required from the interview. This part of the interview is thus intended to set the scene and prepare the participant for the questions that will follow (Guion et al., 2011).

After the set of opening questions have been administered to gain an overall view of the business and how the business makes use of information technology, the specifically selected topics can be questioned. Introductory questions on the selected topic will be administered, as well as the suggested probing techniques to ensure that the participant is well informed about the topic as well as understands what is expected of him/her as representative for the small business.

The second interviewing approach to be undertaken will be the delivery of "specific, direct and indirect questions (Qu & Dumay, 2011:249). These questions will be formulated around the introductory questions to gain an understanding of the selected topic and its relation to the small business. Again, the use of probing techniques, such as open-ended and follow-up questions that the interviewer deems important in solving the research question, may be asked.

As suggested, specific questions will be used to address the identified topics and will be asked in such a manner that they will allow for a series of direct and indirect follow-up questions to emerge. The use of the “follow-up and probing” technique has been highlighted throughout this section of the chapter and is also suggested by Qu and Dumay (2011:250) and Turner (2010:758).

A direct question will be to have the participant focus directly on a particular example and give an explanation of the situation, while indirect questions will be used to obtain the participant’s opinion so that it may be analysed. Probing will then be used to guide the participant around the topic of questioning to ensure that the response is as accurate and complete as possible.

The first tool that has to be designed is the IT-dependency tool as described in Chapter 2, which will be used for purposive sampling when selecting the small businesses. After the IT-dependant organisations have been selected, the semi-structured interviews can commence with more specific data relating to cyber and information security awareness.

3.20 Design of the interview and interview questions

The outcome of another South African study emphasises the “need for” the presence of “information security awareness” in business organisations as well as the “importance” of a localised approach to the needs of the business (Thomson, 2008). This raises the need to gather empirical evidence regarding information security awareness in the small information technology-dependant business organisations of Gauteng. This is stated as part of the research objectives that will help solve the defined research question.

Once the business organisation’s IT-dependency has been established, the semi-structured and in-depth interview discussion can be executed. It was explained in the ‘elite/expert interviewing technique’ section of this chapter how the representative will be selected form the participant business. This is a common selection technique by which the most relevant IT person in the small business is selected for interviewing (Tsohou, Kokolakis, Karyda & Kiountouzis, 2008:330).

As previously mentioned, this will be done by using the key-themes identified in Chapter 2, similar research tools and the research question and objectives that will help tailor the tool to the small business environment of Gauteng. It has also been explained how this tool will be administered by having the key-information technology person in the business answer the questions.

Structured and semi-structured questions have to be created using the suggested approach of consolidating various sources. The questions are designed so that some will contain follow-up questions and probing suggestions so as to gather evidence for analysis. Supporting literature and reference to previous sections will again be used to ensure a holistic and sound approach is adopted for the research instrument.

One of the qualitative research approaches to be taken is the phenomenology approach by which the phenomenon of information security awareness in the small IT-dependant business organisations of Gauteng is studied. The concept of phenomenology is explained in chapter 2 where the importance to the study is also discussed. This chapter highlighted how a number of theories and frameworks will be used to formulate the interview questions. The research conducted and formulation of interview questions will be done using elements such as "practical experiences, existing research" as well as the research question and objectives (Rowleyq, 2012). Along with this approach, the grouping of themes or 'self-categories', as explained in Chapter 2, will help to guide how the interview questions will be formulated.

This was explained as 'self-categorising' by which key themes and topics are drawn from the literature discussed in Chapter 2 along with practical experiences. With bounded rationality and planned behaviour the identified self-categories will form part of the conceptual model that will guide the research objectives.

When the interview questions are formulated the research question and objectives have to be carefully aligned so that each interview question addresses the research question in its own way. How the responses to the interview questions will be analysed also has to be carefully planned and considered when formulating the interview questions so that it aligns with the research question and objectives.

The theory of planned behaviour from Icek Ajzen that was used in the model of Kruger and Kearney to measure information security awareness will also be used as guidance for designing the interview questions and conducting the interviews in this study. According to the model of 'planned behaviour' and as explained in the literature, information security awareness has "three dimensions": namely "knowledge, attitude and behaviour" (Ngoqo & Flowerday, n.d. and Ajzen, 1991:179). These dimensions are weighted and in Chapter 2 it was indicated that researchers adapt these weightings according to the importance of each one towards measuring information security awareness. Weightings to quantify the 'knowledge, attitude and behaviour' components of the 'self-category' are sometimes assigning with percentage weightings to each. For this qualitative study no percentage weightings will be used, as the conceptual model will guide the interpretation of the results.

The next section will describe the self-categories that were drawn from the literature as the categories or topics needed to understand the information security awareness as well as other elements of the businesses. References to the literature from Chapter 2 will be used for the motivation of each of the themes or categories for which the interview questions are made. To identify the categories, the literature and objective to answer the research question will be used as guidance. Addendum A includes the entire set of questions that form part of the second research instrument to be used. The questions are grouped as described and are formulated around testing the organisations' knowledge, attitude and behaviour in terms of information and cyber security in the business environment.

The themes drawn from the literature review in Chapter 2 that will form part of the research instruments include the following:

1. Information and technology as part of the business
2. Business financials
3. Information and technology failures
4. Passwords
5. Phishing and cyber security
6. Software and business IT applications
7. Personal and sensitive information

3.21 Formulating the interview questions

The themes listed above will be incorporated into the research instruments to gather the data so as to answer the research question. This is in line with the objectives of the research highlighted in Chapter 2.

Following some of the defined techniques for measuring information security awareness, especially those applied to the business environment of South Africa, the questions and techniques can be developed for this study's requirements. The grouping of information and cyber security and awareness related topics were also observed by a similar study that was conducted on the South African mines, which used "6 main focus areas" with several types of questions for each area (Kruger & Kearney, 2005).

From the existing tools that are used to investigate cyber and information security as well as to measure information security awareness, a number of approaches were selected to guide the research approach:

- The "Vocabulary Test Method" uses information security awareness terminology and a set of pre-defined explanations from which the participant has to select the best or most correct explanation (Kruger et al., 2010:321). These questions will be used to test the participant's knowledge on the identified topics relating to information and cyber security awareness. These close-ended questions will be followed by more in-depth and open-ended questions that will investigate the participant's and the organisation's understanding of information and cyber security awareness.

- Kruger et al. further explain that probing techniques such as "scenario questions" can be used to make sure that the respondent understands the question during the interview (Kruger & Kearney, 2005). Scenario based questions are different from the vocabulary test as they do not directly test the participants knowledge on a certain terminology, but rather their understanding of the impact and concern that the business has regarding the discussed term (Kruger, Flowerday, Drevin & Steyn, 2011).
- Scenario questions instead of terminology testing (Kruger, Flowerday, Drevin & Steyn, 2011). This technique will be helpful as the IT-representatives in the small business organisations may not always know the exact meaning or definition of a specific terminology, but may still be able to apply its meaning in practice.

The above-mentioned references for setting interview questions were identified and described in Chapter 2 as well as the above to formulate the research instrument. The selected questions are also in line with the proposed techniques mentioned to analyse qualitative data. The section below will identify the categories selected for questions and motivate the selection of the intended question. The selection of the categories was done in Chapter 2 where the information and technology needs for the study were discussed.

Information and technology as part of the business (example):

Have you observed changes through the use of IT during your employment with the organisation?

Yes	No

Changes can be examined using probing methods to understand the change in business processes or day-to-day activity regarding the use of information and technology. The observed changes by the respondent will indicate to the users how agile the organisation is as well as its capacity for change.

This question proposes the observation of the respondent towards one of the research topics studied: Is the respondent aware of any change in business processes and the use of IT.

Business Financials:

When financial and other sensitive information is used in the business and processed electronically, it was mentioned that it affects some of the studied elements in this research. This is explained in Chapter 2 and forms part of what needs to be studied in the small businesses of Gauteng. The use of electronic bookkeeping is incorporated into the definition of an IT-dependant business as a stipulation of the daily use of the technology.

The following question will investigate how the business organisation handles its financial transactions. The focus will be on the use of online banking and how it is executed as part of the daily business activities. The same reason investigated for sensitive information and cyber security from Chapter 2 applies to the necessity for this question. Again, probing or confirmation from another employee in the organisation will be used to ensure the participant understands the questions.

Information and technology failures:

Studying the information and technology environment through the participant's view of problems cannot give concrete evidence of the failure of an IT plan in the company, but can give an indication of how the business relies on IT processes as part of its business activities. Relying on information technology thus creates the IT-dependency that exists in the business, which was discussed in Chapter 2 where the subject of study was unpacked. The questions in this section also relate to the discussion in Chapter 1 on critical business processes and how IT can play a part in those business processes. Again, these questions may be supplemented with probing and follow-up questions.

An example can be used to explain the set question to the participant without directly influencing his/her opinion. The criticality of IT to the business was tested with the IT-dependency tool and now a better understanding has to be gained of the business organisations dependency on information technology.

The business problems that have been reported should be investigated to determine how they affect information and technology in the business organisation. Although the exact cause and truth behind this probed question can only be understood in the subsequent one-on-one interview, it can still be used to indicate whether the business has had incidents of interest to the study.

The question regarding the loss of personal or sensitive information will be directly stated and carefully explained to the participant to understand if the business has suffered a loss. If the participant is uncertain, confirmation can be gained from within the business or a by way of a better explanation to ensure that the most accurate answer is recorded.

The interviewee is to be reminded that the study will be anonymously recorded and that no reference to the name of the business will be made unless explicit approval is acquired.

Passwords:

Passwords and the complexity of passwords was investigated in the literature review and explained to be relevant to the purpose of this study. This question's response can be contrasted against the previous loss of information question to gain a better understanding of why the incident has or has not occurred.

One of the referenced studies conducted within a South African and global organisation explored the use of passwords and its criticality to the security of information and technology in the small business, as was discussed in Chapter 2. The awareness of information and cyber security was clearly highlighted in chapter 2 when it was applied to the small business organisations of Gauteng.

Phishing and cyber security:

The questions relating to phishing were adapted from a study done by Kruger et al. 2011 in which the "scenario" of phishing was tested rather than the word meaning. The participant does not necessarily need to know exactly what the term 'phishing' means, but what is tested is how the respondent will act when presented with a case of phishing.

If the organisation does not make use of internet banking, any other online activity that requires the use of information will be discussed.

Following the interviewee's response to the above-mentioned scenario question, the discussion will focus on understanding how phishing, as a possible cyber security threat, is perceived in the small businesses of Gauteng.

The purpose of understanding these threats, risks and other security concerns form a big part of understanding the information security awareness in business organisations. Chapter 2 presented a detailed discussion of how this impacts the research question and objective.

Furthermore, phishing and cyber security forms an important self-category that will help understand how information and the IT of the business are protected. This also gives an understanding of how the business has created awareness around these threats.

Software and business IT applications:

The use of software in the business was described as that which uses information that can include personal and sensitive information. There is a need to understand the software that is used in the business and how it makes use of information in its business operations.

Furthermore, the possible dependency of the business organisation on the use of software has to be understood. Besides the business's use of information technology and software, the dependency of the software itself needs to be understood, as well as how it influences the daily operations of the business.

Personal and sensitive information:

Finally, all the personal and sensitive information that is gathered, processed and stored by the small business organisation has to be understood. This self-category is very important in understanding the information security awareness of the organisation and how it protects this information. By identifying the personal and sensitive information that is used in the business it will be easier for the researcher to ask more specific questions around the awareness of the safe and correct use of the information types.

3.22 Limitation of the research instruments

Such as any research instrument there will always be a limitation to its use. It is important for the researcher to plan appropriately for the limitations of the research instrument and to ensure that they are understood and recorded before writing the research findings. The first limitation is that the tools do not cover each "individual's" information security awareness level in the organisation, which can give an overall view of how aware the business organisation is (Mugo, 2012:53). It has been explained that the best information technology representative will be selected for the interview. It is believed that this will give the researcher the best possible result without interviewing every employee that is affected by the use of information and technology in the organisation.

The second limitation to the research instruments is that it is not tailored to every individual organisation's "structure" and does not necessarily access every operational level where information and technology is used (Mugo, 2012:53). This is related to the previous limitation where not all employees on all the levels of the business organisation can be interviewed. It is therefore important to carefully select the correct IT-representative in the business organisation. In the design of the research instruments it was also mentioned that during the interviews alternate resources can be used to strengthen the quality and depth of the data that is captured.

The qualitative data gathered will not be quantified, as It is more important for the research to gather an in-depth understanding of the small business organisations of Gauteng. This understanding will be supported by the conceptual model and viewpoints that is used for the understanding of the information security awareness of the small businesses of Gauteng.

3.23 Data Collection

As the research makes use of a “non-standardised, qualitative research approach,” the interviews must be “audio-recorded” and then “transcribed” into a “written document” (Pearlson & Saunders, 2009:485). It was specified in Chapter 2 that five interviews shall be conducted, each of about fourty minutes long, which will then be analysed in Chapter 4. The research design in Chapter 1 also specified that an “inductive” research approach will be adopted, which requires the gathered data to be grouped into “themes” from which “theories and relationships” can be identified (Pearlson & Saunders, 2009:490). Inductive reasoning is selected because a sample can be drawn from a population and once the “results” have been generated from the population, “inductive generalisation” can be applied “back on to the population” (Mouton, 2012:118).

This approach to the collection and analysis of data from the small businesses in Gauteng was specifically selected because of various reasons provided in the Literature. After the data has been collected, it will be analysed and described in Chapter 4. The support for the analytic techniques used will again be referenced from the literature review and previous chapters. The next chapter will start with the collection of the data, as discussed throughout this chapter.

Chapter 4

`

The research instruments utilised in this study have been designed and supported with reference to current literature in the field. The need for two tailored research instruments have been explained and are necessitated by the lack of current research and specific needs of the population of the study. By using these instruments data was gathered for analysis. This chapter analyses all the research data and captures the results obtained.

Chapter 4

Data Analysis

4.1 Introduction

The data has been gathered from the sample of small IT-dependent business organisations that were selected for the research study. The results are analysed according to the design of the research instruments and in support of the research problem.

Following the discussion around conducting interviews for data collection in Chapter 3, this chapter focuses on the analysis of the research data. To analyse the captured data from the interviews, the recordings are transcribed verbatim to preserve the integrity of the data that is ready for analysis.

When coding the collected data, careful attention is given to "defining codes clearly in a mutually exclusive way", which will help with the reliability of the data (Campbell, Quincy, Osserman & Pedersen, 2012). Relationships between self-categories and findings are to be drawn as previously suggested.

By continuing from Chapter 3, the first section of this chapter will explain how the qualitative data is to be analysed. This will be followed by the documentation of the research results. Overall, Chapter 4 will give a good overview of the research results by explaining how it fits into the research objectives and the design of the research instruments.

4.2 Qualitative Data Analysis

The literature and research methods have already described the need for a qualitative study and have presented the main reasons for conducting a qualitative research study on the small business organisations of Gauteng. The following section will expand on how the data gathered at the end of Chapter 3 will be analysed from a qualitative perspective.

The use of self-categories and the design of the research instruments are described in the previous chapter. The gathered data will now be analysed according to the design of the research methods. The approach to the analysis was discussed in the development of the research tools as well as how the interview questions are grouped and placed in a specific order when interviewing the participant. Section 3.1.3, in the previous chapter, elaborated on the data collection approach and how it is aligned to the design of the research instruments.

Bounded rationality was described as the understanding or knowledge of the participant that will be interviewed as representative for the small business organisation of Gauteng. This knowledge or understanding of the participant was described in Chapter 2, where the different types of knowledge that can exist in a business organisation were also identified. The analysis of the qualitative data was further referenced in Chapter 3 with the design of the research instruments.

In Chapter 2, the reasons for selecting a qualitative research approach over a quantitative research approach was explained and supported with a number of academic sources and scientific reasoning. Because of the abstract nature of qualitative research compared to quantitative numbers, there is no "standardised process" for analysing data, although three categories are identified: "Summarising, categorising and structuring or ordering" (Saunders et al., 2009:490). The self-categorising theory and the design of the instrument described how the interview questions, and, ultimately, the data that is gathered, should be grouped into categories. This can be seen in the previous chapter where the questions were formulated and in how they were grouped and structured accordingly.

The use of self-categories will make it easier to recognise relationships as well as to break down the research problem into smaller elements. Raw data will be used rather than a summarised form when analysing and observing the results. Categorisation or the use of self-categories will thus be one of the primary qualitative approaches used to analyse the data.

Before analysing the gathered results, a background will be given on the small information technology-dependant business organisations that were selected as part of the study's sample. This makes it easier to present the results and to understand from which sample organisation the result was obtained.

4.3 Background of research sample

a) **Organisation 1:** Finance and Business services

This organisation specialises in offering payroll and tax-related services to other small business organisations. Organisation 1 is based on a partnership business structure. The organisation has six permanent employees and two other employees on contract basis. The organisation and co-owner of the small business organisation indicated that the organisation makes use of information technology on a regular basis and has a dependency on IT. When describing its everyday business processes and activities, it was noted that IT forms a large part of the company and how it makes its revenue. One of the directors of this small IT-dependant business organisation was interviewed after selecting the sample through the IT-dependency tool.

b) **Organisation 2:** Retail and Motor Trade and Repair services

This organisation specialises in the trade and repair of second-hand vehicles and is a leader within its operating market in Gauteng. The business has a single owner along with a number of management staff. Organisation 2 employs around 45- 50 workers, which classifies it as a small business organisation according to the National Small Business Act of 1996. During the execution of the IT-dependency tool sampling, it was confirmed that the organisation makes use of IT on a daily basis and that it forms part of the competitive advantage for the business when trading in second-hand cars. The owner of the small business organisation was interviewed.

c) **Organisation 3:** Finance and business services

Organisation 3 is a small auditing firm that has a relatively large client base in the Gauteng province. The organisation makes use of personal and sensitive information on a daily basis and during the execution of the sampling tool (the IT-dependency tool) the business was shown to be dependant on the use of IT. It was confirmed that financial, tax and other personal and sensitive information form part of the daily business use and is handled through the use of IT. The partner and owner of the auditing firm were interviewed after selecting the organisation with the IT-dependency tool.

d) **Organisation 4:** Finance and business services

This organisation employs 15 people and operates in the advertising industry of Gauteng, as well as in the rest of Africa. The organisation indicated the daily use of information technology as well as the dependency of the business on IT. Some of the services rendered are based on e-commerce and a number of other business processes supported by the use of information technology. It was also noted that a big portion of the company revenue is earned through IT, including e-commerce and online advertising. The senior manager, who reports directly to the owner of the business, was interviewed after selecting the organisation with the sampling tool.

4.4 Analysis approach: information security awareness

Chapter 3 explained how information security awareness is to be measured by making use of the suggested conceptual model approach. This conceptual model includes the use of bounded rationality and planned behaviour as part of the measurement of awareness. The information and technology component is included by the self-categories identified in Chapter 2. These self-categories for supporting the research question and research intent include the following:

1. Information and technology as part of the business
2. Business financials
3. Information and technology failures
4. Passwords
5. Phishing and cyber security:
6. Software and business IT applications:
7. Personal and sensitive information:

In Chapter 2 the use of self-categories was explained by which themes and topics are drawn from the literature and the researcher’s interviewing experience; Chapter 3 furthered this approach by incorporating the use of these self-categories in the research instruments. By including these self-categories in the research tool, a conceptual approach is created for measuring information security awareness in the small business organisations.

Setting the research questions in a specifically formulated manner will supports this and this will be in accordance with the research instruments to measure the information security awareness and other IT-security related aspects of the small business organisations. As defined in the theories of 'bounded rationality and planned behaviour' in Chapter 2, the following three factors will be used to analyse awareness in the businesses:

- Knowledge
- Behaviour
- Attitude

To measure information security awareness in the small business organisations these three factors are used as part of the self-categories of interview questions. The measurement of awareness will assist in answering one part of the research question and will support the research objectives.
ATLAS.ti^{TM} was used to distinctly 'theme' the data towards interpreting the meaning. In-Vivo codes is drawn from interpretation for interpretation.

4.5 Other data measurements and self-categorising of data

Following the measurement of the information security awareness, the analysed qualitative data can be interpreted further. The qualitative results that were obtained will firstly be used when explaining the ratings for each of the self-categories.

Other evidence obtained during the interview, apart from the information security awareness elements, should also be used in the research study. In Chapter 5 the analysis of the data is presented, where the categories and the relationship between the self-categories are described.

The evidence gathered will be grouped according to 'self-categories', as described in Chapter 3 where the categories were derived from the literature. The grouping of results according to the self-categories will make it easier to analyse and interpret the data that was gathered, as stated in the design of the research instrument.

4.6 ‘Unitising’ of data

The research instrument in Chapter 3 described how the data that is recorded during the interviews would be transcribed ‘verbatim’, along with some additional notes on the interview and some particular observations. The purpose of this is to keep the data as accurate as possible once the analysis process is started.

The analysis of the qualitative data will be done using the “Categorising of data” technique, by which raw in-vivo quotes will be attached to categories that are formulated from the data itself, as well as from the conceptual models approach (Saunders et al., 2009:492). The development of the categories will be from the raw data and have to be supported by the conceptual approach that is followed to help answer the research questions. The categories for interpreting the qualitative data are different form the self-categories that were drawn from the literature to help guide the research instruments.

When grouping the data, the “analytical process of unitising data takes place where a unit of data”, in this case any data recorded and captured during the interview, is “grouped” according to the categories that have been derived (Saunders et al., 2009:493). The raw data or ‘in-vivo’ data is what is to be attached to the derived categories that were obtained from the living participant in their “natural setting” (Dictionary.com, Collins English Dictionary, Unabridged, 2009). The In-vivo data would thus be the data obtained from the actual living participant in their own environment of the small business organisation in Gauteng.

The raw data will be used for the analysis and grouping of the units of data that is collected. This approach is used in accordance with the design of the research instrument that is used to measure the information security awareness of the small IT-dependent business organisations of Gauteng.

The units of data will be analysed with the approach mentioned in section 4.3: Measuring information security awareness. By measuring the knowledge, attitude and behaviour of the participants from the units of data, the information security awareness of the small business organisation can be measured and better understood.

The categories with units of data attached will form part of each of the self-categories, which contains information about the participant’s and organisations knowledge, attitude and behaviour regarding the subject of discussion. Other rich qualitative information will also be captured and analysed to help answer the research question and achieve the research objectives.

4.7 Discussion

Following the explanation of the analysis technique: the categorising of data through 'unitising of data', the discussion on the results obtained can be made. The discussion is separated into the self-categories that were used to drive the interviews, which all contained elements of information security awareness needed to help answer the research question. The self-categories were obtained from the literature in Chapter 2 and used during the data gathering, to be analysed and discussed to help understand the research problem and solve the research question.

The analysis of the results obtained will begin in the next section. Quotations from the interviews will form part of the analysis for external validity purposes and as proof of the research results that are obtained. The previous section explained how the unitising of data is used as reliability for the use of the data that was obtained using the selected research instruments. Variables affecting one another can then be identified as casual relationships to help support the evidence that was obtained. This can then be elaborated upon in the next chapter where the findings and discussion take place.

4.8 Awareness of Technology Dependency (IT as part of the business)

All interviewees from the five sampled small organisations agreed and confirmed that they make use of Microsoft^{TM} and Microsoft Office^{TM} related products in the business. The interviewees also acknowledged that they are IT dependent, with the strongest dependency being in the area of financial reporting, such as accounting packages, payroll and online payment solutions. Pastel^{TM} was the most commonly mentioned software package used by these small organisations, while two interviewees mentioned VIP^{TM} as the preferred payroll solution. An interviewee from Organisation 1 explained that Pastell^{TM} and VIP Payroll^{TM} are used in conjunction with online banking applications.

Outside of the reliance of vendor-based software, an interviewee from Organisation 2 specified that their small organisation also makes use of customised software applications that are tailored to their own specific business needs. The interviewee (owner) expressed the dependency of this tailored software solution as follows:

> "Software that is specifically written in-house [is] everything!"

The interviewee from Organisation 3 confirmed that their small organisation uses accounting Caseware^{TM}, Pastel^{TM} and Pastel Payroll^{TM}. Interviewees from organisations 4 and 5 both confirmed the use of Microsoft^{TM} and Pastell^{TM}. The interviewees responded positively to the idea that information technology brings change to the organisation and that such change is welcomed and supported. The perceptions of changes, as explained by the interviewees, include anything from the automation to improvements of business processes using information technology. The responses included:

> *"yes definitely"; and*

> *"we really support the change information technology brings to the business."*

Two participants indicated that 'cost savings' and 'time savings' were drivers for change in the small business organisations. Interviewees from organisation 1 and 3 expressed some concerns regarding the IT change and the ability for the small organisations to keep up with the changes. Interviewees from both these organisations also suggested that the migration to new external applications caused disruptions that they were uncomfortable with, such as the following response from one interviewee:

> *"the SARS system that keeps changing is a nightmare."*

All interviewees where able to articulate their understanding of the IT business needs and were able to describe the business processes, operations and tools that are used by the small organisations. All of the respondents confirmed that their financials (accounting and reporting) are done using information technology driven systems. One interviewee articulated this as follows:

> *"Our entire business is dependent on information technology! From sales to marketing to client communications."*

Interviewees also expressed concern that such dependency and use of technology also brings unintended consequences, such as disruptions and integration or interoperability issues. An interviewee from Organisation 1 illustrated one such process failure as being attributed to a 'compatibility' issue that was not anticipated:

> *"…exactly what happened today… I will introduce a certain program and maybe it's a newer version and then it's not compatible to old versions…."*

4.9 Awareness of Risk, Trust and 3rd-Party IT Service Providers

Regarding the need for small organisations to back up data, organisations 1, 2 and 4 reported that the back up of data is done at least weekly for data from critical business operations. It was explained by the interviewees from these small organisations that the contracted 3rd-party IT vendors mostly handled the back ups. However, an interviewee from Organisation 2 mentioned that additional daily back ups are taken by employees of that organisation. Interviewees from organisations 1, 2 and 4 also confirmed off-site storage of back ups by 3rd-party IT vendors. Incidentally, interviewees from organisations 3 and 5 indicated that back ups are not mandatory practice and are only "advised to employees".

An interviewee from Organisation 2 gave the example of a backup that was not made for two months, and when a failure occurred, the small business organisation lost two months of work. The failure and loss of business information was devastating to the organisation with the interviewee (business owner) stating that the business has not been able to fully recover since the occurrence. Some of the interviewees' responses were as follows:

> *"I don't want to tell you how much two months is in this company! We service over 300 cars a month. It was a nightmare!"*
>
> *"I lost everything! [I'll] never be able to catch-up on everything!"*

This scenario was replicated in Organisation 3, as the interviewee described a scenario where a failure in business IT happened because of accidental damage to the backup disk brought about by careless handling, as the interviewee explained:

> *"My clerk dropped [the] back up [disk]! Now I cannot restore and the data is lost!"*

The loss of information caused a lot of disruption to the business and the interviewee (owner) further explained how the information was critical to the trading and repairing of motor vehicles. The dependency of information technology in the small business organisation was again emphasised by the interviewee.

In the aftermath of this event, the interviewee acknowledged that measures were taken to contract a 3rd-party vendor to resolve the problem. Three interviewees indicated that their organisations contract 3rd-party IT-vendors who are responsible for the maintenance and repair of the company's information technology. The 3rd-party vendors are specifically contracted to assist with back ups and restorations from systems failure.

Two interviewees indicated that they do not contract 3rd-party IT-vendors and take it upon themselves to act on restorations from systems failure when these arise. Systems failures that exacerbate business risks that were mentioned during the interviews include failures in business e-mail, internet connection, VOIP telephones, loss of data or information as well as failures in business specific IT-application software.

4.10 Awareness of Handling and Archiving Data (Business Financials)

An interviewee from Organisation 2 (vehicle trade and repairs) described a situation where large amounts of personal and sensitive information is handled as part of daily business operations and there is no specific policy that addresses how such data is to be handled or archived as soon as the organisation is done processing the data. The data is archived both electronically and in a hard-copy format. The interviewee described the kind of personal and sensitive data handled and archived by the company as including:

> *"ID, drivers [licences], payslip, bank statements, proof of residence, electronic signature and other regulatory required information"*

Furthermore, the interviewee (owner from Organisation 2) explained that there is a regulatory requirement that information handled by the small organisation must have an archive and retention period of a minimum of ten years, as required by law. The respondent explained:

> *"Hard copy files are required by the law to be kept for 10 year! Not 5 year anymore! I have to keep that file for 10 years….so it has to be kept securely for 10 year..."*

An interviewee from Organisation 1 also mentioned that most of the personal and sensitive information is firstly captured by hard copy because of "*some of their clients lack of access to information technology*". Hard-copy files are retained until captured electronically and then archived. The interviewee described such information as including:

> *"tax numbers, UIF numbers, full names and addresses, company names and registration details"*

4.11 Awareness of Online Banking (Business Financials)

Online banking was selected as a starting point to understand and assess awareness levels and attitude of the interviewees regarding common threats that abound through the use of online banking. When asked about their experiences regarding the use of online banking facilities, none of the interviewees of the small organisations expressed concerns regarding the use of online banking. Further probing revealed that the interviewees did not have sufficient understanding of the inherent risks associated with online banking. The discussions highlighted a concern that there were minimal controls in place to address security risks. What was generally accepted by a majority of the interviewees was that online banking provided "*inherent benefits*" while having an ability to "*integrate with the business applications*".

It was revealed that the small organisations were primarily dependent on the banks to provide the necessary assurance and the guarantees regarding security. There was no indication that the small organisations were proactive. An interviewee from Organisation 1 explained that they are satisfied with the way the online banking authentication codes are changed on a monthly basis:

> *"Our codes change every month, you change your codes and there is two sets of codes to change, and there is approval that you have to do."*

An easy way out of the entire confusion and worry about risks, as explained by an interviewee from Organisation 3, is that of restricting online banking or doing away with it entirely:

> *"restricting access to the online banking"; [*because]
>
> *"enough comfort exists over the possible risks".*

Interviewees from Organisation 2 and 4 both indicated no concerns regarding the use of online banking, however, both stated that they were aware of the possible risks. The nature of risk that they seem to agree on is:

> "*loss of financials*"

4.12 Awareness of Phishing

Interviewees from all sampled small organisations confirmed that they had in the past received phishing requests via e-mail and that personal and sensitive information was asked for. Most confirmed that they would not respond to a possible phishing e-mail requesting online banking information. An interviewee (owner) from Organisation 2 acknowledged recognising common forms of phishing and admitted to being a constant target. The interviewee has on several occasions received a large number of phishing e-mails. The interviewee has taken the liberty of proactively sending out e-mails to all other employees warning them about the risk of responding to phishing and other malicious e-mails, as he expressed:

> *"[I] sent [out] e-mail to all the staff that they don't touch it!"*

One of the interviewees (co-owner) from Organisation 1 gave a specific example of a phishing related request that the small business has experienced in the past. The participant acknowledged not responding, as he identified that it was not genuine. The interviewee explained:

> *"I received one this week of somebody that states you must reply and contact the bank because there is a cheque paid into your account that has not been cleared. I went into my bank account and saw that there is no other money that I know about."*

The interviewee form of Organisation 2 (owner) explained that he occasionally creates awareness amongst his employees in the small business when phishing scenarios present themselves:

> *"If I get something like that I remind the employees not to respond."*

An interviewee from Organisation 1 also confirmed that employees are made aware of the risks of phishing. However, this, as he seemed to suggest, was made verbally:

> *"I just said to them, ignore it!"*

An interviewee from Organisation 3 pointed out that there is no awareness initiative in place to warn employees about the threats and risks that exist around phishing. When probed further about the dangers of phishing, the interviewee responded as follows:

> *"If the employees click on the links [on the email], it's their own problems. Then it would be their work that is affected."*

> *"I haven't spoken to them about it and if they are stupid enough to fall for it they have to learn from it."*

Interviewees from organisations 4 and 5 acknowledged that they are unaware of policies that exist in their small businesses regarding sensitising them or making them aware of the possible risks of phishing.

4.13 Awareness of Personal and Sensitive Information

It emerged from the interview sessions that most organisations do not have a rigid approach to how personal and sensitive information is stored and accessed. An interviewee from Organisation 3 confirmed that business and customer information is stored on individual laptops, backup drives, hard-copy files and other available information storage mediums on the business premises or owned by the business, as the interviewee expressed:

> *"There is no specific place, it's mostly company information and we store it everywhere."*

The same interviewee (Organisation 3 owner) also stated that the small business had restricted access to hard-copy personal and sensitive information kept in locked filing cabinets, but that is electronically accessible to all the employees of the business.

> *"Hard copy information gets stored in the cabinet behind here… that can be locked…this information is also electronically available on the system…"*

> *"…everybody has access to the information…the business is so small so everybody that works here [and needs] the information every day [gets it]… In a bigger business I guess there would be a risk… personal information of the employees is stored in my office..."*

The interview process revealed differences in how the small organisations treat personal information. An interviewee from Organisation 2 seemed distraught that a section of employees inadvertently accessed certain information that they were not privy to:

> *"I cannot have my sales people look at my information! I should never have had them look at all of that information! Sales people must sell!*

None of the interviewees suggested that they have 'lost' any of their own personal and sensitive information. All interviewees agreed that they have not experienced the abuse of personal and sensitive information in their organisations.

Interviewees from three organisations (organisations 1, 2 and 4) confirmed that their organisations use a server to centrally store the business and customer information. The interviewees also stated that their vendors keep a backup of the data stored on the central server. From the interviews it was ascertained that access to the central server is, however, restricted. Access to the central server for these three organisations is only given to specific employees in the business organisation:

> *"to prevent the abuse of this information that is electronically or physically stored"*

One of the reasons given by an interviewee for restricting access is that the employers understand the premium that this kind of information holds:

> *"[I] restricted access was because of the possible abuse of the information that is kept by the company [such as] selling of information to the competition."*

> *"[I] discourage [this to] sales staff…because of access to information detailing profitability of car sales."*

4.14 Awareness of Password Use

Interviewees from organisations 1, 2, 3 and 5 seem to have established that their representative small organisation has slack policies regarding passwords. An interviewee from Organisation 3 even suggested that they do not enforce the policies. When asked why there was this slack attitude towards passwords, an employee from Organisation 1 responded as follows:

> *"We started with passwords on individual computers, but I asked them to remove it because it's just a nuisance."*

Interviewees from organisations 1, 2 and 3 confirmed that access to the server was restricted by passwords. Interestingly, only one of the small organisations sampled consistently enforces the use of passwords on employee computers.

4.15 Responsiveness to Protection of Data/Information

An interviewee from Organisation 2 reported that they make use of an anti-virus and firewall software and password protected Wi-Fi access. As the interviewee explained, this resulted from a previous incident in the organisation where a virus infected systems as a result of compromise from the organisation’s Wi-Fi systems. The interviewee explained:

> *“The neighbours where downloading from our Wi-Fi!! We stopped it and added a password to the Wi-Fi.”*

4.16 Awareness of Illegal Software (Software and business IT applications)

An interviewee (co-owner) from Organisation 1 explained that no illegal software is used in the small organisation. The interviewee also explained that the small organisation has had a software audit in the past; as was explained:

> *“About three or four years ago we got a software audit on that.”*

The interviewee explained that the software audit gave the small business motivation not to ever make use of illegal software as part of its business operations. It also emerged that software audits were not the only motivations that dissuaded small businesses from using illegal software. The emergence of sophisticated anti-piracy techniques were highlighted as others forms of motivation. An interviewee from Organisation 3 revealed that the small organisation had:

> “*…illegally made use of an accounting software solution.*”

The highlighted enterprise was cut short by modern anti-piracy techniques:

> *“…forcing [us] to purchase [our] own licensed copy.”*

The interviewee form Organisation 3 (owner) provided a justification as to why they previously made use of illegal software in their business while articulating some distress with the modern security techniques that make it more difficult for them to make use of illegal software:

> *“These days [software owners] make a license that you need to have [beforehand], making it difficult. With Pastel you get a new code every year, so if you don’t renew your license fee you can’t use the program or support.”*

The interviewees from organisations 2 and 4 seemed not to be faced with this problem and assured the interviewer that their organisations have policies that prevent the use of illegal software “*on work computers*”*.* Further prodding revealed that Organisation 2 routinely performed spot-checks on employee computers. Upon the commencement of employment, the employees are required to sign a contract permitting these checks, as highlighted by the interviewee (owner):

> *"My IT-guy comes in and [conducts] a spot check here and there on the computers… and the employees sign a letter [stipulating] anytime can that IT-guy come in and go onto their computers."*

The interviewee from Organisation 2 expressed his approach towards strict deterrence on using illegal software on the business-owned computers by stating:

> *"We have nothing as such! I'll kill someone if he does that."*

Incidentally, within the same breath, the interviewee acknowledged having certain blind-spots concerning the activities his employees perform on their work computers:

> *"…If you ask me… if my employees are doing things on their computers, how would I know? I don't always look at their things; I don't know what they do on their computers… I'm sure if they are downloading illegal stuff my IT-guy would pick it up..."*

4.17 Awareness of Anti-virus Software Use

The use of anti-virus software is generally regarded as being very important among all interviewees of the sampled small organisations, confirming that they use anti-virus software on their work computers. Most interviewees claimed to have up-to-date software - with the exception of the interviewee from Organisation 3 (owner) - who revealed that the copy used on the premise has expired:

> *"Yes [we have] but it's outdated. Mine is expired and I have to get it updated."*

The fact that the small organisation was using outdated anti-virus software did not constitute a big issue for the owner. It was further revealed that organisations 3 and 5 did not have a specific IT-vendor that looked after the company's information technology assets, particularly with regards to the deployment of and constant monitoring of the anti-virus software. However, interviewees from organisations 1, 2 and 4 revealed that their organisations contract 3rd-party IT-vendors whose duties include, amongst other things, keeping the anti-virus software updated.

Above and beyond the need for up-to-date anti-virus software, the interviewees from organisations 1, 2 and 4 also mentioned that their organisations make use of firewall software for additional information protection. These interviewees also mentioned that the protection of the company's information technology assets are maintained by the same vendors responsible for updating their anti-virus software and other information security solutions. The interviewees from both 0rganisation 3 and 5 reported that no additional information security practices are carried out in their organisations, besides that of having anti-virus software solutions.

4.18 Awareness of Physical Security

Regarding physical controls implemented by the small business organisations relating to the protections of assets, an interviewee from Organisation 2 explained that the office premises of the organisation are kept locked outside of business hours and that alarms are utilised. In addition, the organisation has contracted a security company that is constantly on patrol. The interviewee (owner of Organisation 2) also explained that the server is locked in a secure room with an air conditioner. He confirmed that there has never been an incident regarding the theft of information technology:

> *"…we've been lucky; no one has ever broken in and stolen our computers and other equipment."*
>
> *"…we are extremely lucky..."*

An interviewee from Organisation 1 explained that only two employees from the small organisation have keys to unlock the office where the server and important documents are kept. He further explained that the rest of the employees are only issued with a remote control to open the front gates of the premises. The interviewee, however, expressed some anxiety over the physical security of the business assets, given the pattern of theft and robberies that have been reported around the neighbourhood:

> *"Physical security [around protecting our server] is a bit of a luck…"*

Interviewees from the rest of the small business organisations' sample also mentioned that their premises are equipped with security gates and alarms to protect their business premises and IT-assets stored on-site. They did, however, express concern around the physical protection of their information technology assets. The interviewee from Organisation 4 articulated this anxiety by referring to a report of robberies that have taken place in their office block and by explaining that information and technology assets belonging to another business organisation have been stolen:

> *"…there was a break-in here on Monday! Not in our office, but in the same building again!"*
>
> *"…they came to the photo studio next door and wiped them out! And on this floor is a private school with about 40 computers that was uninsured, which got stolen!"*

Chapter 5

`

The analysed results have now been documented and studied, with a large number of anticipated as well as unanticipated results obtained. In this Chapter, the findings will be discussed by measuring the information security awareness from the results. The information security awareness is measured using the knowledge, attitude and behavioural results obtained and analysed.

Chapter 5

Findings and Discussions

5.1 Introduction

By studying the analysed results from the previous chapter, the findings can be written along with the discussions around the research findings.

References shall be made to the design of the research tool, as presented in Chapter 3, when explaining the need for the self-category, specific questions and information security awareness. The Literature from Chapter 2 will be incorporated into the findings made in the conclusion in Chapter 6. Chapter 6 will also be used to make suggestions and conclude on the findings chapter and research question. The specific research objectives will be discussed in this chapter and the research question answered.

5.2 Self-categories and the research findings

Following the discussion of the results from each of the self-categories, the overall findings of the information security awareness can be given along with the other researcher's observations that were made during the study of the small IT-dependent business organisations in Gauteng, South Africa.

A discussion will be made on the findings of all the self-categories and the research results that were documented in Chapter 4. These discussions will be used when looking at the information security awareness of the participant small business organisations.

The self-categories were used to guide the research interview as well as the underlying topic of information security awareness in the small IT-dependent businesses of Gauteng. In the interpretation of the analysed research results, the results obtained from the self-categories will be appended and analysed as a whole.

5.3 Coding of Research Results

In the design of the research instrument it was suggested that the results obtained will be coded and categorised to interpret the analysed results. Literature describes the "categorising of data" as the "development of categories and attaching these categories to pieces of analysed data" (Saunders et al., 2009:492). In Chapter 3, where the instrument was designed, it was also explained how the qualitative analysis approach of coding and categorising would be the most appropriate for in-depth interviews.

The following section will begin by identifying codes from the responses, which will then be categorised and interpreted. All of the responses analysed and documented in Chapter 4 will be used for coding and categorising. This will be done across all the self-categories used to guide the interview, as well as the additional results obtained and analysed.

5.4 Final Interpretation

In the final interpretation, the questions and responses obtained in the results analysis will be placed in the tables below. The responses will also include the results obtained by using probing techniques or additional results obtained besides those directly relating to the pre-determined questions. These will be referred to as the 'topic' that was under discussion during the interview for which there was not necessarily a set question, but a response was nevertheless obtained.

From the responses, codes will be derived using the conceptual model as a guideline. Various other techniques will also be used to derive the codes that will be used to build the categories obtained from the research results. These include the "terms captured from the data, actual terminologies used by the respondents and terms derived from existing theories and literature" (Saunders et al., 2009:240).

Finally, Categories will be developed from the derived codes.

Awareness of Technology Dependency (IT as part of the business)

No:	Question / Theme	Response	In-vivo Codes	Categories
1	Do you see yourself as being dependent on software applications?	*“Software that is specifically written in house [is] everything!”*	*everything* *dependency*	IT-dependency
2	Do you support the change that information technology brings to your business organisation?	*“yes definitely’; and “we really support the change information technology brings to the business because…”* *‘the SARS system that keep on changing’ is a nightmare”*	*Support for change* *nightmare*	IT acceptance Resist system changes
3	Describe the business processes you would consider dependant on information technology?	*“Our entire business is dependent on information technology! From sales to marketing to client communications”*	*entire business* *dependent*	IT-dependency
4	How would you respond to a failure of Information Technology in a critical business process? Past failures:	*“Exactly what happened today… I will introduce a certain program and maybe it’s a newer version and then it’s not compatible with the old versions”*	*introduce a certain program* *nightmare*	Change failure Examples of failure Hard copy and digital storage of information

Table 5.4.1

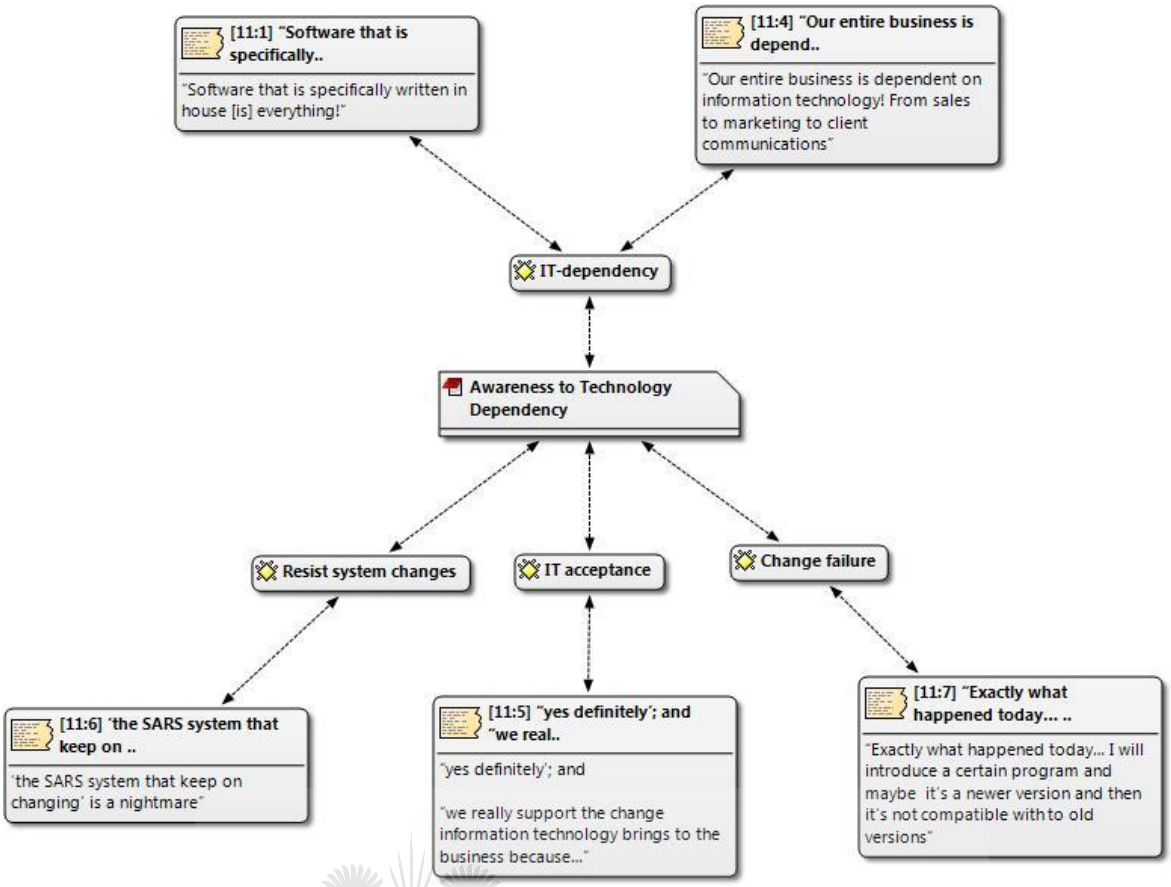
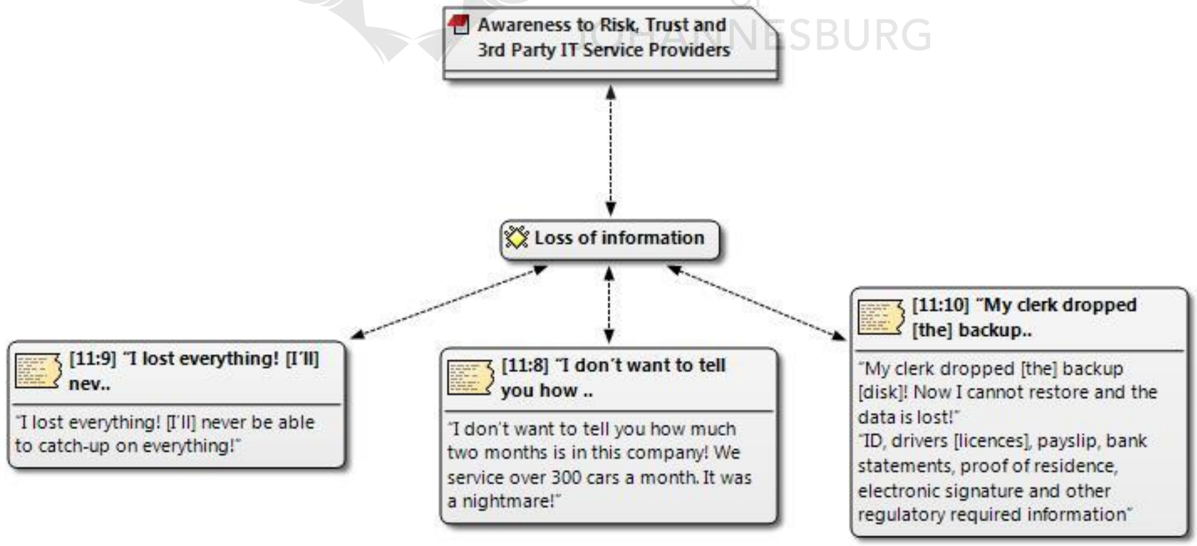

[11:1] "Software that is specifically..
"Software that is specifically written in house [is] everything!"
[11:4] "Our entire business is depend..
"Our entire business is dependent on information technology! From sales to marketing to client communications"
IT-dependency
Awareness to Technology Dependency
Resist system changes
IT acceptance
Change failure
[11:6] 'the SARS system that keep on ..
'the SARS system that keep on changing' is a nightmare"
[11:5] "yes definitely'; and "we real..
'yes definitely'; and
"we really support the change information technology brings to the business because..."
[11:7] "Exactly what happened today... ..
"Exactly what happened today... I will introduce a certain program and maybe it's a newer version and then it's not compatible with to old versions"

Figure 5.4.1

The table and figure above show the interpreted results from the first self-category that was used to introduce the research topic and what is required from the participants during the interview. A number of categories were derived from the quoted 'in-vivo' results that were analysed. Each of the table and figures to follow will include the individual question or theme along with its quoted responses, followed by the drawn in-vivo codes and derived categories.

Awareness of Risk, Trust and 3rd Party IT Service Providers				
No:	Question / Theme	Response	In-vivo Codes	Categories
5	Has there been a loss of information in the business?	*"I don't want to tell you how much two months is in this company! We service over 300 cars a month. It was a nightmare!"* *"I lost everything! [I'll] never be able to catch-up on everything!"*	*nightmare* *lost everything*	Loss of information
6		*"My clerk dropped [the] backup [disk]! Now I cannot restore and the data is lost!"*	*Cannot restore* *Data is lost*	Loss of information

Table 5.4.2


Awareness to Risk, Trust and 3rd Party IT Service Providers
Loss of information
[11:9] "I lost everything! [I'll] nev..
[11:8] "I don't want to tell you how ..
[11:10] "My clerk dropped [the] backup..

"I lost everything! [I'll] never be able to catch-up on everything!"

"I don't want to tell you how much two months is in this company! We service over 300 cars a month. It was a nightmare!"

"My clerk dropped [the] backup [disk]! Now I cannot restore and the data is lost!"
"ID, drivers [licences], payslip, bank statements, proof of residence, electronic signature and other regulatory required information"

Figure 5.4.2

The second self-category responses from the table and figure above look at the 'Awareness of Risk, Trust and 3rd Party IT Service Providers' of the participant small business organisations. The loss of information was a strong theme that emerged, with a number of quoted results. The following section of the findings and discussions will elaborate on these results.

Awareness of Handling and Archiving Data				
No:	Question / Theme	Response	In-vivo Codes	Categories
7	What information is stored by the business?	*"ID, drivers [licences], payslip, bank statements, proof of residence, electronic signature and other regulatory required information"* *"tax numbers, UIF numbers, full names and addresses, company names and registration details"*	*ID, electronic signature, bank statements, payslip, drivers* *Company details*	Personal and sensitive information
8	Where is the information stored?	*"Hard copy files are required by the law to be kept for 10 year! Not 5 year anymore! I have to keep that file for 10 years....so it has to be kept securely for 10 year..."*	*Hard copy files* *Kept securely for 10 years*	Hard copy and digital storage of information

Table 5.4.3

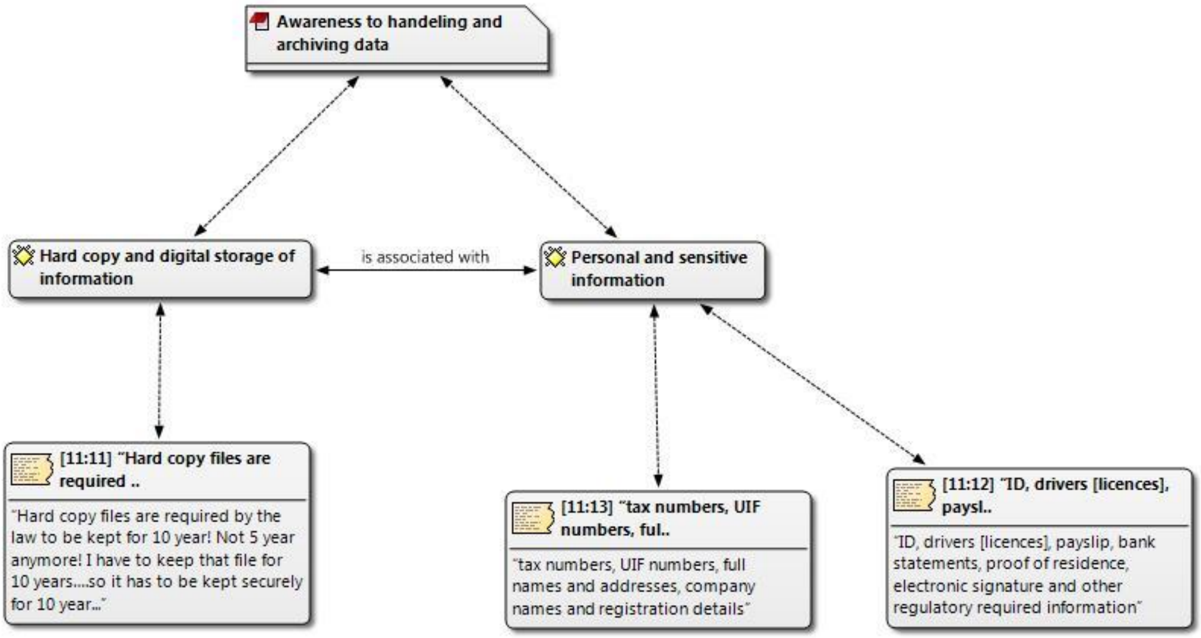

Awareness to handeling and archiving data
Hard copy and digital storage of information
is associated with
Personal and sensitive information
[11:11] "Hard copy files are required ..
"Hard copy files are required by the law to be kept for 10 year! Not 5 year anymore! I have to keep that file for 10 years....so it has to be kept securely for 10 year..."
[11:13] "tax numbers, UIF numbers, ful..
"tax numbers, UIF numbers, full names and addresses, company names and registration details"
[11:12] "ID, drivers [licences], paysl..
"ID, drivers [licences], payslip, bank statements, proof of residence, electronic signature and other regulatory required information"

Figure 5.4.3

The table and figure above follows and expands on the previous discussion by looking at the awareness of handling and archiving data in the business. Two main categories are derived that are supported with quoted evidence and further discussed in the next section of the chapter.

Awareness of Online banking (Business financials)

No:	Question / Theme	Response	In-vivo Codes	Categories
9	Do you think there is a risk for your organisation to use online banking?	*"Our codes change every month, you change your codes and there is two sets of codes to change, and there is approval that you have to do."* *restricting access to the online banking"* *enough comfort exists over the possible risks*	*Change codes* *Restrict access* *Comfort over risks*	No risk concern Restricted access
10	The inherent risk agreed on	*loss of financials*	*Loss*	Loss of financials

Table 5.4.4

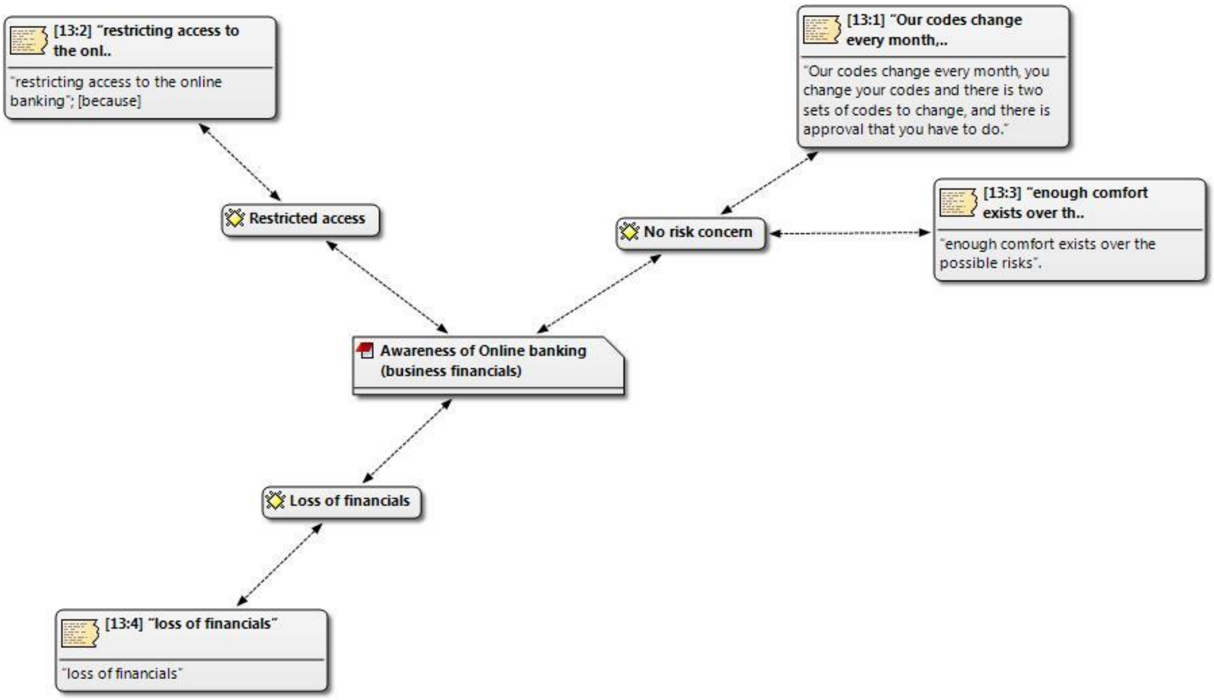

[13:2] "restricting access to the onl..
"restricting access to the online banking"; [because]
[13:1] "Our codes change every month,..
"Our codes change every month, you change your codes and there is two sets of codes to change, and there is approval that you have to do."
Restricted access
No risk concern
[13:3] "enough comfort exists over th..
"enough comfort exists over the possible risks".
Awareness of Online banking (business financials)
Loss of financials
[13:4] "loss of financials"
"loss of financials"

Figure 5.4.4

The table and figure above show the results around online banking and the use of online banking in the small business organisations. Again, a number of categories are drawn from the quoted evidence that was recorded during the interviews. The next section of Chapter 5 will elaborate and discuss the categories and identified relationships.

Awareness of Phishing				
No:	Question / Theme	Response	In-vivo Codes	Categories
11	How would you respond to a phishing e-mail?	*"[I] sent [out] e-mail to all the staff that they don't touch it!"* *"I received one this week of somebody that states you must reply and contact the bank because there is a cheque paid into your account that has not been cleared. I went into my bank account and saw that there is no other money that I know about"*	Don't respond Received one this week	Phishing awareness Ability to identify phishing
12	How is awareness created around phishing in the business?	*"If I get something like that I remind the employees not to respond"* *"I just said to them, ignore it!"*	Remind employees Not to respond Ignore it	Phishing awareness Ability to identify phishing
13	No awareness created around phishing in the business	*"If the employees click on the links [on the email] it's their own problems. Then it would be their work that is affected"* *"I haven't spoken to them about it and if* they are stupid enough *to fall for it they have to learn from it"*	Their own problems Their own work affected Haven't spoken to them Stupid enough to fall for it, learn from it	No phishing awareness initiatives

Table 5.4.5

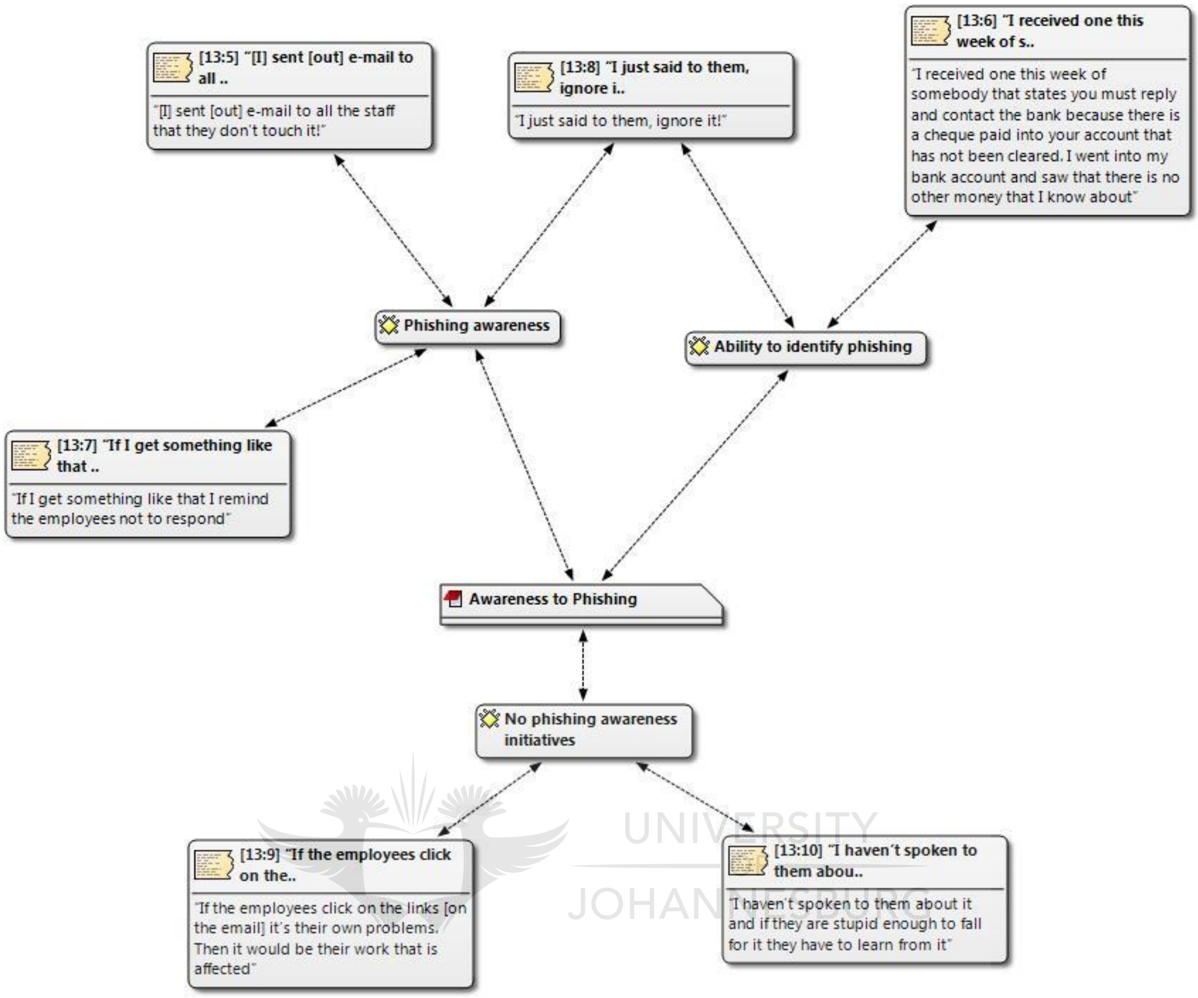

[13:5] "[I] sent [out] e-mail to all ..
"[I] sent [out] e-mail to all the staff that they don't touch it!"
[13:8] "I just said to them, ignore i..
"I just said to them, ignore it!"
[13:6] "I received one this week of s..
"I received one this week of somebody that states you must reply and contact the bank because there is a cheque paid into your account that has not been cleared. I went into my bank account and saw that there is no other money that I know about"
Phishing awareness
Ability to identify phishing
[13:7] "If I get something like that ..
"If I get something like that I remind the employees not to respond"
Awareness to Phishing
No phishing awareness initiatives
[13:9] "If the employees click on the..
"If the employees click on the links [on the email] it's their own problems. Then it would be their work that is affected"
[13:10] "I haven't spoken to them abou..
"I haven't spoken to them about it and if they are stupid enough to fall for it they have to learn from it"

Figure 5.4.4

The awareness of phishing in the business organisations is explained in the table and figure above. A number of categories with relationships from the quoted responses are shown. The next section will elaborate on these categories and identified relationships from the analysed results.

Awareness of Personal and Sensitive Information				
No:	Question / Theme	Response	In-vivo Codes	Categories
14	Where is the information stored in the business?	*"There is no specific place, it's mostly company information and we store it everywhere"* *"Hard copy information gets stored in the cabinet behind here… that can be locked…this information is also electronically available on the system…"*	No specific place, everywhere Hard copy information	Hard copy and digital storage of information
15	Who can access the information?	*"…everybody has access to the information…the business is so small so everybody that works here [and needs] the information every day [gets it]… In a bigger business I guess there would be a risk… personal information of the employees is stored in my office..."* *"I cannot have my sales people look at my information! I should have never have had them look at all of that information! Sales people must sell!*	Everybody has access in the business Cannot have my sales people look at the information	Access to business information No information security Restricted access
16	Why restrict access to information?	*"to prevent the abuse of this information that is electronically or physically stored"* *"[I] restricted access because of the possible*	*prevent abuse of information* *restrict*	Abuse of information concerns Restricted access

		abuse of the information that is kept by the company [such as] selling of information to the competition” *“[I] discourage [this to] sales staff…because of access to information detailing profitability of car sale”*	*access* *selling of information to the competition* *Discourage access to information*	

Table 5.4.5

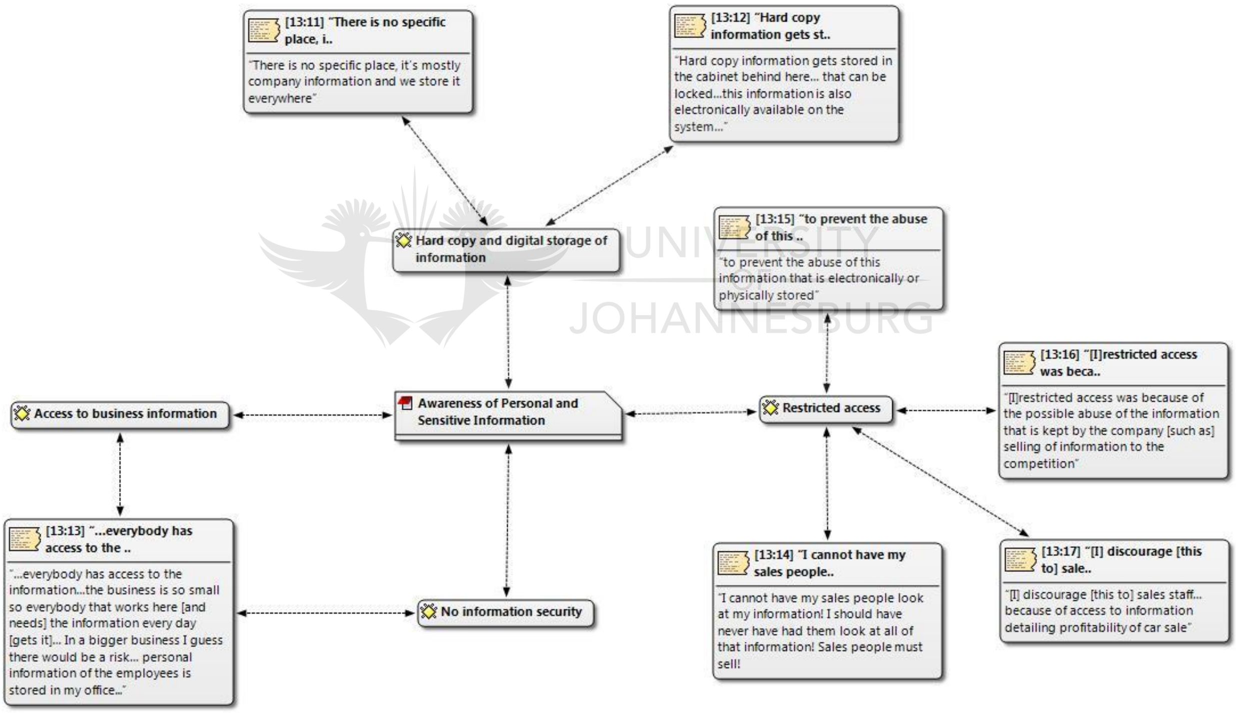

[13:11] "There is no specific place, i..
"There is no specific place, it's mostly company information and we store it everywhere"
[13:12] "Hard copy information gets st..
"Hard copy information gets stored in the cabinet behind here... that can be locked...this information is also electronically available on the system..."
Hard copy and digital storage of information
[13:15] "to prevent the abuse of this ..
"to prevent the abuse of this information that is electronically or physically stored"
[13:16] "[I]restricted access was beca..
"[I]restricted access was because of the possible abuse of the information that is kept by the company [such as] selling of information to the competition"
Access to business information
Awareness of Personal and Sensitive Information
Restricted access
[13:13] "...everybody has access to the ..
"...everybody has access to the information...the business is so small so everybody that works here [and needs] the information every day [gets it]... In a bigger business I guess there would be a risk... personal information of the employees is stored in my office..."
No information security
[13:14] "I cannot have my sales people..
"I cannot have my sales people look at my information! I should have never have had them look at all of that information! Sales people must sell!
[13:17] "[I] discourage [this to] sale..
"[I] discourage [this to] sales staff... because of access to information detailing profitability of car sale"

Figure 5.4.5

Awareness of Password Use Awareness of Protection of Data/Information				
No:	Question / Theme	Response	In-vivo Codes	Categories
17	Does your organisation make use of passwords?	*“No”* *“We started with passwords on individual computers but I asked them to remove it because it’s just a nuisance”.* *“The neighbours where downloading from our Wi-Fi!! We stopped it and added a password to the Wi-Fi.”*	No Passwords just a nuisance Neighbours downloading from our Wi-Fi Stopped it and added password	Lack of passwords

Table 5.4.6

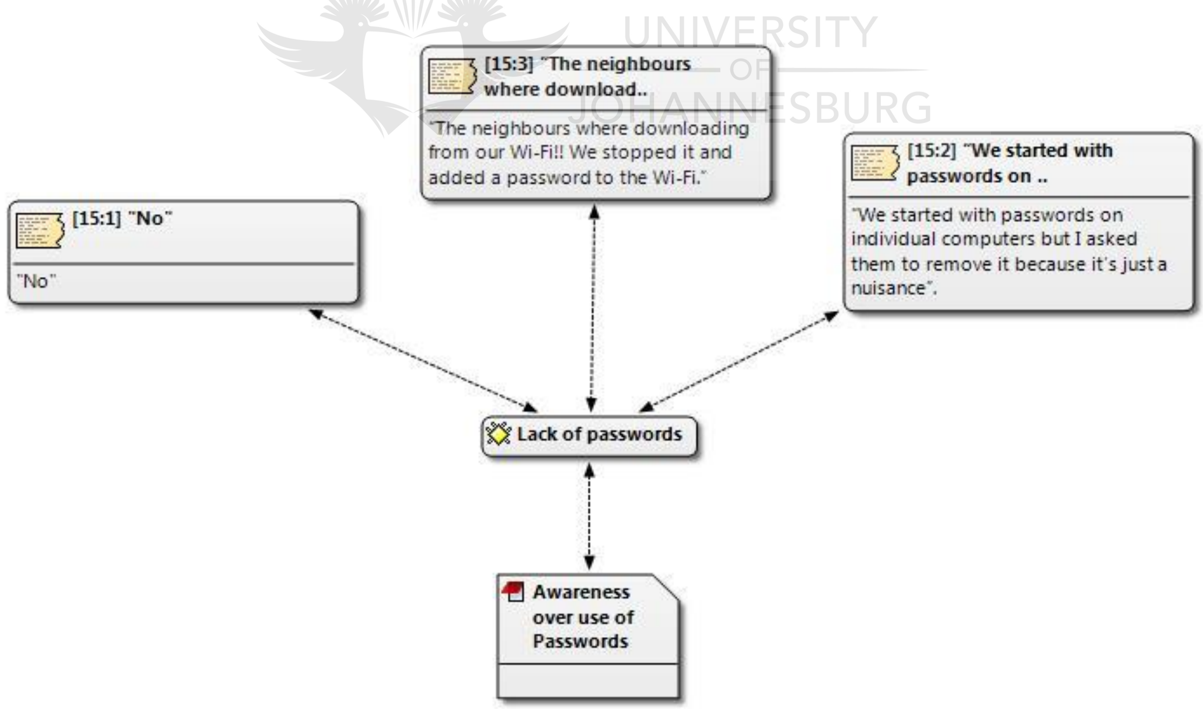

[15:3] "The neighbours where download..
"The neighbours where downloading from our Wi-Fi!! We stopped it and added a password to the Wi-Fi."
[15:2] "We started with passwords on ..
"We started with passwords on individual computers but I asked them to remove it because it's just a nuisance".
[15:1] "No"
"No"
Lack of passwords
Awareness over use of Passwords

Figure 5.4.6

Awareness of Illegal Software				
No:	Question / Theme	Response	In-vivo Codes	Categories
18	Does the business make use of illegal software?	*"About three or four years ago we got a software audit on that."* *"…illegally made use of an accounting software solution."* *"…forcing [us] to purchase [our] own licensed copy."* *"These days [software owners] make a license that you need to have [beforehand] making it difficult. With Pastel you get a new code every year so if you don't renew your license fee you can't use the program or support."*	Software audit *Illegally made use of software* Forcing to purchase license Software licenses	Illegal use of software Software license

19	Awareness of illegal software	*"My IT-guy comes in, and [conduct] a spot check here and there on the computers… and the employees sign a letter, [stipulating] anytime can that IT-guy come in and go onto their computers."* *"We have nothing as such! I'll kill someone if he does that."* *"…If you ask me… if my employers are doing things on their computers, how would I know? I don't always look at their things; I don't know what they do on their computers… I'm sure if they are downloading illegal stuff my IT-guy would pick it up…"*	Spot check Sign a letter Nothing as such How would I know what employees are doing	Prevention

Table 5.4.7

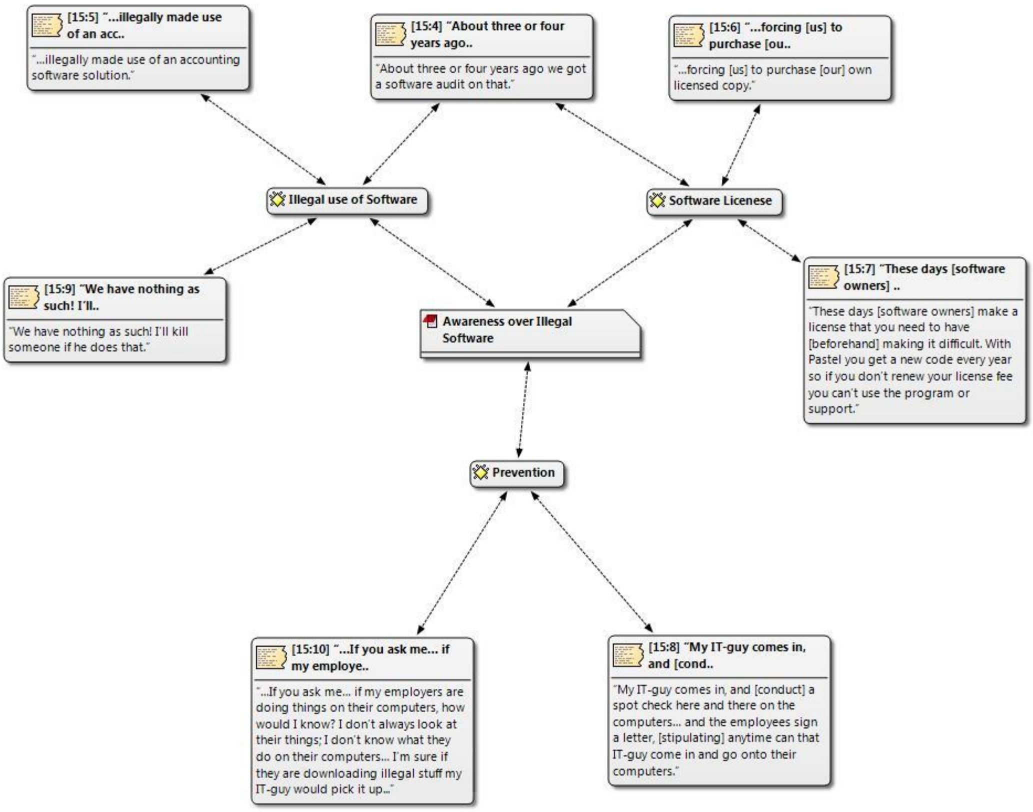

[15:5] "...illegally made use of an acc..
"...illegally made use of an accounting software solution."
[15:4] "About three or four years ago..
"About three or four years ago we got a software audit on that."
[15:6] "...forcing [us] to purchase [ou..
"...forcing [us] to purchase [our] own licensed copy."
Illegal use of Software
Software Licenese
[15:9] "We have nothing as such! I'll..
"We have nothing as such! I'll kill someone if he does that."
Awareness over Illegal Software
[15:7] "These days [software owners] ..
"These days [software owners] make a license that you need to have [beforehand] making it difficult. With Pastel you get a new code every year so if you don't renew your license fee you can't use the program or support."
Prevention
[15:10] "...If you ask me... if my employe..
"...If you ask me... if my employers are doing things on their computers, how would I know? I don't always look at their things; I don't know what they do on their computers... I'm sure if they are downloading illegal stuff my IT-guy would pick it up..."
[15:8] "My IT-guy comes in, and [cond..
"My IT-guy comes in, and [conduct] a spot check here and there on the computers... and the employees sign a letter, [stipulating] anytime can that IT-guy come in and go onto their computers."

Figure 5.4.7

Awareness of the Use of Anti-virus Software				
No:	Question / Theme	Response	In-vivo Codes	Categories
20	Do you make use of Anti-Virus software to protect your information technology?	*"Yes"* *"Yes [we have] but its outdated. Mine is expired and I have to get it updated."*	Yes Outdate	Outdated anti-virus Anti-virus

Table 5.4.8

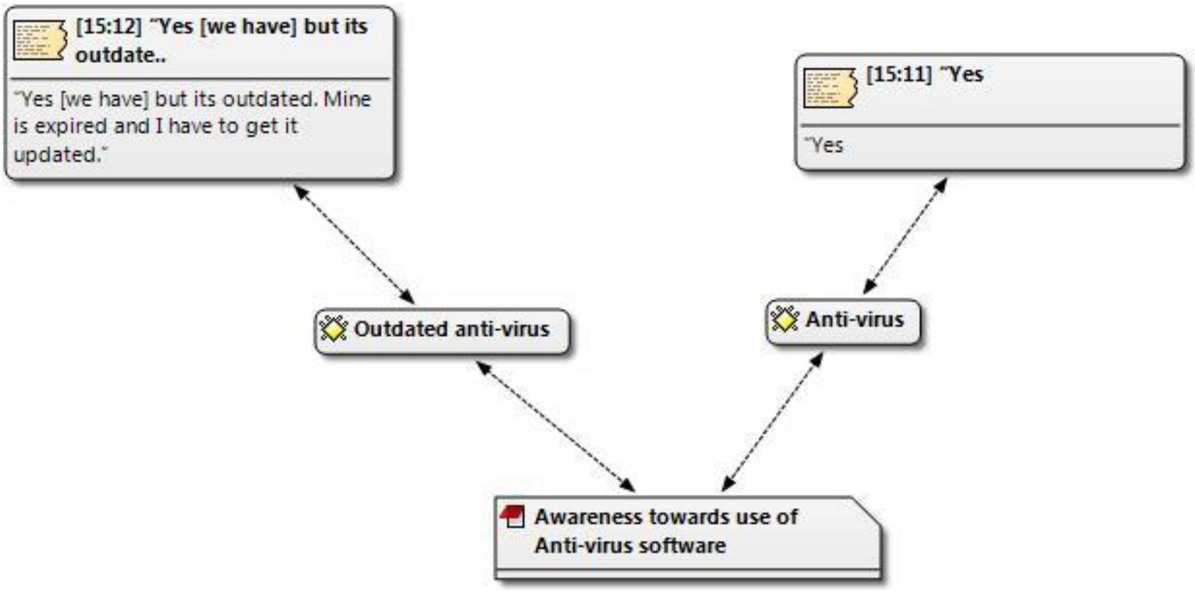
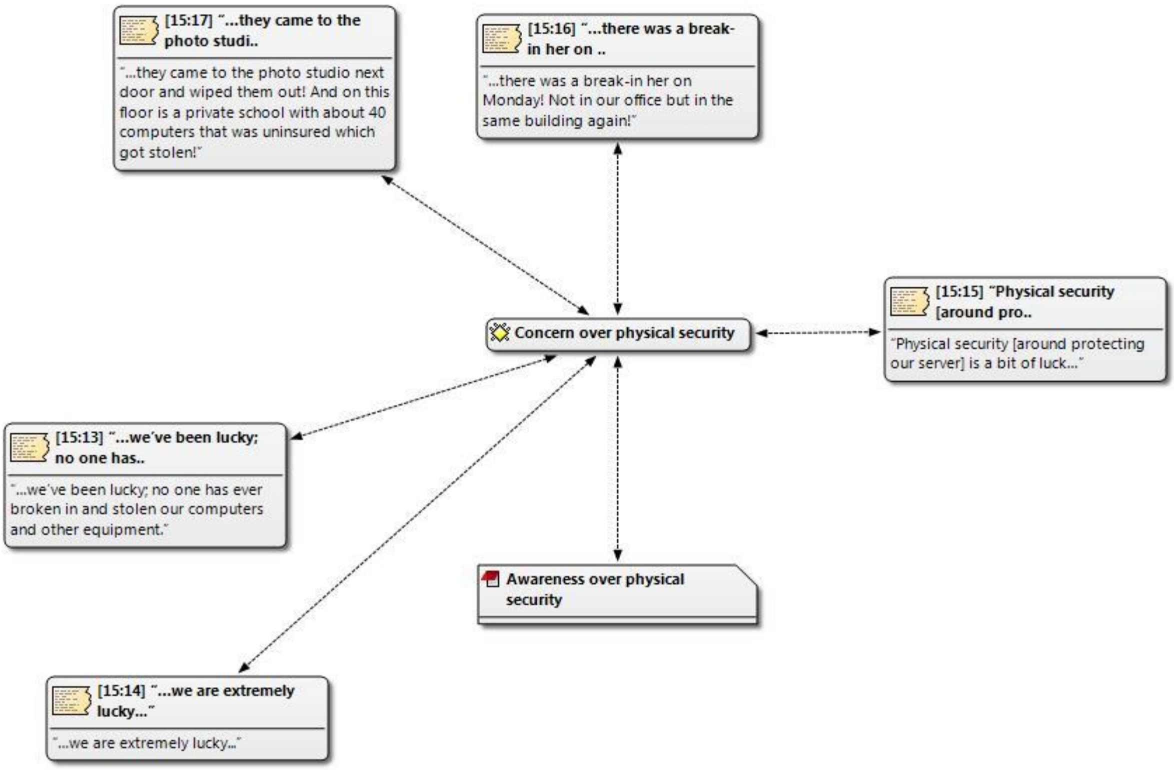

[15:12] "Yes [we have] but its outdate..
"Yes [we have] but its outdated. Mine is expired and I have to get it updated."
[15:11] "Yes
"Yes
Outdated anti-virus
Anti-virus
Awareness towards use of Anti-virus software

Figure 5.4.8

Awareness of Physical Security				
No:	Question / Theme	Response	In-vivo Codes	Categories
21	Physical access:	*"…we've been lucky; no one has ever broken in and stolen our computers and other equipment."* *"…we are extremely lucky..."* *"Physical security [around protecting our server] is a bit of a lack…"* *"…there was a break-in here on Monday! Not in our office but in the same building again!"* *"…they came to the photo studio next door and wiped them out! And on this floor is a private school with about 40 computers that was uninsured, which got stolen!"*	No one has broken in and stolen Extremely lucky Bit of a lack There was a break-in here Wiped them out 40 computers uninsured	Concern over physical security

Table 5.4.9



[15:17] "...they came to the photo studi..

"...they came to the photo studio next door and wiped them out! And on this floor is a private school with about 40 computers that was uninsured which got stolen!"

[15:16] "...there was a break-in her on ..

"...there was a break-in her on Monday! Not in our office but in the same building again!"

Concern over physical security

[15:15] "Physical security [around pro..

"Physical security [around protecting our server] is a bit of luck..."

[15:13] "...we've been lucky; no one has..

"...we've been lucky; no one has ever broken in and stolen our computers and other equipment."

Awareness over physical security

[15:14] "...we are extremely lucky..."

"...we are extremely lucky..."

Figure 5.4.9

5.5 Categories: Discussion

Table 5.5: Discussion

No	Category	Discussion
1	Information Technology Dependency	Software as well as business process examples explain how organisations are dependent on the use of IT. These results support the use of an IT-dependency tool that was used for criteria sampling (Ch. 3), supporting the organisational dependency on information technology. Quotations from participant responses clearly show how important the use of information technology is in the business organisations.
2	IT acceptance	All participants responded with a positive attitude to the change that information technology brings to the organisation. Changes include anything from the automation or improvement of business processes by using information technology. Some of the responses include: “yes definitely” and, “we really support the change information technology brings to the business”. Examples of ‘cost savings’ and ‘time’ were given as reasons for accepting the change brought through IT in the business. The category of ‘IT acceptance’ clearly supports the self-category of ‘Awareness of Technology Dependency’, as the quoted evidence shows a close relationship. A relationship exists between the IT-dependency and IT acceptance categories, as the evidence suggests.
3	Change failure & Resist system change	Failures caused by changes of IT-related components in the business were also derived from the quoted evidence that was analysed. The category of ‘Resistance to system changes’ is strongly supported by the ‘change failure’ category and evidence of failures relating to system changes that is captured as research evidence.
5	Loss of information	The loss of information within the business presents as a strong theme with a lot of supporting evidence. The dependency on business information along with the use of information

		technology is clearly highlighted with quoted evidence as support. A number of instances were recorded where businesses give examples of recorded IT or business failures resulting in the loss of business information. The loss of information supports the category 'IT Dependency' and is a strong recurring theme in the 'Loss of information' category. Organisations' dependency on information as well as information technology is critical towards the support and understanding of the research problem.
6	Personal and sensitive information	Evidence of personal and sensitive information used in the businesses is captured as quoted evidence. A number of different examples of the use of personal and sensitive information in the businesses is recorded and analysed. Personal information includes "tax numbers, unemployment fund numbers, full names and addresses and proof of addresses, identity numbers, licenses, payslips, bank statements, electronic signatures". Sensitive information consists of "historical company records, client names and company registration numbers and other business related information." It was further noted in the analysis of the research evidence that little knowledge exists around the use of 'personal and sensitive' information or the regulatory compliances towards the use of this information in the businesses.
7	Hard copy and digital storage of information	**Self-category: Awareness of Handling and Archiving Data** Information is stored in hard-copy files as well as electronically on hard disk drives. The hard-copy storage of information is, in most cases, transferred to electronic format. Information is stored in different places in the organisation, such as a central server, individual laptops, removable hard drives and filing cabinets. Storage of information includes the storage of personal and

		sensitive information. There is a strong relationship between the storage of business information and personal and sensitive information. The 'awareness of handling and archiving data' self-category gave result to the 'hard copy and digital storage of information' category. The storage of business information, including personal and sensitive information, is further related to the category of the 'loss of information' and supports the evidence recorded. **Self-category: Awareness of Personal and Sensitive Information** The storage medium and place of storage of business information is commonly known and described. In the 'awareness of personal and sensitive information' self-category, the participants are aware of the category or theme of 'the hard copy and digital storage of information'. Again, evidence suggests that 'personal and sensitive' business information is stored electronically as well as on hard-copy files.
8	No risk concern	**Self-category: Awareness of Online Banking** Under the 'Awareness of online banking' self-category, a strong theme that emerged was that of little concern over the risk of online banking. No specific risk concerns around the use of online banking were recorded and the participants indicated that they are satisfied with the current security measures in place. 'Restricted access' is another strong theme linked to security around online banking and as an internal control used by the business to secure its online bank accounts. The last theme in the self-category that emerged is the possible risk of "financial loss." Results show that although the participant organisations have little concern regarding the secure use of online banking, the possibility of a 'loss of financials' is widely known.

9	Restricted access (access to information)	Access to information is not always restricted and it can be seen that in some instances, the entire organisation has access to the information that the business stores. Information access is in some cases restricted for a particular business reason. None of the coded responses includes restricting access to information for the protection of stored personal and sensitive information. **Self-category: Awareness of personal and sensitive information** Restricted access to business information is again drawn and categorised from the quoted evidence. This is an extremely strong theme that emerged from the analysed data in the self-category. The category of ‘restricted access’, however, does not inform or support the self-category of ‘personal and sensitive information in the business’. It is established from the analysed data that access to business information is often restricted, but not because of privacy reasons such as ‘personal and sensitive’ information.
10	Access to business information & no information security	In support of the previous category and self-category of the analysed evidence, the access to business information was also studied. The evidence suggests that personal and sensitive information that is used in the business is not always restricted. One of the analysed quotes suggested that information, including personal and sensitive information, is accessible to everyone in the business and is not restricted. A second category derived from this research evidence is that no information security exists in the business organisations.
11	Loss of financials	The loss of financials theme contradicts the “no risk concern” category and indicates the business organisations are aware of the underlying risks. The possibility of a loss of financials when using online banking is commonly known and acknowledged by the participant small business organisations.
12	Ability to identify phishing	The participants of the study are able to identify ‘phishing’ and

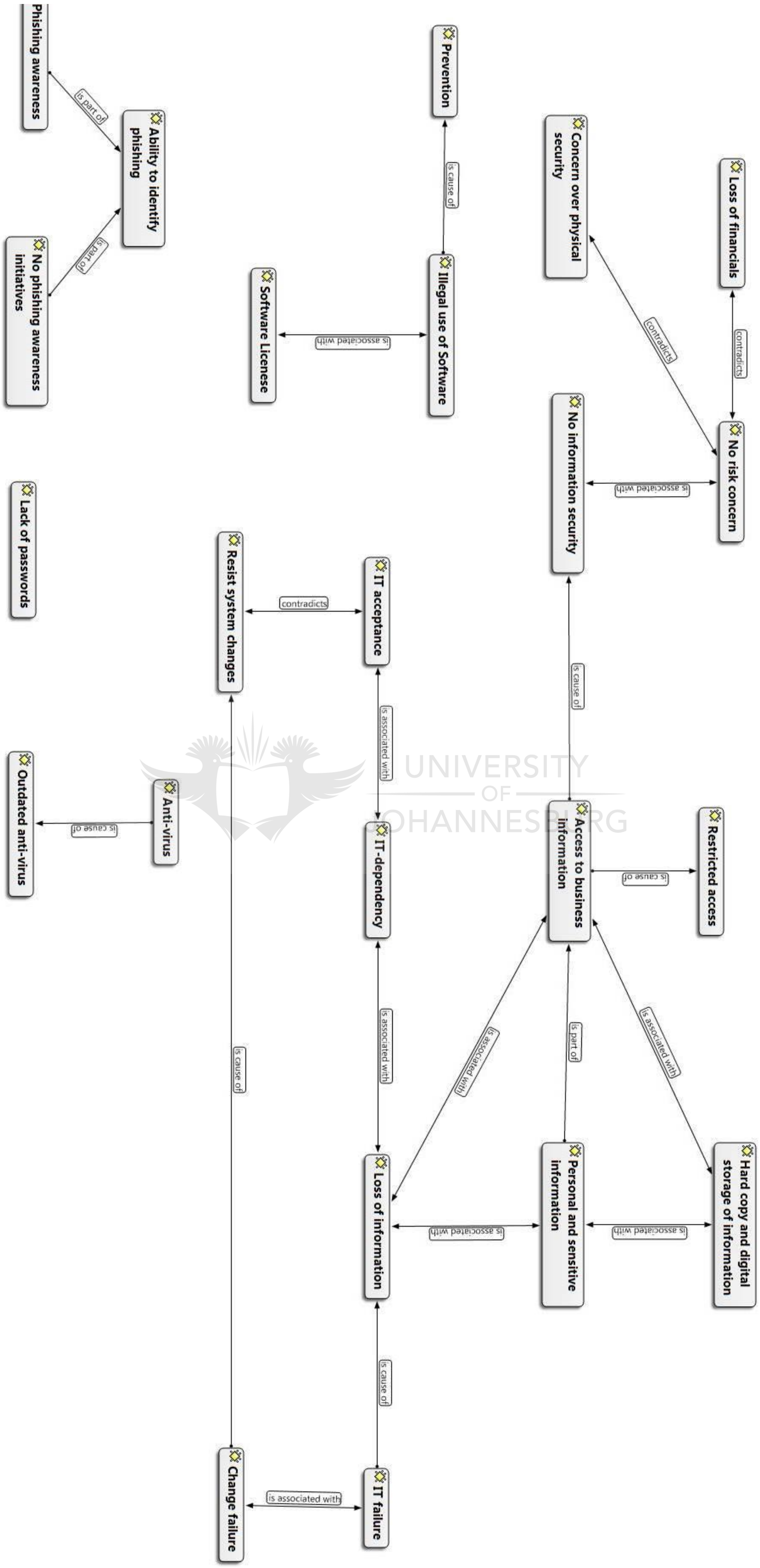
		phishing related threats. Quoted evidence shows that most of the participants are able to give specific examples of phishing related threats that have been noted by business.
14	Phishing awareness	Examples of phishing related awareness initiatives currently used by the business is mostly informal in nature and happens on an ad-hoc basis. The category of 'phishing awareness' has a strong relationship with the category: 'ability to identify phishing', and confirmed that the awareness of phishing and the risks of phishing exist in the business.
13	No phishing awareness initiatives	Another strong and contradicting category is that no phishing awareness initiatives exist in the business. Quoted evidence suggests that the owners or IT representatives of the participant organisations do not care about the risks of phishing and making their employees aware of the risks.
14	Lack of passwords	The most overwhelming theme that emerged from the 'awareness of password use' self-category is the 'lack of passwords' in the small business organisations. A number of quotes showed that a lack of password usage in the small business organisations exists, with little concern for the associated risks.
15	Software licences & Illegal use of software	Knowledge in the business around software licensing emerged as a strong category from the analysed data. Clear examples of software licensing obstacles as well as software audits have been captured and recorded. This category is strongly supported by another category: 'Illegal use of software', as the category furthers on the strong awareness the small businesses have around the legal and illegal use of software.
16	Prevention	The last category from the 'awareness of illegal software' is prevention. Prevention emerged as a theme from the analysed transcripts and shows that little prevention takes place internally regarding the illegal use of software in the small businesses. The category of 'prevention' supports the previous categories – 'software licenses and Illegal use of software' – as participants are clearly aware of the possible illegal use of

		software in the business. Very few initiatives are in place to prevent the use of illegal software.
17	Anti-virus & Outdated anti-virus	Results show that the use of anti-virus software in the small business environments is not as common as initially expected. Although anti-virus software is used, it is not always maintained and updated. There is, however, a strong awareness around the function of an anti-virus and other security related tools, such as firewalls. Although awareness exists, little effort is made by the businesses to make use of these security techniques.
18	Concern over physical security	The awareness of physical security is the last self-category that was tested during the fieldwork of the research. An overwhelming theme that emerged was the 'concern around physical access' in the small businesses of Gauteng. Quoted evidence shows examples regarding this concern for the small business organisations. This result was not anticipated by the research and is included in detail in the last discussion of the summary chapter.
19	IT-failure & Loss of information	Failures in information technology are clearly reflected in the analysed responses from the participants. Coding reveals examples of information and technology failures that resulted in the loss of information and the interruption of business operations. The criticality of the use of IT and information is noted from the codes derived.
20	No risk concerns	A lack of user awareness and concern around the use of online banking is observed. Coding suggest organisations are satisfied with their current use of online banking and have little concern over the risks that exist. No specific risks or concerns are mentioned in the responses. Phishing and the awareness of phishing risks in the business are, however, known and understood on a high level. Examples of phishing related incidents are captured from the interview responses.

Table 5.5: Discussion

The image below shows the final, complex, associations of the research categories that have been explained. In Chapter 6, an illustration of the final, complex, research findings will be concluded and used as part of the answer to the research question.

Figure 5.5: Final complex view



Chapter 6

`

This chapter will use the categories, relationships and other research findings to conclude on the research journey undertaken. The final research results obtained from the analysis of quoted evidence will be compared to the conceptual model to answer the research question. This will assist in answering the research question and show how the research objectives have been met. The trustworthiness of the research and possibilities for future research will also form part of the conclusion on the research work and discoveries made.

Chapter 6

Conclusion

6.1 Introduction

Following the discussion of the research findings in Chapter 5, the final conclusion can be made on the research results and research findings. In this chapter, the final research objectives will be met that includes answering the research question. This will be done using the research findings and relating the findings to the conceptual model and the other chapters of the research dissertation.

The figure below shows the conceptual model that was used as the research approach towards the intended research population that was studied. Lastly, the final summary of the research findings will be presented, which will be used with the conceptual approach to answer the research question.

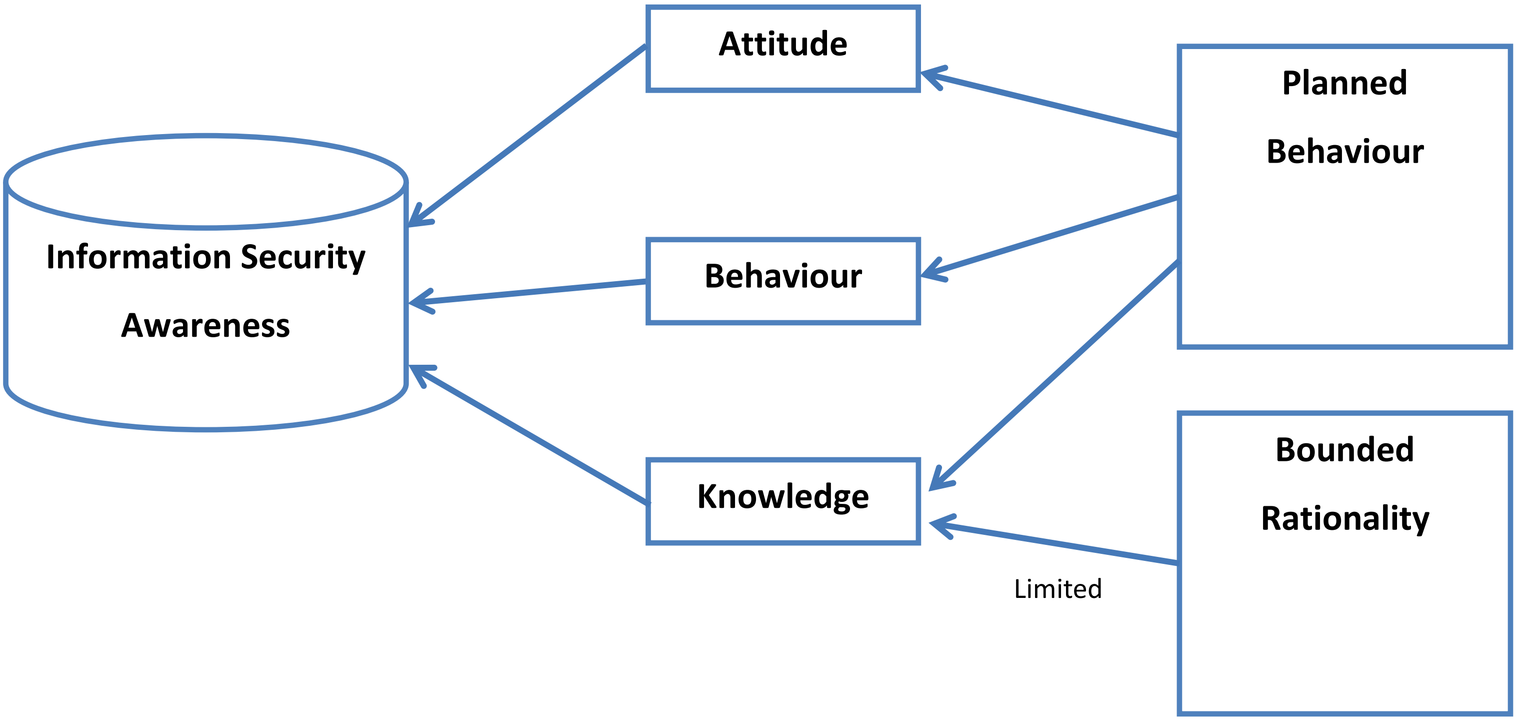


Figure 6.1: Conceptual Model

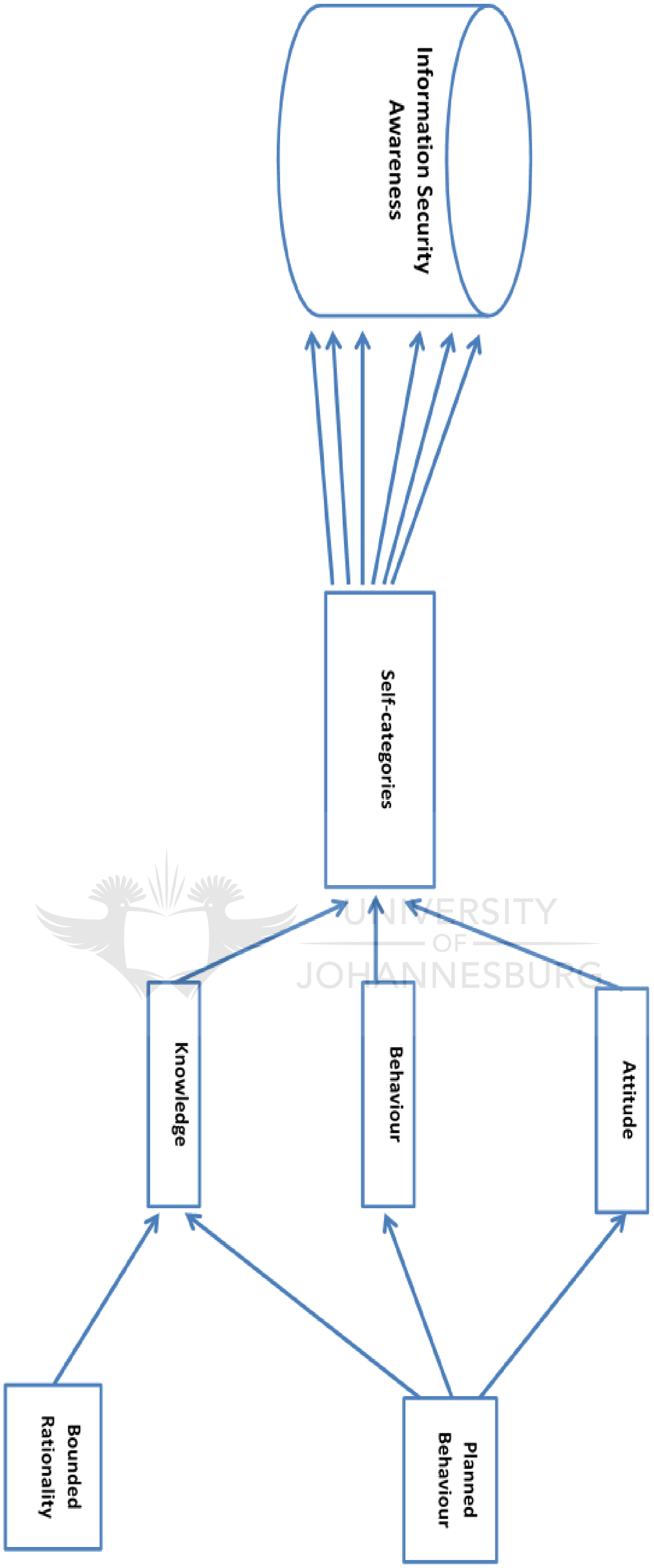


Figure 6.2: Summarised research findings

Figure 6.1 illustrates how the information security awareness of the small business organisations produced results within the derived self-categories. Self-categories were used to identify a number of themes around the research problem and what would be required from the literature as part of the research study. The approach of determining the information security awareness is defined in the conceptual model that has now been combined to the self-categories that was derived from the literature in Chapter 2. From the self-categories and conceptual approach that was followed, a number of 'categories' were derived from the quoted research evidence. These categories have been analysed and discussed in Chapter 5 of the research study and are illustrated visually with all the relationships drawn between the quoted evidence and in-vivo codes.

Figure 6.2 shows how the information security awareness and conceptual approach was linked to the self-categories that were derived from the literature in Chapter 2. In Chapter 5, the research findings were unveiled and discussed. The final interpretation was discussed according to the codes derived from the quoted research evidence, as shown in the previous chapter.

The approach delivered the results described in Chapter 5 and is illustrated as the 'complex view' of the final interpretation. This complex view is summarised in Figure 6.2 above, to use as part of the conceptual model and final research interpretations in answer to the research problem.

In figure 6.3 below, the final 'complex view' of the research findings drawn in Chapter 5 is illustrated again. The next section will conclude on the findings and their relationships, so as to help with the understanding of the research problem.

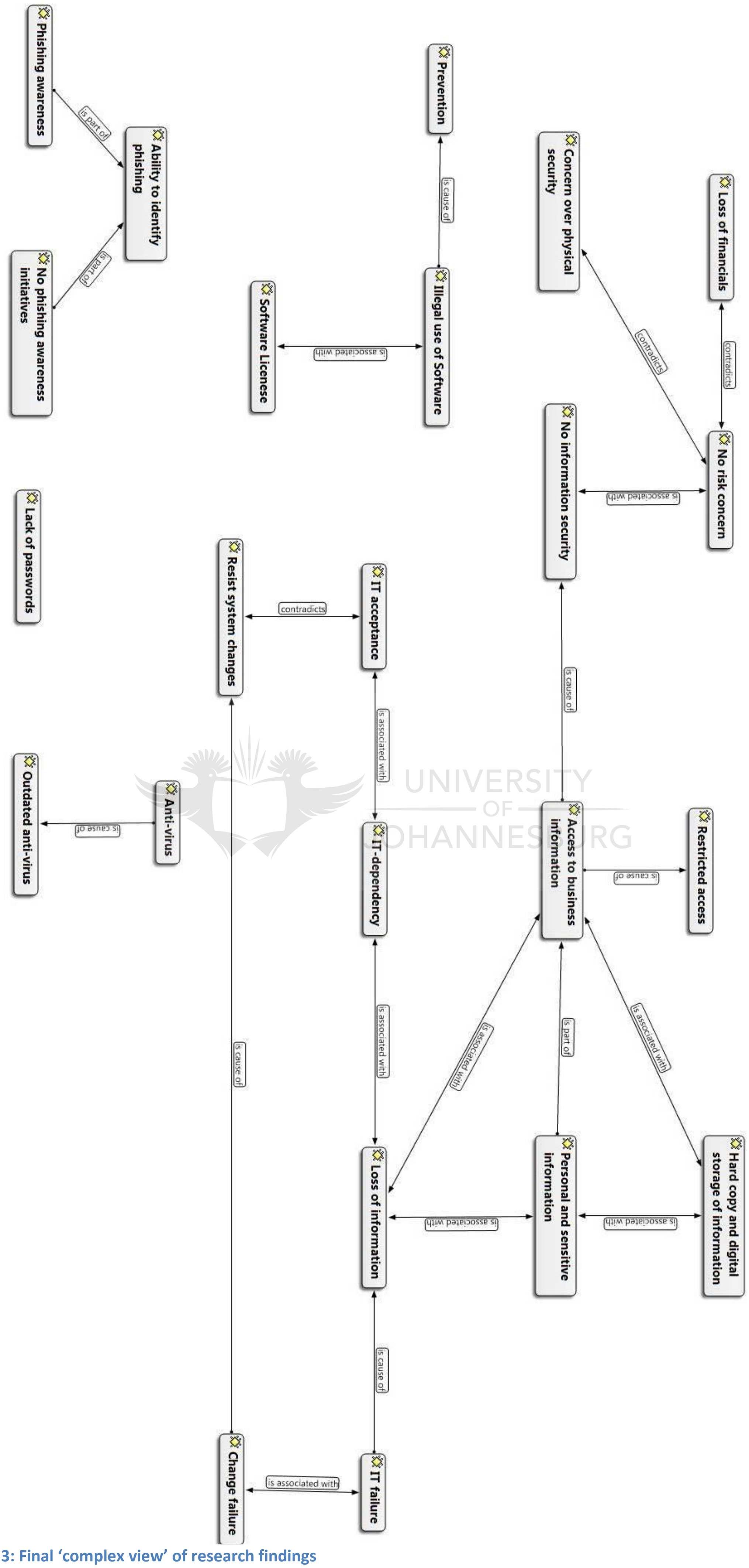


Figure 6.3: Final 'complex view' of research findings

6.2 Trustworthiness of Data

Before any further findings can be revealed, the trustworthiness of the data gathered in the research and used as part of the analysis and findings must be assured. As part of the qualitative research approach that was followed, the integrity of the empirical research data needed to be preserved. In preserving the integrity of the research results by avoiding interpreter bias, only quoted evidence from respondents was used for coding and deriving the categories for interpretation.

The In-vivo or quoted evidence from the respondents gave meaning to the categories and allowed for the interpretation of the categories and relationships to be identified between the different categories. The quoted evidence further supports the integrity of the data by using in-vivo coding and deriving categories from these pieces of evidence. The codes were further interpreted according to the overall conceptual research approach as well as the specific self-category it was placed in.

6.3 Final Conclusion on Research Findings

The first section of this chapter illustrated how the conceptual model is supported by the final research findings and the 'self-categories' drawn as themes from the literature. The previous section on the trustworthiness of the research data and the integrity of how the empirical evidence was preserved throughout the research process supports these illustrative figures.

In Chapter 5, the findings and discussion of the analysed research data took place. This included the coding of the quoted evidence as well as the identifying of categories. The chapter also presented the final interpretation of the research findings and a discussion on the relationships that were drawn between the categories. The last table in Chapter 5 discussed each category and the relationship it has with the other categories are be used when answering the research question. Below is the research problem that was posed in Chapter 2 as what needs to be answered for the research outcome.

Information technology dependency is one of the first categories identified in the research findings. This category comes across as a strong theme throughout the research findings and supports the research method of using a sampling technique 'IT-dependency tool'. This approach was to study business organisations that are dependent on the use of information technology as part of the business. The dependency on information technology was to be studied and understood in the context of the Gauteng and South African business environment.

Conclusion on research self-categories:

A second category that was derived from the research results was that of ‘IT acceptance’, which is strongly related to the previous category, showing how information technology is accepted as part of the business and how it forms part of the business culture. The relationship between the two categories is also illustrated in figure 6.3.

‘Resist system changes’ is another category that presents a contrast to the acceptance of IT in businesses. Although it is not as influential as the acceptance of IT in businesses, it does however affect the findings of the study. ‘Change failure’ as a category supports the ‘Resist system changes’ category through a number of quoted examples of IT failures resulting in a resistance to system changes.

Another category that is supported by substantial quoted evidence is the ‘loss of information’ category. The loss of information refers to critical business information that is lost due to a business or business-IT failure. The quoted evidence linked to the category of ‘loss of information’ shows a number of examples on how a loss of information can occur in the everyday small business environment.

‘Personal and sensitive information’ is another of the categories identified when drawing findings from the research results. The terminology of ‘personal and sensitive’ information is not always used by small businesses, however, quoted evidence shows that all of the participant business organisations make use of personal and sensitive information in some form. The extensive use of personal and sensitive information is further supported by the strong use of information technology in the capturing, storing and processing of information. There is little knowledge over legislative and regulatory compliance in terms of the use of ‘personal and sensitive information’ that exists for the small business.

Personal and sensitive information has a strong relationship with the category of ‘access to business information’ and forms part of how the ‘personal and sensitive’ information is used and accessed in the business. Personal and sensitive information is also associated with the category of ‘hard copy and digital storage of information.’

The ‘hard copy and digital storage of information’ category presented some unexpected results, showing that information, including personal and sensitive information, is also stored in hard-copy format and not only through the use of information technology. Information technology is, however, also used to process information for the business organisation. The ‘hard copy and digital storage of information’ has a direct relationship with the category of ‘access to business information’.

‘Access to business information’ refers to how, when and where information is used, processed and stored by the small businesses organisations. The research results indicate that access to information in the small business organisations is not always restricted and can be accessed by any employee in the business. Some examples of restricted access in the business were obtained, although none was specific to the protection of personal and sensitive information.

This finding resulted in the creation of the category of ‘no information security’ that shows little business concern over information security in the business. Little to no information security initiatives in the business has a supporting relationship with the following categories:

- Access to business information
- Restrict access (to business information for other business reasons besides the protection of personal and sensitive information)
- Hard copy and digital storage of information
- Personal and sensitive information
- Loss of information (also associated with a number of other categories)

In the first section of this chapter the complex relationship between the research findings that includes the above listed categories is shown. The relationship between the access to business information, restriction of business information and personal and sensitive information is displayed. There is, however, no support for restricting access to business information and personal and sensitive information. This supports the need for the category of ‘no information security’.

The ‘no information security’ category showed that there is little information security concerns in the small business organisations of Gauteng. Restricted access to information is known to the small business organisations, but little other initiatives exist for protecting information in the business.

‘No risk concern’ is another category that emerged when looking at the use of online banking in the business organisations. The findings are based on quoted evidence that shows small business organisations have little concern over the security of online banking. Although online banking is linked to the ‘restricted access’ category, there is no further association between the ‘no Information security’ and the ‘no risk concerns’ categories.

The ‘no risk concerns’ category contradicts the ‘loss of financials ’category and is centred around the use of online banking in the small businesses and other direct financially related risks through the use of information technology.

In the findings, the possible loss of financials is known to the small business organisations, although there is very little to no risk concern or information security present in the businesses. Some of the quoted evidence suggests the overall benefits of information technology in the businesses are much greater than the associated risks, including information security risks. From the findings it can be seen that although the organisations are aware of some of the risks that exist around the abuse of personal information, very little, or no, actual business actions are taken against these risks.

Some more *technical* categories also form part of the results, as the use of information technology and the security around the safe use of IT in the business forms part of the final conclusion on the research findings.

The 'ability to identify phishing' is a category that is associated with all of the participant organisations. The term 'phishing' is not always known to the participants, but still forms part of the business culture. This relates to two further categories: 'phishing awareness' and 'no phishing awareness initiatives.' These findings show that although the term phishing is not always known, participants can articulate clear examples of phishing related incidents that have occurred in the businesses. There is also an indication that participants do not see phishing as a large enough risk to have formal practices or processes in place to either create awareness or mitigate the direct threats of phishing.

'Lack of passwords' is another category that emerged when analysing at the security practices of the small business organisations. The possible use of passwords as security tool in the use of IT is known to the small business organisations, but little formal practices or processes are implemented around the use of passwords. The 'lack of passwords' category has no immediate associations with other categories, but is grouped with the 'no information security, no phishing awareness, and, no risk concern' categories on the complex categories relationship diagram.

'Software licences' and 'illegal use of software' are two categories that were drawn around the specific uses of Information Technology in the business. Organisations are aware of software licences and the 'illegal use of software', which supports the findings of awareness that exists around the use of software and the use of licensed software in the business. These findings are associated with the category of 'prevention', which explains that the small businesses are aware that software in the business should not be used in an illegal manner. The possibility of using illegal software is clearly known to participants, but is not associated with the culture of the business.

'Anti-virus' and 'outdated anti-virus' are two categories that were derived when studying the use of anti-virus and firewall software in the small business organisations. These two categories relate to one another, as not all of the participant organisations made use of updated anti-virus software as part of the information security in the business.

One of the unexpected categories that emerged was the large concern of the small business organisations over their ‘physical security’, including information technology. The findings suggest that this is owed to the high crime-rate in South Africa and the need to protect business assets from theft.

The last category identified is ‘IT failure’, which is supported by a number of other categories. Findings show clear examples of IT failures and how they affect the daily operations of the businesses. IT failure is associated with ‘change failure’, explaining some of the IT-related failures that the small business organisations have experienced. The categories of ‘IT failure’ and ‘change failure’ are linked to the category ‘no risk concern’ and ‘no information security’, confirming that there is little security over information and technology in the businesses.

Research Question:

What is the current information security awareness in small information technology-dependant business organisations in Gauteng, South Africa?

Research Objectives:

- Identify the information and cyber security awareness espoused regarding use of personal and sensitive information
- Identify how the use of information and technology forms part of a critical process in small organisations.
- Identify how personal and sensitive information collected by small organisations is stored and used.

The final conclusions of the research findings suggest that there is no information security awareness in the small business organisations of Gauteng. Little information security awareness initiatives exist in the small business organisations and they also appear to have little concern over information security.

There is a strong awareness around the use of information technology in the businesses as well as a strong awareness of the dependency of the businesses on IT. There is, however, little awareness of the information security practices in the studied small business organisations, which helps to explain why there is no information security awareness.

Little knowledge exists around personal and sensitive information and the use of this information in the businesses. This is mainly owed to the lack of formal IT and information security that exists in the small business organisations. A good understanding of how information technology is used in the small business organisations of Gauteng has been obtained from the findings. This includes the security and information security aspects of the use of information and technology in the small businesses.

However, from the final conclusions it is clear that the small business organisations of Gauteng have little IT security, no information security and, ultimately, no information security awareness as part of the business operations. The categories around IT security, information security and information security awareness, which were drawn from the literature, give detailed and precise information on how they are perceived in the organisations.

The research findings provide new insight into the different IT and information security elements that were studied in the small IT-dependant business organisations of Gauteng. IT-dependant organisations were mainly selected because of the large diversity of small business organisations that exist in South Africa. This can vary from a small business that has no use of information technology to a small business that is completely dependent on IT.

The research objectives have been met as the information security awareness of the small IT-dependant business organisations of Gauteng have been studied and concluded upon. This was done by studying various sources and conducting fieldwork through qualitative interviews and examining the results. A good understanding of the personal and sensitive information uses in the small business organisations has been obtained, as well as an understanding of the related risks.

In answering the research question, the research limitations and future research possibilities will be concluded on. In doing so, future research can be conducted in the small business organisations of Gauteng and the rest of South Africa. The research findings of this research paper can help with future research, as it gives a good starting point for how the different IT security aspects are perceived and treated in small business organisations.

6.4 Generalisation of the Research Findings

The research methodology section in Chapter 3 explained that the research findings from the province of Gauteng cannot scientifically be generalised to the rest of the small business organisations in South Africa. However, it is established that when applying the findings to the rest of the IT-dependant small business organisations of South Africa, these findings can give a good indication of the information security awareness in the small business organisations.

Small, IT-dependent business organisations from a diversity of industries were studied, which can also exist in the other provinces of South Africa. Literature shows that information technology is used throughout South Africa in small business organisations, supporting the businesses in a number of ways.

Although the study is qualitative in nature and cannot scientifically be generalised in any form, the results can support future research when studying the same population in the other provinces of South Africa. The Gauteng province is among those with the largest number of small business organisations operating in different industries, which make use of information technology.

This is mainly because Gauteng hosts two of the country's largest cities – Johannesburg and Pretoria – and provides the largest contribution to the country's gross domestic product, as was discussed in Chapter 2. Although the research findings can be generalised in some manner, the limitations are identified in the next section.

6.5 Limitations of the Research Findings

The research findings are based on results that were obtained by analysing qualitative data obtained from interviews with the respondents. Even if the integrity of the data is maintained, the results and findings cannot be quantified. The research results are also qualitative in nature, with no numerical results to be interpreted.

The generalisation of the research findings to the rest of South Africa is not statistically possible for research purposes, but gives a good insight into and indication of the of information security awareness in South African small business organisations.

The findings are presented from the researcher's perspective, but are produced using acceptable scientific research methods followed during the research expedition. This included the interpretation of quoted evidence around the different research topics that were studied.

6.6 Future Research

From the research completed and findings discussed, a number of further opportunities exist that can be pursued. Section 6.4 described how the research results can be generalised to the rest of the small business organisations in South Africa so as to understand the studied topic of interest.

The same research instruments used in this research study can also be applied to the other eight provinces in South Africa. By studying the other provinces, an overall understanding of the IT uses in the small business organisations of South Africa, including their information security awareness, can be obtained.

Using the qualitative information obtained as a starting point for understanding the small business organisations of Gauteng, a quantitative research instrument can also be designed to study the population. Statistical and quantitative results over a larger number of participants can be used as future research for studying information security awareness in the small business organisations of South Africa.

The research instruments used in this study are also not completely restricted to small business organisations. They can be adapted for medium and large sized business organisations when studying the use of IT and information security awareness.

In Chapter 2, the literature clearly shows a lack of formal research done on information security and information security awareness in the small business organisations of South Africa. Because of the increase in numbers of these businesses and the important role they play on the economy of South Africa, there is still a great need for more research to be done.

6.7 Final Conclusion

Chapter 6 has presented the final conclusion on the research findings by answering the research problem. The research objectives have also been reflected upon as part of the conclusion of the research journey. In answering the research questions, new understandings have been added to the current literature and knowledge that exists around the small business organisations of Gauteng and the information security awareness that exists in these businesses.

New knowledge has been gained on the information technology uses and information security awareness that exists in small business organisations. This knowledge is specific to the small business organisations of South Africa which places an African context to a global debate of information security awareness.

Bibliography

Ajzen, I. (1991). The theory of planned behavior. *Organizational behaviour and human decision process*, 50:179-211.

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

Al-Khatib, J. A., Malshe, A. & Sailors, J. J. (2009). The impact of deceitful tendencies, relativism and opportunism on negotiation tactics: a comparative study of US and Belgian managers. *European Journal of Marketing*, 45(1/2):133-152.

Alony, I., Whymark, G. & Jones, M. (2007). Sharing Tacit Knowledge: A Case Study in the Australian Film Industry. *Informing Science Journal*, 10:41-59.

Arduini, F. & Morabito, V. (2010). Business Continuity and the Banking Industry. *Communications of the ACM*, 53(3):121-125.

Arp, R. (2007). Consciousness and Awareness - Switched-On Rheostats: A Response to de Quincey. *Journal of Consciousness Studies*, 14(3): 101-106.

Baard, V. C. & van den Berg, A. (2004). Interactive information consulting system for South African small businesses – Part 1. *South African Journal of Information Management*, 6(2): 1 - 27.

Baskerville, R., Spagnoletti, P. & Kim, J. (2014). Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response, 51(1): 138 - 151

Beheshti, H. M. (2004). The impact of IT on SME's in the United States. *Information Management and Computer Security*, 12(4):318-327.

Boucher, D. & Flowerday, S. (2011). Privacy: In pursuit of information security awareness. Information Security South Africa (ISSA). In proceeding of: Information Security South Africa Conference 2011, Hyatt Regency Hotel, Rosebank, Johannesburg, South Africa, August 15-17, 2011. Proceedings ISSA 2011

Bhattacharya, D. (2011). Leadership styles and information security in small business. *Information Management and Computer Security*, 19(5):300-312.

Blumberg, B., Cooper, D. R. & Schindler, P. S. (2008). *Business Research Methods (Second European Edition)*. McGraw-Hill Education.

Boucher, D. & Flowerday, S. (2011). Privacy: In pursuit of information security awareness. Information Security South Africa (ISSA). Available from: http://icsa.cs.up.ac.za/issa/2011/Proceedings/Research/Baucher_Flowerday.pdf

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *An International Journal of Police Strategies and Management*, 29(3):408-433.

Business Roundtable. (2007). *Growing Business Dependence on the Internet.* Business Roundtable. Available from: http://businessroundtable.org/media/news-releases/business-roundtable-ceos-release-internet-security-report

Campbell, J. L., Quincy, C., Osserman, J. & Pedersen, O. K. (2012). Coding In-Depth Semi-Structured Interviews: Problems of Unitization and Inter-Coder Reliability and Agreement. Socialogical Mothods Research, 42(3): 294-320

Carkenord, B. (2009). *Seven Steps to Mastering Business Analysis.* J.Ross Publishers, 2009

Carruthers, J. (1990). A Rationale for the Use of Semi-structured Interviews. *Emerald*, 28(1):63-68.

Charney, S. (2010). *Collective Defense - Applying Public Health Models to the Internet.* Microsoft Corporation. Available from: https://www.microsoft.com/mscorp/twc/endtoendtrust/vision/internethealth.aspx

Chen, C. C., Medlin, B. D. & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management and Computer Security*, 16(4):360-376.

Cobit 4.0. (2006). *Control Objectives 4.0.* Governance Institute.

Coertze, J., van Niekerk, J. & von Solms, R. (2011). A web-based information security management toolbox for small-to-medium enterprises in Southern Africa. *Information Security South Africa (ISSA)*, 1-8. Available from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6027515&contentType=Conference+Publications (Accessed 2 August 2012).

Department of State Security. (2012). *South African Government Information.* Available from: http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794 (Accessed 30 July 2012).

Dictionary.com Unabridged. (2009). *Semantics*. Retrieved July 20, 2013, from Dictionary.com: http://dictionary.reference.com/browse/semantics

Duan, Y. & Cruz, C. (2011). Formalizing Semantic of Natural Language through Conceptualization from Existence. *International Journal of Innovation, Management and Technology*, 2(1):37-42.

Edoho, F. M. (2013). Information and Communication Technologies in the Age of Globalisation: Challenges and Opportunities for Africa. *African Journal of Economic and Management Studies*, 4(1): 9-33.

FinScope. (2006). *FinScope Small Business Pilot Survey Gauteng 2006.* Available from: http://www.finscope.co.za/finscope/scriptlibrary/getfile.aspx?filename=PR_SmallBusiness.pdf&file=../module_data/71e3e62d-1eeb-412e-893b-970e98f6a3fa/downloads/2f797631-b99c-4d22-8a04-3dd84172b54c.file

Fox, N. (2009). *Using Interviews in a Research Project.* Available from: http://www.rds-eastmidlands.nihr.ac.uk/resources/doc_download/14-using-interviews-in-a-research-project.html

Frauenberger, C., Good, J. & Keay-Bright, W. (2010). Phenomenology: a Framework for Participatory Design. Proceedings of the 11th Biennial Participatory Design Conference 187-190. Available from: http://dl.acm.org/citation.cfm?id=1900474

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

Gauteng Provincial Government. (2010). *Gauteng SMME Policy Framework (2010-2014).* Gauteng: Department of Economic Development. Available from: http://www.ecodev.gpg.gov.za/policies/Documents/Gauteng%20SMME%20Policy%20Framework%20Revised%20100527.pdf

Grobler, M. & Jansen van Vuuren, J. (2010). *Broadband broadens scope for cyber crime in Africa.* Information Security for South Africa (ISSA): 1-8. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5588287&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5588287

Grobler, M., Jansen van Vuuren, J. & Zaaiman, J. (2011). Evaluating Cyber security Awareness in South Africa. 113-121. Available from:

http://researchspace.csir.co.za/dspace/bitstream/10204/5108/1/Grobler1_2011.pdf?origin=publication_detail

Government Communication and Information System. (2012). *The Local Government Handbook - Gauteng*. Available from: http://www.localgovernment.co.za/provinces/view/3.

Groenewald, T. (2004). A Phenomenological Research Design Illustrated. *International Journal of Qualitative Methods*, 3(1): 1-26

Guion, L. A., Diehl, D. C. & McDonald, D. (2011). Conducting an In-depth Interview. University of Florida - IFAS Extension. Available from: https://edis.ifas.ufl.edu/fy393

Harnesk, D. & Lindstrom, J. (2011). Shaping security behaviour through discipline and agility. *Information Management and Computer Security*, 19(4):262-276.

Harvey, W. S. (2011). Strategies for conducting elite interviews. *Sage Journals*, 11(4):431-441.

Hewner, M. & Knobelsdorf, M. (2008). Understanding Computing Stereotypes with Self-Categorization Theory. Proceedings of the 8th International Conference on Computing Education Research, 72-75

Hogg, M. A. & Reid, S. A. (2006). Social Identity, Self-Categorization, and the Communication of Group Norms. *Communication Theory*, 16:7-30.

Hornsey, M. J. (2008). Social Identity Theory and Self-categorization Theory: A Historical Review. *Social and Personality Psychology Compass*, 2(1):204-222.

ISACA - Cobit 5. (2012). *Cobit 5: A busienss framework for the governance and management of enterprise IT.* ISACA. Available from: http://www.isaca.org/COBIT/Pages/default.aspx?cid=1003566&Appeal=PR

ISACA - Cobit 5. (2012). *Cobit 5: Enabling Processes.* ISACA. Available from: http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx

ISO/IEC 27002:2005. (2005). *Information Technology - Security Techniques - Code of practivce for Information Security Management.* Available from: http://webstore.iec.ch/preview/info_isoiec27002%7Bed1.0%7Den.pdf

Johnson, J. & Henderson, A. (2002, February). Conceptual Models: Begin by Designing What to Design. AMC Digital Library*9(1)*, 25-32.

Johnson, P., Buehring, A., Cassell, C. & Symon, G. (2007). Defining qualitative management research: an empirical investigation. *Qualitative Research in Organizations and Management: An International Journal*, 2(1):23-42.

Jones, B. D. (1999). *Bounded Rationality.* Annual Review of Policitcal Sciences, 2: 297-321.

Kaiserlidis, L. M. & Lindvall, J. (2004). On the Duality of Information Technology: Understanding the Connection Between 'Automate' and 'Informate. 5th European Conference on Organization Knowledge, Learning and Capabilities, Innsbruck, Austria, April, 2004.

Kallinikos, J. (2011). The "Age of Smart Machine": A 21st Century View. *Encyclopedia of Software Engineering*, 1.

Karyda, M., Kokolakis, S., Kiountouzis, E. & Tsohou, A. (2012). Analyzing trajectories of information security awareness. *Information Technology and People*, 25(3):327-352.

Kaspersky Lab. (2012). *Global IT Security Risks: 2012.* Availabe from: http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26):10862-10868. Available from: http://www.academicjournals.org/ajbm/pdf/pdf2011/28Oct/Khan%20et%20al.pdf.

KPMG South Africa. (2013, November 27). Protection of Personal Information Bill (POPI) becomes law. Available from: http://www.kpmg.com/za/en/issuesandinsights/articlespublications/protection-of-personal-information-bill/Pages/default.aspx.

Kritzinger, E. & Smith, E. (2009). A prototype for enhancing information security awarenss in industry. *Proceedings of the World Academy of Science Engineering and Technology*, 54:521-530. Available from: http://waset.org/publications/944/prototype-for-enhancing-information-security-awareness-in-industry

Kruger, H. A. & Kearney, W. D. (2008). Consensus ranking - An ICT security awareness case study. *Elsevier*, 27 (7-8): 254-259.

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *Information Security South Africa (ISSA 2011).* Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6027505&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6027505

Kruger, H., Drevin, L. & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Emerald*, 18(5):316-327.

Kruger, H. A., Flowerday, S., Drevin, L. & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *Information Security South Africa (ISSA 2011):* 1-7.

Kruger, H. & Kearney, W. (2005). Measuring Information Security Awareness: A West African Gold Mining Environment Case Study. Proceedings of the 2005 ISSA Conference, Johannesburg, South Africa. Available from: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/018_Article.pdf

Kyobe, M. (2010). Towards a framework to guide compliance with IS Security policies and Regulations in a university. *Proceedings of the 2010 Information Security for South Africa (ISSA 2010) Conference*. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5588651&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5588651

Labuschagne, W. A. & Eloff, M. (2012). Towards an automated security awareness system in a virtualized environment. Proceedings from the 11th European Conference on Information Warfare and Security. Available from: http://uir.unisa.ac.za/handle/10500/7705

Ladzani, W. & Netswera, G. (2009). Support for rural small businesses in Limpopo Province, South Africa. *Development Southern Africa*, 26(2):225-239.

Lester, S. (1999). *An introduction to phenomenological research.* Stan Lester Developments. Availabe from: http://www.sld.demon.co.uk/resmethy.pdf

Mafiri, M. (2002). Socio-Economic Impact of Unemployment. 7-12. Available from: http://upetd.up.ac.za/thesis/available/etd-08162004-135251/unrestricted/00front.pdf

Mainelli, M. (2013). Learn from insurance: cyber bore. *The Journal of Risk Finance*, 14(1):100-102.

Mbonyane, B. & Ladzani, W. (2011). Factors that hinder the growth of small businesses in South African townships. *European Business Review*, 23(6):550-560.

McDonald, G. (2010). Ethical relativism vs absolutism: research implications. *European Business Review*, 22(4):446-464.

Mejias, R. J. (2012). An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. *45th Hawaii International Conference on System Sciences*, (3258- 3267). Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6149219&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6149219

Moore, N. & Stokes, P. (2012). Elite interviewing and the role of sector context: an organizational case from the football industry. *Qualitative Market Research: An International Journal*, 15(4):439-440.

Mouton, J. (2012). *How to succeed in your Master's and Doctoral Studies: A South African Guide and Resource Book.* Van Schaik.

Mugo, E. A. (2012). A Model to Measure Information Security Awareness Level in an Organization: Case Study of Kenya Commercial Bank. Available from: http://ir.library.strathmore.edu/fileDownloadForInstitutionalItem.action;jsessionid=4C2BA693C06D4A0FED07BCB70688B82C?itemId=494&itemFileId=449.

Migiro, S. O. & Magangi, B. A. (2011). Mixed methods: A review of literature and the future of the new research paradigm. *African Journal of Business Management*, 5(10):3757-3767.

Nattrass, N., Wakeford, J. & Muradzikwa, S. (2003). *Macro Economics: Theory and Policy in South Africa.* David Philip Publisher.

National small business act 102 of 1996. (1996). *No. 102 of 1996: National Small Business Act.* Available from: http://www.info.gov.za/acts/1996/a102-96.pdf.

Njenga, K. & Ndlovu, S. (2012). On Privacy Calculus and Underlying Consumer Concerns influencing Mobile Banking Subscriptions. *IEEE*. Information Security for South Africa (ISSA). Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6320453&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6320453

Ngoqo, B. & Flowerday, S. (n.d.). Awareness - the Achilles heel of student mobile phone users: an exploratory study of information security behaviour.

Nordströma, T., Söderströmb, M. & Hansethc, O. (2000). *Business Development in IT-dependent organisations. Proceedings of IRIS 23*. Laboratorium for Interaction Technology, University of Trollhättan Uddevalla. Available from: http://heim.ifi.uio.no/~oleha/Publications/iris23_ITdependent.pdf.

Okere, I., van Niekerk, J. & Carroll, M. (2012). Assessing Information Security Culture: A Critical Analysis of Current Approaches. *Information Security for South Africa (ISSA)* , 1-8. Available from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6320442

Oxford Dictionaries. (n.d.). *Awareness*. Retrieved 08 25, 2013, from http://oxforddictionaries.com/definition/american_english/awareness

Perks, S. (2010). Problem-solving techniques of growing very small businesses. *Journal of Enterprising Communities: People and Places in the Global Economy*, 4(3):220-233

POPI Bill. (2009). *Protection of Personal Information Bill.* Minister of Justice and Constitutional Development.

Protection of Personal Information Act. (2013, November 26). Government Gazette No. 37067. Available from: www.gov.za/documents/download.php?f=204368

Qu, S. Q. & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management*, 8(3):238-264.

Reid, A., Petocz, P. & Gordon, S. (2008). Research interviews in cyberspace. *Qualitative Research Journal*, 8(1):47-62.

Robbins , S. P., Judge, T. A., Odendaal, A. & Roodt, G. (2009). *Organisational Behaviour: Global and Southern African Perspectives.* n.d. Pearson.

Rowley, J. (2012). Conducting research interviews. *Management Research Review*, 25(3):260-271.

Saint Mary's University of Minnesota. (2003). *Qualitative Research vs. Quantitative Research*. Twin Cities Campus Library. Available from: http://www2.smumn.edu/deptpages/tclibrary/tutorials/finding/qualitative.pdf

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime*, 15(4):432-443.

Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students.* Prentice Hall.

SBP. (2009, August). *Small business development in South Africa*. SBP: business environment specialists. Available from: http://www.sbp.org.za/uploads/media/SBP_ALERT_smme_development_in_SA.pdf

Scheers, L. v. (2010). Challenges of small family groceries shops in South Africa. *World Journal of Enterprenuership, Management and Sustainable Development*, 6(3):221-231.

SEDA. (n.d.). *About Seda*. Small Enterprise Development Agency (SEDA). Available from: http://www.seda.org.za/AboutSEDA/Pages/WhoweAre.aspx.

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

Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, 5(4):311-321.

SouthAfrica.info. (2012). *Gauteng province, South Africa*. Available from: http://www.southafrica.info/about/geography/gauteng.htm#.UqQZP_QW3Gw.

SouthAfrica.info. (2011). *South Africa's population*. Available from: http://www.southafrica.info/about/people/population.htm#provinces (Accessed 20 August 2012).

Stats SA. (2012). *Census 2011 Municipal report – Gauteng.* Statistics South Africa. Available from: http://www.statssa.gov.za/Census2011/Products/GP_Municipal_Report.pdf

Statistics South Africa. (2012). *Quarterly Labour Force Survey Quarter 2, 2012.* Statistics South Africa. Available from: http://www.statssa.gov.za/Publications/P0211/P02112ndQuarter2012.pdf.

Stephanou, A. & Dagada, R. (2008). The impact of information security training on information security behaviour: The Case for further research, n.d. Available from: http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/54.pdf

Stewart, G. & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management and Computer Security*, 20(1):29-38.

Thomson, M. (2008). Making information security awareness and training more effective. *Information Security Journal: A Global Perspective,* 207-227. Available from: http://dl.acm.org/citation.cfm?id=1477818.

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

Trend Micro. (2012). *Is your business at risk of losing data? 5 Data Security Risks every small business should know about.* Trend Labs. Available from: http://www.trendmicro.co.uk/media/misc/why-small-business-lose-critical-data-en.pdf

Tsohou, A., Kokolakis, S. & Karyda, M. (2008). Process-variance models in information security awareness research. *Information Management and Computer Security*, 16(3):271-287.

Turner, D. W. (2010). Qualitative Interview Design: A Practical Guide for Novice Investigators. *The Qualitative Report*, 15(3):754-760.

Upfold, C. & Sewry, D. (2005). An investigation of information security in small and medium enterprises (SME's) in the Eastern Cape. Available from: http://eprints.ru.ac.za/2702/

Urban, B. & Naidoo, R. (2012). Business sustainability: empirical evidence on operational skills in SMEs in South Africa. *Journal of Small Business and Enterprise Development*, 19(1):146-163.

Veiga, A. D. & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, 11(1): 196-207.

Zuboff, S. (1985). Automate/Informate: The Two Faces of Intelligent Technology. *Organizational Dynamics*, 14(5):5. Available from: http://connection.ebscohost.com/c/articles/4637632/automate-informate-two-faces-intelligent-technology

Addendum A: Information technology dependency tool

Question 1:

How many individual employees in total are employed or contracted by the business organisation?

According to the Small Business Development Act of 1996, can this business be defined as a small business organisation that exists in Gauteng, South Africa?

Yes	No

Question 2:

Does the business have any visible Information Technology that is used by the employees of the small business organisation?

Yes	No

Question 3:

From the Information Technology use in the business, can you think of any which cannot be replaced with a manual (no technology use by the business) process? Please describe the process.

Yes	No

Question 4:

a) *From the above question, describe the information that is used within this business process.*

b) *Is the above described information personal or sensitive information which makes it relevant to the described population criteria?*

Yes	No

Addendum B: Interview Questions

Question 1:

Describe the changes in the use of IT within your organisation since employment with the organisation?

Yes	No

Question 1a: Organisational change

Do you support the change that Information Technology brings to your business organisation?

Question 1b: IT Critical business process

Describe the business processes you would consider dependant on Information Technology

Question 1c: Dependency Behaviour

How would you respond to a failure of Information Technology in a critical business process?

Question 2a: Finance and sensitive information

Describe how your organisations financial systems are supported through Information Technology

Question 2b: Online banking

Do you think there is a risk for your organisation to use online banking?

Question 2c: Banking behaviour

How would you respond to an e-mail requesting you to log in to your online bank account?

Question 3a: Information Technology Failure

Describe the failures in the business you have observed in which information technology was involved

Questions 3b: Information loss

Does your loss involve the loss of personal or sensitive information?

Question 3c: Information Behaviour

Where do you keep the personal information that is kept by the organisation?

Question 4a: Passwords

Does your organisation make use of Passwords?

Yes	No

Question 4b: Password Behaviour

Which password would you consider the most secure?

- *Qwerty*
- *123456789*
- *p@$0mn%*
- *password1*

Question 4c: Password Complexity

Please describe the use and complexity of the password.

Question 5a: Phishing

How would you respond to an e-mail from your bank asking you to "follow a specific link and to confirm your personal details?" (Kruger, Flowerday, Drevin, & Steyn, 2011.)

Question 5b: Phishing understanding

Please elaborate on your understanding of phishing.

Question 5c) Cyber threats

Explain the cyber threats your business is concerned about

Question 6a: Illegal software

Does your business make use of licensed software without paying royalty fees?

Question 6b: What Information Technology software applications does your organisation make use of?

Question 6c: What information is processed through the mentioned software in Q8b?

Question 7a: Antivirus software

Do you make use of Anti-Virus software to protect your information technology?

Yes	No

Question 7b: Technology mitigating techniques

Describe the mitigating techniques that your organisation use to protect its information technology

Question 7c: Information protection

Describe how the organisation protects its information

Addendum C: Interview transcribes

Organisation 1:

IT dependency tool

Question 1:

How many individual employees in total are employed or contracted by the business organisation?

6 permanent employed – daily basis, 1 technical vendor, 2 other people on a contract basis,

According to the Small Business Development Act of, 1996 can this business be defined as a small business organisation that exists in Gauteng, South Africa?

[✓ Yes]	No

Question 2:

Does the business have any visible Information Technology that is used by the employees of the small business organisation?

[✓ Yes]	No

Question 3:

From the Information Technology use in the business, can you think of any which cannot be replaced with a manual (no technology use by the business) process? Please describe the process.

[✓ Yes]	No

Question 4:

a) *From the above question, describe the information that is used within this business process.*

b) *Is the above described information personal or sensitive information which makes it relevant to the described population criteria?*

[✓ Yes]	No