Cape Peninsula
University of Technology

INFORMATION SECURITY IN HOSPITALITY SMMEs IN THE CAPE METROPOLE AREA: POLICIES AND MEASURES IN THE ONLINE ENVIRONMENT

by

DAVID SEIKOKOTLELO BEDI

202056600

Thesis submitted in the fulfilment of the requirements for the degree

Master of Technology: Office Management and Technology

In the Faculty of Business

At the Cape Peninsula University of Technology

Supervisor: Dr. Stuart Warden

Cape Town Campus

December 2013

CPUT copyright information

The dissertation/thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

DECLARATION

I, David Seikokotlelo Bedi, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed **Date**

ABSTRACT

In the past Small Medium and Micro Enterprises (SMMEs) used to be confined to a particular geographical location to conduct their business. This is no longer the case especially since the introduction of the internet. The World Wide Web (Web) now offers SMMEs an opportunity to market, communicate, advertise, purchase and sell goods and services online 7 days a week, 24 hours a day around the globe. However, doing business online is not without risk, as companies also have to ensure that they have adequate security measures in place. SMMEs need to be kept updated on security threats that keep on emerging. They need to keep their information secure in order to avoid unnecessary losses. The advances in modern technology, especially with computers that are connected to the internet have resulted in SMMEs being exposed to cyber-attacks. In most cases, these companies do not have the financial muscle to effectively address such data breaches. Even though cyber-attacks are on the rise, hospitality SMMEs still leave themselves vulnerable to these attacks. Data breaches can be a result of both internal and external attacks. Research indicates that internal attacks are not easy to detect thus making them more deadly than external attacks. It is therefore, important for SMME to come up with policies that will curb inside attacks. However, information security policies are not common amongst hospitality SMMEs.

SMMEs are not always aware of the risks that they are exposed to even though their customers expect them to keep information secure whenever they conduct online business. Most of the hospitality SMMEs are expected to provide online bookings. Credit cards are commonly used in this instance and if the information is not kept secure, companies may face lawsuits from customers. Even though the majority of the hospitality SMMEs indicate that they keep credit card data secure, there are still cases where some do not ensure secure transactions whenever credit card information is exchanged. Vulnerability assessment in order to check if there are any loopholes in networks is rarely carried out by SMMEs. These companies hire IT experts on a temporary basis; further exposing themselves as they there is no one to monitor their networks on a daily basis. In most cases SMMEs believe that technology is their answer to security problems. They omit the human aspect of security.

Even though SMMEs indicate that data loss is one of the challenges they are facing, they still fail to put measures in place to address this. This research examines measures and policies implemented by hospitality SMMEs in their quest to address

data security breaches. Only hospitality SMEs that are connected to the internet are used in this research.

ACKNOWLEDGEMENTS

First of all I would like to thank God for giving me strength and courage to effectively conduct this research. I wish also to express my sincere gratitude to my supervisor, Dr Warden, for his support, guidance and encouragement throughout my research activity. A special word of thanks to the following people:

- Ms Corrie Uys for helping with statistics
- Mr Godwin Kaisara for his advice
- Mr Laban Bagui who took time going through my thesis
- The SMME Managers who availed themselves for the study
- Friends and colleagues for their advice, encouragement and support
- My fiancé who stood by me despite the circumstances

I would also like to thank my family for their undivided support, encouragement and understanding and their financial support. My special thanks to my brother Keabetswe Bedi, my sisters Onyana Bedi and Ranolang Watlhaga for the support they gave me, both financially and emotionally.

DEDICATION

I would like to dedicate this thesis to my mother who had to endure many questions from relatives as she was always defending me. Ke a leboga Selolonyane Thobega. Le wena Ntate, Tshegofatso Thobega, this piece of work will surely put smiles in your faces. A Modimo a le segofatse betsho.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

GLOSSARY

Abbreviations	Explanation
ICT	Information and Communication Technology
SMMEs	Small Medium Micro Enterprises
SMEs	Small Medium Enterprises
GDP	Gross Domestic Product
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
IT	Information Technology
PCI	Peripheral Component Interconnect
DTI	Department of Trade and Industry

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1 Introduction

Organisations are increasingly conducting their business electronically, in spite of identified security issues that businesses need to contend with (Coertze, Van Niekerk & Von Solms, 2011:1; Gupta & Hammond, 2005:297). For these business activities, information and the integrity of information, is of paramount importance (Coertze *et al.*, 2011:1). There are several factors that contribute to the success of business. One of these factors is information, which can greatly contribute to the success of a business if managed well, in conjunction with information systems (IS). In multi-national companies, information is increasingly becoming a production factor, but small businesses lags behind larger businesses when it comes to exploiting information for competitive advantage (Goucher, 2011:18; Lybaert, 1998:171). Sharma and Bhagwat (2006:199) state that information is the backbone of every business irrespective of its size or operation. It is certainly relevant in today's business environment where geographical distance is no longer an issue because of the internet. Flowerday and Von Solms (2005:605) define information as the "oxygen of the modern age". Several organisations rely on information for their success (Geber, & Von Solms, 2001:581) rather than on physical goods and services (Flowerday & Von Solms, 2005:605). Information, being the backbone of most businesses, is stored in different formats. It can be stored online, transmitted from one network to another, printed, sent via fax, stored on tapes or compact disks and can be sent as emails, to name a few. Therefore, it should be emphasised that no matter in what format information is stored; it should be protected in order to avoid unauthorised disclosure, manipulation, modification or destruction (Gerber & Von Solms, 2001: 581).

Most organisations use Information Systems (IS) as part of their business procedure where they make use of information. Therefore, security should be carefully considered as most organisations' business processes are incorporated into each other. For example, buying and selling goods all rely on IS (Kankahalli, Teo, Tan and Wei, 2003:139). Zuccato (2007:256) is of the opinion that IS should be protected by means of information processing system security. Whittman and Matford (2005:8) define information security as protection of information and its supporting elements, which include systems and hardware that are used to store and transmit information.

The main goal of information security is to ensure that an organisation's information assets are not disclosed to unauthorised personnel (Wiant, 2005:451). Shoniregun, Nwanko, Imafidon and Wynarczyk (2005:67) cite a study by the South African Department of Trade and Industry, which indicates that two thirds of small businesses that have sensitive information have suffered serious security breaches. These breaches and statistics highlight the real risks of an attack on a website and the scale of the problem, which appears to be heading out of control. The report reveals for example, that small businesses which were attacked by hackers tripled in 2004, while four out of five businesses were attacked by either a virus or had been a victim of online fraud (Shoniregun et al., 2005:67). Organisations are increasingly conducting their business electronically, in spite of identified security issues that businesses need to contend with (Coertze, Van Niekerk & Von Solms, 2011:1; Gupta & Hammond, 2005:297). For these business activities, information and the integrity of information, is of paramount importance (Coertze et al., 2011:1).

1.1.1 Small Micro and Medium Enterprises (SME)

Different countries use many definitions to describe small businesses, typically, Small and Medium Enterprises (SMEs). One country may define SMEs as enterprises with less than five hundred employees, while in another country, SMEs may be defined as enterprises with less than two hundred and fifty employees (Ayyagari, Beck & Dermiguc-Kunt 2007:415). However, many governments have emphasized the importance of promoting their SMEs (Carron, Lund-Thompsen, Chan, Muro, Bhushan, 2006: 980). SMEs play an important role in economic development because of their dynamic structure and flexibility which gives them the opportunity to acclimatize to changes in their different business environments and economic variations. These companies usually come up with innovative ideas and products, provide employment opportunities in the region they are operating in and also help improve the gross domestic product (GDP) of their home countries (Senol, Akturk & Demirel, 2008:480). Nkwe (2012:29) avers that the development of these companies can contribute to poverty alleviation as well as growing a generation of potential entrepreneurs. For example, Venesaar and Loomets (2006:8) found in Estonia, that SMEs amount to 80 percent of total industry turnover.

In the case of South Africa, an important new category is included; Small Medium and Micro Enterprises (SMMEs). SMMEs also play a role in the development of the local economy, particularly in a developing country (Zindiye & Mwangolela, 2007:90; Thurik & Wennekers, 2004:141).

South African SMMEs are defined according to the industry in which they operate. In the catering and accommodation industry, they are enterprises that:

- have a total financial turn-over of less than 64 million rand per year;
- have total assets of 10 million rand excluding fixed assets, and
- employ less than 200 hundred people (South Africa, 2003).

SMMEs are important to the South African economy as they are a valuable source of employment and assist in upgrading human capital (Dallago, 2004). This may aid South Africa, which is facing the difficult task of trying to establish its economy in order to transform itself into a world class economy. As this activity is proceeding the country is also trying to meet the expectations of its people by making sure that democracy is maintained. It is postulated by Kesper (2001:172), that in order to achieve the above, the role of SMMEs needs to be scrutinised and emphasised. SMMEs can also be used to achieve a dynamic and flourishing private sector by increasing exports, as well as maintaining industrial competitiveness (Zindiye & Mwangolela, 2007:90; Smallbone, Welter, Isakova & Slonimski, 2001:254).

The hospitality industry SMEs are likely to be affected by credit card fraud than SMEs in other industries (IDA, 2008; Ragan, 2009). This is because payment card transactions have become a critical part of the hospitality industry (Berezina *et al*., 2012:992).That being the case, SMEs in the hospitality industry lack the necessary experience to effectively deal with online data breaches as a result putting their information resources at risk. These companies rely on limited resources and budgets and as a result fail to provide security for their networks and customer information (IDA, 2008). According to a survey by Cobanglu and DeMicco (2007:43), 20 percent of 234 hotels that were surveyed experienced network intrusion in the 12 months prior to the study. It is reported that virus attacks were the most common threat. The other persistent problem was denial of service where 7.5 per cent of hotels experienced this problem.

SMMEs in the hospitality industry increasingly conduct their business online. The internet allows customers to access SMMEs websites for reservations as well as obtain information about the services they offer. This type of interaction can be detrimental to the company's information if it is not monitored (Cobanoglu & DeMicco, 2007:45). Connecting the business to the internet can be risky at times because unauthorised people can take advantage and access sensitive information (Posthumus & von Solms, 2004:641).

The literature referenced in this section, spanning over ten to twelve years clearly points to the dangers SMMEs in the hospitality industry are facing today to protect their information while increasingly needing to trade online. It is also over this period that the internet became a dominant technology and rapid changes in technology, business processes, marketing methods and the niche positioning of SMMEs, has led to such a complex issue of security. This research is focussed on the security related issues hospitality SMMEs are facing. The final outcome of this research proposes guidelines to alleviate many problems facing these SMMEs.

1.2 STATEMENT OF THE RESEARCH PROBLEM

SMMEs are faced with a challenge to protect of protecting information as well as ensuring customer transactions whenever they conduct business with them. Advances in modern technology have led to vulnerabilities in security and privacy which is a challenge for SMMEs. More and more information is created and transformed into digital format, saved in different storage devices and sent via the internet (Tawileh, Hilton & McIntosh, and 2007:1). Tawileh *et al*. (2007:1) cite Householder, Houle and Dougherty (2002:5) indicating that the growth in internet usage has changed the way the corporate world conduct their business in order to achieve their goals. As a result, a number of companies, especially SMMEs are struggling to draft policies and measures due to lack of guidance from an experienced information security expert (Coertze, Van Niekerk & Von Solms, 2011:2). It is common that companies such as SMMEs that are not constricted by audit procedures and compliance regulations omit security and put it lower on the priority budget list (Goucher, 2011:18). Crimes such as spam, phishing, viruses, identity theft, and hacking have plummeted making it difficult for companies to effectively deal with information security. In South Africa, SMMEs have not established adequate policies and measures to protect their information (Caralli & Wilson, 2004; Coertze *et al*., 20011:2).

Considering the many issues discussed, the research problem identified by the researcher within the ambit of this thesis is stated as:

SMMEs within the hospitality industry do not have sufficient procedure to protect their information as well as customer information in an online environment.

In an effort to solve this stated problem, an appropriate research question with a number of research sub-questions is formulated. These are provided in Table 1.1 and include appropriate research methods and objectives.

Table 1.1: Research questions summary

RESEARCH QUESTION	**What policies and measures do SMMEs use to protect their information as well as ensuring adequate customer information protection in an online environment?**	
RESEARCH SUB-QUESTIONS	**RESEARCH METHOD**	**OBJECTIVES**
What are the trends of information security both locally and internationally?	Literature analysis	To find trends in information security and how they have evolved over time
What policies and measures are in place for businesses to ensure customer security when conducting online business?	Literature Analysis/Survey	To find out what measures have been put in place by SMMEs to ensure secure online transactions.
To what extent is security training provided in hospitality SMMEs?	Literature/Survey	To find out whether SMMEs in the hospitality industry provide training for their staff members or not.
What are hospitality SMMEs doing to protect customers in an online environment?	Literature/Survey	To understand procedures and policies in place by hospitality SMMEs to protect customers in an online environment.
How is credit card fraud dealt with in hospitality SMMEs?	Literature/Interviews	To find out what hospitality SMMEs are doing to address credit card fraud.

1.3 AIMS OF THE RESEARCH

The aim of the research is to understand the challenges that hospitality SMMEs face as they try to address online security as well as ensuring adequate customer security. Considering that SMMEs in the hospitality industry are expected to be connected to the internet so that they can cater their customers. On the other hand, they are also expected to put adequate measures in place to ensure smooth transactions. Basically the research intends to provide some understanding of some policies and measures that have been put in place by hospitality SMMEs to address security breaches in an online environment. A number of models were considered to help hospitality SMMEs to address these breaches.

1.4 CURRENT STATUS OF THE RESEARCH

The global network has provided both multi-national companies and SMEs with an opportunity to trade online (Tawileh *et al.,* 2007:1). Goucher (2011:18) avers that it will be wrong to speculate that inadequate security deployment by SMEs can be attributed to high costs that are associated with buying online and, more importantly, hardware maintenance, anti-virus and other software tools, which are necessary for the protection of information and security related systems. Most of the time, the problem arises from lack of understanding and awareness of security matters (Goucher, 2011:18). The crux of the problem is that SMEs are in the dark about the risk or the consequences (Goucher, 12:2011). On the other hand, Caralli and Wilson (2005) admit that SMME's are not willing to make long term investments on security management because they are concerned about losing qualified personnel to large companies, therefore proving that they understand the importance of information security. However, Goucher (2011:18) dismisses this by disclosing that "if one digs deeper into the piece there are indications that the SMEs questioned may not have been very clear about the security issues".

1.4.1 Online security in SMEs

Online security issues exist since people owning companies have realised the importance of information, especially with the interconnection of computers in recent years (Isomaki & Bilozerov, 2011; 298). With the adoption of e-commerce, SMEs are now facing a difficult and complex situation (Robinson, 2001:12). Many SMEs are lagging behind when it comes to secure online transactions (Robinson, 2001:12; Yildrim, Akalp, Aytac & Bayram, 2010: 361). These companies still have a long way to go to emulate large businesses which are already responding to customer demand for cashless payment schemes, automation of sales programmes, supply chain integration applications, secure database access for employees working in remote areas and secure web access and messaging (Robinson, 2001:12). The gap between large companies and SMEs in addressing online security has been widening substantially as a result of scarcity of resources available to SMEs (Tawileh, Hilton & Mcintosh, 2007:332). This is not helped by the fact that SMEs believe that they are not a target. SMEs believe that attackers are only interested in large companies because they have more financial resources to tap into (Ribeiro, 2012). Researchers however indicate that SMEs, which are more vulnerable, are always a target (Millard, 2007; Morgan, 2006:3; Park *et al*., 2008: 92; Ribeiro, 2012).

1.4.2 Information security in SMMEs in South Africa

Similar to Europe, where a number of countries have used SMEs as a platform towards industrialisation and economic development, South Africa can also use SMMEs as a tool to curb unemployment (Berry, Von Blotnitz, Cassim, Kesper, Rajaratnan & Van Seventer, 2002). Zindiye and Mwangolela (2007:90) indicate that SMMEs can play a major role in South Africa, since formal employment opportunities have not increased as expected.

South Africa is still in the process of publishing its final National Cyber Security Framework (Kortjan & Von Solms, 2012:5). Many SMMEs are finding it difficult to put adequate security measures in place because of costs escalation. As a result of this lack of resources, these companies are experiencing challenges in implementing information security policies as well as monitoring their implementation model (2011:1). SMMEs are more vulnerable when it comes to recovery and knowing what to do in the event of a security incident or breach. According to a survey conducted by Upfold and Sewry (2005), 47 percent of respondents reported that they do not have any procedures and policies in place for recovery processes. Conversely, 65 percent of respondents believe that they have appropriate mechanisms which authenticate users to log into the system. Even though SMME's are aware of the need for information security, in many cases, this awareness is minimal. Virus protection and data back-ups are the most commonly used means of security precautions by SMMEs (Upfold & Sewry, 2005).

1.4.3 Information security in the hospitality industry

In order for SMMEs to be competitive in this sector, they require technology, amongst other things. There are a number of factors that contribute to technological advancement in the hospitality industry such as increased transaction volumes and international communication needs (Berezina, Cobanoglu, Miller & Kwansa, (2012:992). These advances led to the application of computer systems technology (Cobanoglu & DeMicco, 2007:44). As technology usage increases, the number of security breaches that occur in the public and private sectors increases as well, and as a result these organisations might suffer financially (Garg, Curtis & Halper, 2003: 74; Flink, 2002). Ever since the adoption of modern technology by the hospitality industry in the 1970s, information security problems have persisted (Berezina *et al*., 2012:992).

South African hospitality SMEs have not been fortunate when it comes to data breaches. A study by Bedi and Warden (2009:9) discloses that 82 per cent of the respondents who took part in their study suffered a data breach of some sort.

1.5 RESEARCH METHODOLOGY AND DESIGN

According to Struwig and Stead (2001:44), a methodology is the overall procedure that is followed in the data collection in order to gain knowledge. Leedy (1997:144) avows that there are various methods that can be followed in data collection and analysis. For this study, Mixed Method was followed. It was considered appropriate because it offered the researcher the opportunity to simultaneously generalize from the sample to the population as well as gain richer contextual understanding of the phenomenon that is being investigated (Creswell, 2007:208).

Research design is the overall method that has been followed in the data collection (Leedy, 1997:93). Sequential explanatory method was used for this study. This allowed the researcher to explore the findings collected through the quantitative method and understand some problems that are facing hospitality SMMEs. In other words, the results that were collected through quantitative research were used to draft questions for interviews considering that credit card fraud was not effectively dealt with in the survey study (Cresswell, 2008:215). Explanatory design analysis was then used in the data analysis. This method is commonly used whereby the quantitative method was used first to collect data. Then the researcher considered extreme cases, and followed them up with the qualitative research method.

1.6 DELIMITATION OF THE RESEARCH

The target group for this study are hospitality SMMEs conducting their business in the Cape Metropole area. The research will focus on travel agencies and accommodation providers. The industry was selected based on the fact that tourism plays an important role in the embellishment of the economy and the industry has also increased its offerings to the customers (Berezina et al., 2012:992). The fact that employees in the low-level section of these companies have access to key customer information (Sharma, 2013) and the fact that these companies tend to use out-dated systems for their operation (Ragan, 2009), makes this study relevant. According to Sharma (2013), the hospitality industry deals with a vast range of information such as customer information, employees' information and guest information. In most cases, SMMEs fail to comply with the PCI-DSS standards. Cape Town is one of the most

popular destinations for international, regional and domestic tourists (George, 2010:806).

1.7 ASSUMPTIONS OF THE RESEARCH

The expected results from the study are that SMMEs in the hospitality industry do not have adequate procedures to deal with the increasing security breaches. Considering that SMMEs tend to lack the financial resources to invest in information security, it is expected that these companies' security application will be basic.

1.8 CONTRIBUTION OF THE RESEARCH

New and advanced technologies provide hospitality SMMEs with opportunities but they also introduce them to risks. As is the case with big companies in this industry, SMMEs are expected to be connected to the internet in order to effectively cater for their clients who might be from outside the country and expect their information to be handled in a proper way. This research contributes to the body of knowledge by providing information on the perceptions of information security related issues based on the study of hospitality SMMEs in Cape Town and it also provides guidelines on how SMMEs can address the increasing security breaches in an online environment.

1.9 LIMITATIONS OF THE RESEARCH

Considering that the study only considered hospitality SMMEs that were connected to the internet, this resulted in a low response. These companies tend to rely on consultants for their IT services, and it was a challenge to meet the managers from these IT companies as some of them were only hired on a part time basis.

1.10 LAYOUT OF THE THESIS

Chapter 1 provides an introduction and background to the research problem. The purpose, scope, research problem as well as research questions were also outlined in this chapter. The methodology and research limitations also were part of this chapter. Overall this chapter is the introductory chapter.

In chapter 2 a review of information security is presented. The benefits and risks of online trading were also discussed. Research sub-questions 1 and 2 were also answered in this chapter. The chapter also examines benefits of information security policies and human aspects in information security.

In Chapter 3, a detailed explanation of the methodology and design of the research were discussed. The reasons for selecting the mixed method research were also discussed in this chapter.

Chapter 4 provides the presentation of the results. Both survey results and interviews were presented in this chapter.

In chapter 5 the results are discussed in detail. Data interpretation was also conducted in this chapter.

Lastly, Chapter 6 provided the conclusion. The research questions, aims of the research and findings are revisited and the final conclusion is drawn. The limitations of the study were also discussed in this chapter.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

In this chapter literature is reviewed and salient issues regarding information security are identified. In Chapter 1, the research question and five research sub-questions are formulated amongst others, while in this chapter, the extent of information security literature research is explored by answering research sub question one (section 2.6) and exploring the background to research sub questions two to five in sections 2.7 through 2.10. The terms SME and SMMEs are used in the same context, but with the understanding that the term SMMEs pertains to South Africa.

Information security has grown from addressing minor security issues to more serious breaches which can cripple a company if not addressed timeously (Siponen, Mahmood & Pahnila, 2014:217). In the past, information security adoption by companies meant dealing with issues such as viruses and worms that were not always catastrophic or too harmful to continue using business systems. However, the landscape started changing as more and more computers got connected to the internet (Dlamini, Eloff & Eloff, 2009:189; Kim, Lee & Ham, 2013:369). Currently, many different security problems are experienced by companies (Von Solms & Van Niekerk, 2013:97). These include technical software failures or errors, deliberate software attacks, mistakes, social engineering, deliberate act of sabotage or vandalism, failures as a result of hardware problems, stealing deliberately, natural disasters and many others (Rezqui & Marks, 2008:243; Von Solms & Van Niekerk, 2013:369). Virus related issues remain a threat to data and information (Dlamini *et al.,* 2009:189)

Information plays an important role in most companies and should therefore be protected (Barlette & Formin, 2008:1, Feng, Wang & Li, 2014:57) and kept secure at all times (Clear, 2007:1). The increase in the use of information and communication technologies (ICT) has contributed to a rise in the number of security breaches (Berezina *et al*., 2012:992). It is estimated that the annual average increase of information security vulnerabilities in developed countries is more than 45 percent per year (Barlette & Formin, 2008:1). SMEs face a difficult task of managing security threats and vulnerabilities (Onwubiko & Lenaghan, 2007). In France for example, 75 percent of companies indicate that they rely on their information resources for survival (Barlette & Formin, 2008:1). In order to effectively address these threats, organisations are forced to invest in information security protection. Information security policies are a stepping stone towards achieving secure networks.

Without proper security policies, a company's information security resources could be compromised (Knapp, Morris, Marshall & Byrd, 2009:493).

2.1.1 Security models

The researcher explored a number of security related models that could possibly be used as a foundation to base this research upon. Four models are briefly discussed.

The GRC security model by Jirasek (2012:2) focuses on the way in which managers and CIOs can improve information security in their companies. The model proposes information security model drivers. It also identifies three major factors that can assist to address information security threats. These factors are:

- ***Laws and regulations***: These are some of the procedures that companies must face with respect to legal action or fines. Abiding by data protection laws is an example of a legal driver. On the other hand, abiding by PCI DSS is an example of regulation drivers.
- ***Business objectives:*** These are when companies come up with a set of business objectives to make profit. Security will then support these business objectives by protecting systems and information that is used in the business processes. For example, with regard to the Microsoft Windows protection code, if the source code was not protected, people could have installed Windows without paying Microsoft licence fees.
- ***Security threats:*** They work against laws and regulations and business objectives. However, they improve information security as well as company needs to respond to threats in order to satisfy the first two drivers (Jirasek, 2012:2). This model was developed to help multinational companies to effectively deal with information security. SMMEs cannot use this model. The model requires a whole lot of professionals and SMMEs lack of finance will be a barrier.

Another model that was considered is the body of knowledge for information security suited to industry by Kritzinger and Smith (2008:226). This model's main aim is to make sure that the non-technical issues of information security are balanced to ensure that the technical issues do not overshadow the non-technical issues in information security.

A number of accomplished nationally and internationally accepted information security documents have been used as the core of the proposed body of knowledge of information security. The documents were compiled by information security experts and contain information regarding the implementation and management of information security issues. The proposed body of knowledge model is divided into technical information security and non-technical issues. Firstly, the model's aim is to make sure that information security issues remain at a low level. Secondly, the division will assist to ensure that technical information security issues do not overshadow the non-technical issues of information security (Kritzinger & Smith, 2008:226). This model was developed as part of the basis for information security retrieval and awareness and it proposes two issues; diverts attention to users with little or no formal background on how to properly secure information they work with, while not excluding professionals. Considering that this model focuses on users and omits other issues, it was not chosen as the basis of this research.

A model of incident response capability proposed by Qian, Fang and Gonzalez (2012:862) provides guidelines for procedures to improve incident response. Accordingly, the model highlights that an increase in incident reports depends on the investment made by management. This is in turn based on the desired incident response capability. Management will then be able to make investments to adjust the incident response capability to their desired level. It should be emphasized that it takes time to build incident response capabilities. The desired incident response capability relies on the perception of frequency of incidents. The model is used to deal with the perception of the frequency of incidents. Some incidents might go undetected as a fraction may escape detection. The size of this fraction depends on the adequacy of the incident response capability. The more the number of detected incidents occur, the more management become convinced that incidents are occurring, and they would realise information is at risk. It is therefore important to organise more incident response capabilities to handle incidents that might arise (Qian *et al*., 2012:862). This model was not adopted because it is based on incident response, especially that SMMEs do not have the financial muscle to just allocate for one activity such as incident response. This model is best suited to companies that are willing to allocate funds for security and hire a number of specialists to focus on different issues pertaining to security infrastructure. Basically if more incidents are detected, perceived information security risk rises, leading to more investment in incident response capability, something which SMMEs might not be prepared for.

Knapp *et al*.,(2009:499) developed an information security model that is comprehensive and directly influences policy development, security training the entire security management as depicted in Figure 2.1. The model emphasizes that information security governance is not merely an internal process but it is also made up of external attributes such as the involvement of the company's top management. It also indicates that internal and external influences play an important role in influencing the entire policy management. For example, while legal and regulatory requirements will affect the content of the company's security policies, legal requirements can also restrict how companies engage in monitoring and surveillance (Knapp *et al*., 2009:499). The model proposes that one of the common ways of coping with information security risk is by establishing training and awareness programmes. It advises SMEs to provide training to employees to sensitize them about security threats and to encourage them to support organizational policy (Tuyikeze & Pottas, 2010:172). Employees' awareness is mentioned as one of the challenges in making sure information security is accomplished. The model further illustrates the individual processes, such as monitoring, that have an on-going characteristic. Companies tend to consider information security as a technical issue rather than a comprehensive issue that needs to be embraced by everyone in the company (Knapp *et al*., 2009:500)

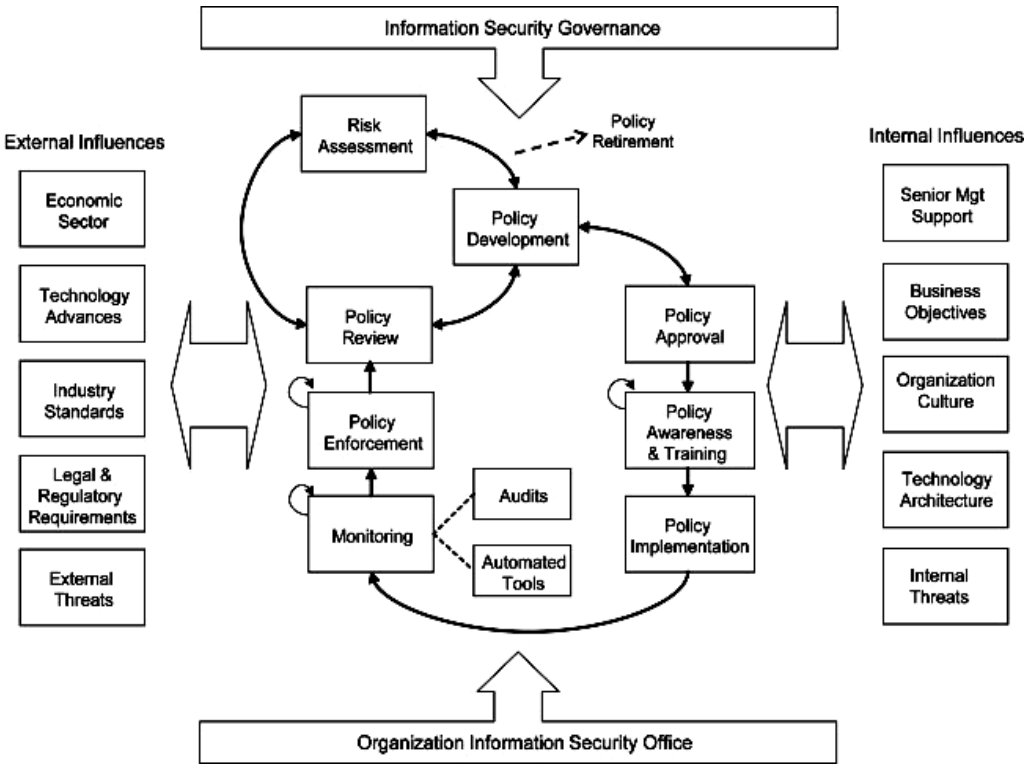

Figure 2.1: Information security model (Adapted from Knapp *et al*., 2009:499)

The model in Figure 2.1 is adopted as the basis for this research to assist hospitality SMMEs to curb security breaches. The main reason for adopting this model is that it identifies four areas considered to have an effect on security. These are: external and internal influences, information security governance and organisational information security office activity. Not all aspects in the model are used, but considering that hospitality SMMEs are expected to be connected to the Internet, it is critical that they avoid compromising customer data at all costs. This model was adopted to devise ways in which hospitality SMMEs can implement training, make use of security policies as ways of dealing with online security. Taking into consideration the fact that information security is generally a management problem, the security culture of the organisation will therefore play an important role in reflecting how management handles and treats security challenges (Knapp *et al*., 2009:501).

2.1.2 Chapter 2 layout

Figure 2.2 represents the literature layout as discussed in this chapter. Only the main headings are listed in the figure.

Considering the role being played by information technology presently amongst businesses, information security should be incorporated into a company's daily business (Chang & Lin, 2007:440). Information should be protected, particularly owing to the volume of transactions conducted on the Internet (Maswera,Dawson& Edwards, 2008:187; Simmons & Burgess, 2000).

2.2 BACKGROUND TO THE RESEARCH

In this section, aspects of e-commerce applications in SMMEs are discussed in points 2.2.1, 2.2.3 to 2.2.4. Some of the benefits of online trading for hospitality SMMEs are also covered. The reason for including these topics is to introduce e-commerce and its importance to SMMEs. When SMMEs adopt e-commerce they also need to put measures in place to address security issues. It is evident that companies need to adopt e-commerce if they are to effectively compete in today's markets.

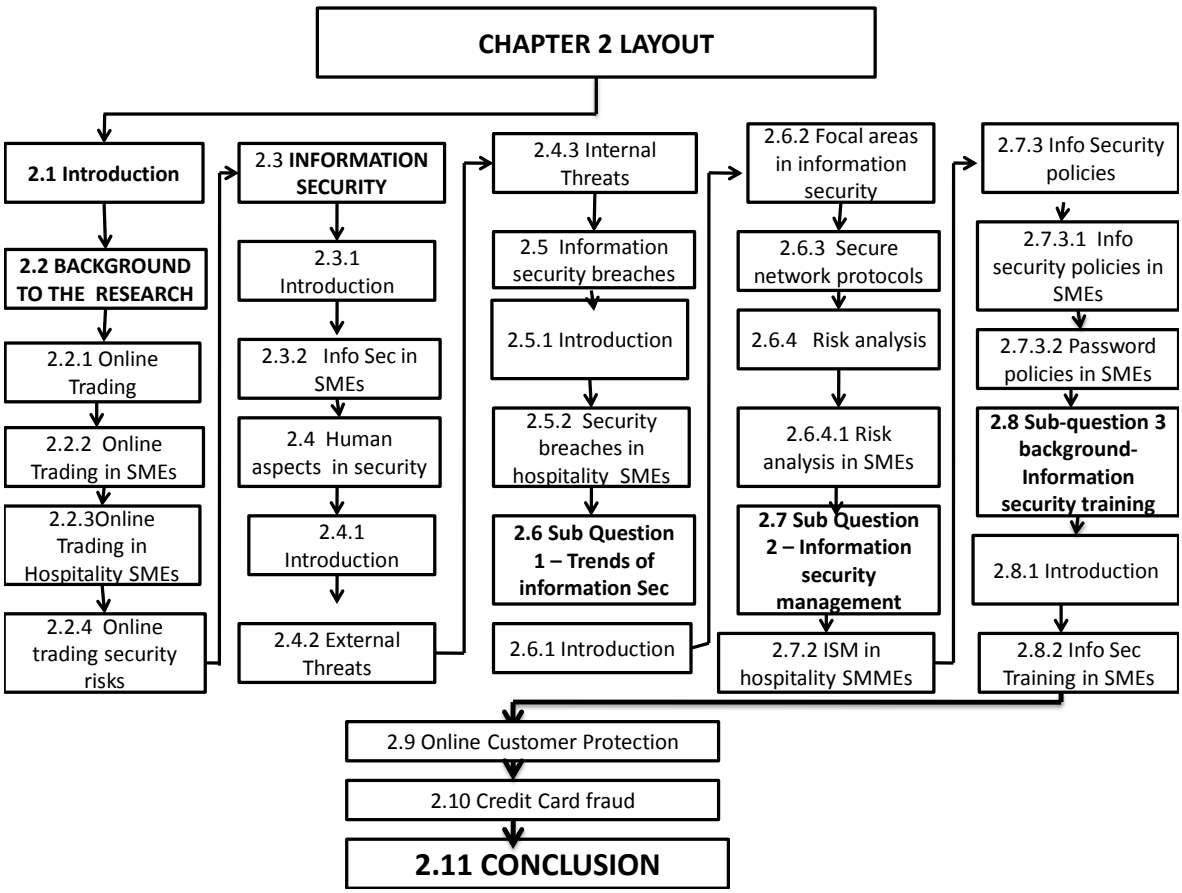

Figure 2.2: **Chapter 2 Layout**

2.2.1 Online trading

An increase in communications technology as well as Internet penetration has facilitated the growth of online trading (Berezina *et al*., 2012:992; Jamaliddin, 2013: 140; Wang & Lin, 2009:2750). Online trading provides companies with the opportunity to effectively provide service online to customers around the world (Damanpour & Madison; Masweraet *al*., 2008:187; 2001:16; Wang & Lin, 2009:2750). The availability and increase in usage of the Internet led to surge in e-commerce (Pozzi, 2013:677; Yao, 2004:54; Nakayama, 2009:239). Companies now use the Internet as a way of expanding their businesses (Berezina et al., 2012:992; Bharadwaj & Soni, 2007:501; Wang & Ahmed, 2009:17). In the United States for example, e-commerce has been growing constantly at double digits since 2008 (Bahmanziari, Odom, & Ugrin, 2009:152). In South Africa, e-commerce is on the rise as well and it is estimated that South Africans spent over 2 million Rand buying goods or services online in 2011 (Gordon, 2011). Online trading has the ability to add value to the way companies operate. Therefore, it assists in improving their operations, especially in developing countries (Kshetri, 2007:443). Online trading has also resulted in a change in the way businesses relate to each other, including business-supplier,

business-client, business-to-end consumer relationships and strategic alliances (Wang & Lin, 2009:2750).

Online trading is no longer an option, but a necessity in modern business practice (Damanpour & Madison, 2001:19; Kim, Chung & Lee, 2011:257). Warden (2007:104) indicates that the rate of Internet use has increased particularly in developing countries and has therefore resulted in an increase in e-commerce transactions as well. Ngai and Wat (2002:415) state that e-commerce has created a new way to conduct business (Lawson, Alcock, Cooper & Burgess, 2003:265; Rao, 2000:54) by providing an opportunity using affordable technology that brings together buyers and sellers, big and small companies from across the globe. Even though online trading was not profitable when first introduced in 2001, it is continuing to contribute to sustainable growth (Doherty & Ellis-Chadwick, 2009:1247; Pozzi, 2013:677). If e-commerce is properly implemented, it can lead to improved efficiency, market share growth or providing competitive advantage (Ferguson, Finn, Hall & Pinnuck, 2010:1).

Companies that lag behind in adopting ICT technologies for e-commerce purposes are likely to lose their competitive advantage. In the United Kingdom and USA, it is estimated that e-commerce accounts for more than 5 per cent of their respective gross domestic products (GDPs) (Xu, Yan & Zheng, 2008:47). The hospitality industry is viewed as one of the industries that embrace the use of the Internet for e-commerce purposes. The Internet therefore, allows customers to reserve accommodation from their own computers and receive near immediate confirmation (Huang, 2008:634; Kim et al., 2011:257). The Internet has proved to be an important channel through which customers and the hospitality industry can mediate in order to acquire information as well as conduct business transactions (Berezinal *et al.,* 2012:992; Bharadwaj & Soni, 2007:635).

2.2.2 Online trading in SMEs

Fillis *et al.,* (2004:181) point out that one of the main benefits that SMEs enjoy by adopting e-commerce, is the ability to access information that was previously accessible to large companies only. A study by Bharadwaj and Soni (2007:508) indicates that 54 percent of SMEs that participated in their study indicated that they "…had improved flow of business" since the adoption of e-commerce. It is predicted that the Internet with its increased usage, will transform the hospitality industry (Kim & Kim, 2004:381; Mapheshoane & Pather, 2012:5). Current economic activities are centralised around online trading and are well suited to SMEs and based on relationships, networks, as well as information. This is in contrast to the past, where size and physical issues played a major role (Peterson, Meinert, Criswell & Crossland, 2007:655). Mashanda, Cloete & Tanner (2012:4) posit that gone are the days that SMEs can ignore the Internet and opt for a wait-and-see attitude. This author reiterates that costs to establish websites have decreased and many SME customers have access to the Internet. By trading online, SMEs are able to carry out a number of business activities (Mapheshoane & Pather, 2012:5; Meinert, Criswel and Crossland, 2007:1462) such as providing catalogues, ordering and payment systems as well as other activities that enhance customer service (Peterson et al., 2007:655).

The Internet and e-commerce provide SMEs with opportunities to gain a competitive edge and the ability to compete with multi-national corporations (Chau, 2003:64; Morgan, 2004; Zuccato, 2007:256), as they can trade beyond their borders without incurring additional costs of erecting new buildings (Moertini, 2012:17; Santarelli & D'Altri, 2003:276). The Internet provides SMEs with an opportunity to market their products online. By using the Internet, SMEs can improve their customer service (Peterson et al., 2007:655; Santarelli & D'Altri, 2003:276). This flexibility is likely to be more advantageous to SMEs than multi-national companies because the decision making process is not complicated in SMEs (Fillis, Johannson & Wagner, 2004:181). By trading online, SMEs are simplifying the process of product search and as a result reduce the process of dealing with too much paper (Mashanda *et al*., 2012:4; Peterson *et al*., 2007:655).

2.2.3 Online trading in hospitality SMEs

As mentioned before, advances in ICTs have changed the way businesses conduct their daily business in many industries including lodging (Berezina *et al*., 2012:991). According to Kim, Chung and Lee (2011:257) the hospitality industry is well suited to using the Internet for a number of reasons. For example; hospitality establishments offer an intangible product, production and consumption cannot be separated, and demand is perishable and keeps on fluctuating (Kim *et al*., 2011:257). E-commerce can also be used by hospitality SMEs to provide efficient transactions as well as improve customer service (Bharadwaj & Soni, 2007:518). E-commerce and tourism are interlinked because the tourism industry is considered to be information intensive (Maswera *et al*., 2008:187). Maswera *et al*., (2008) further add that e-commerce can boost tourism development in Africa due to the variety of attractions such as wildlife, unique resorts and fauna. E-commerce can assist to generate additional revenue by reaching international markets. It provides SMEs in the hospitality industry with the opportunity to set up a direct link of communication with customers and therefore getting rid of barriers between the customers and suppliers (Bharadwaj & Soni, 2007:518).

2.2.4 Online trading security risks

The Internet also brings with it security concerns. If companies connected to the Internet do not effectively address security issues, they can suffer consequences (Tawileh, Hilton & McIntosh, 2008) data breaches such, customer loss, loss of reputation, and can also face penalties (Lee, Kauffman & Sougstad, 2011:905). According to Bharadwaj and Soni (2007:503), governments and organisations at large have identified security and information confidentiality as main factors that deter businesses from conducting online business. Peterson et al., (2007:1462) affirm this by disclosing that only 6 percent of SMEs indicated that they provide online services. There are potential risks that can emanate from online trading especially if online transactions are not well guarded (Bojanc & Jerman-Blazic, 2008:413; Zhoung & Huang, 2009:285). Users are also concerned about Internet privacy and security issues (Bharadwaj & Soni, 2007:503). According to a study by Zheng, Caldwell, Harland, Powell, Woerndl and Xu (2004:35) SMEs in the UK were cautious with online trading because they believed that it exposes them to risks and exposes their information.

The Zheng *et al*., study further revealed that SMEs were stalling in adopting e-commerce because they were concerned that online trading threatens their uniqueness and ability to offer special products. Therefore, interpersonal relationship-based SME business models can be influenced. Peterson *et al*., (2007:656) reveal that trust issues play a role in influencing consumers not to conduct online business particularly with SMEs. The authors further indicate that there are some unresolved security and privacy issues, especially with online payments, which are more pertinent to SMEs.

2.3 INFORMATION SECURITY

In this section, information security applications in both multi-national companies and SMEs, together with stakeholders of information security are discussed (sections 2.3.1 to 2.3.5). Some of the challenges that can be brought by Internet connections in the hospitality industry, are also discussed especially where customers' data is involved. Data breaches are also discussed in order to explore how they affect hospitality SMEs. The reason for including these topics is to reveal to the reader how SMEs, especially hospitality SMEs address information security considering that they deal with customer data on a daily basis. In order for companies in the hospitality industry to be successful, they must be connected to the Internet. As mentioned before, Internet connections pose some challenges.

2.3.1 Introduction

In many cases, security is viewed as "…a barrier rather than an enabler and as a result ends up putting security at a disadvantage in terms of gaining recognition." (Furnell & Thomson, 2009:7). Most companies, private or public, are now dealing with data in a wide range therefore increasing the importance of putting adequate security measures in place to address unauthorised disclosure of personal information (Burdon, Lane & Von Nessen, 2010:115). Furthermore, companies have come to the realisation that in order to effectively compete, they must protect information together with its supporting systems (Chang & Ho, 2006:345, Fulford & Doherty, 2003:106). In the past, physical restrictions to computers was sufficient to deal with security issues, but that has now changed (Desouki & Amstrong, 2010:122; Sveen, Torres & Sarriegi, 2009:95). Kankanhalli, Teo and Wei (2003:140) indicate that increased reliance on ICT has contributed to an increase in security breach impacts.

Bojanc and Jerman-Blazic (2008:217) opine that in most cases threats are moulded merely to attack information, together with its supporting systems. Security threats are escalating and have been increasing ever since the inception of computers, electronic networks, electronic data storage and information exchange (Rhee, Kim & Ryu, 2009:816). A successful attack on a company's computer system can lead to system crash which can cause data loss, and loss of services and business opportunities (Clear, 2007:2; Bojanc & Jerman-Blanzic, 2008:216). Hence, companies have been forced to invest in information security measures as well as data protection devices (Bojanc & Jerman-Blanzic, 2008:216; Fulford & Doherty, 2003:106).

Multi-national companies devote a significant amount of their budget to security products in order to curb security breaches (Rhee *et al*., 2009:816). These companies have increased their expenditure to acquire different products as well as apply policies so as to address security breaches. This indicates that awareness of security threats amongst companies has increased (Gerber & Von Solms, 2008:124). Virus detecting software, firewalls, some encryption devices, intrusion detection devices, and electronic data back-up and hardware equipment are some of the devices that are used by companies as a form of counter-attack against system vulnerability (Rhee *et al*., 2009:816). In order for these products to be effective, a company's management should make it a point that the necessary policies and measures are established to address breaches that might occur as a result of inside attack (Rhee *et al*., 2009:816; Sinogoj, 2004:1). In other words security should be taken as a holistic process to ensure that the integrity of information is maintained (Sveen, Torres & Sarriegi, 2009:96).

According to Stewart (2005:5), "…it might be easy to think that the field of information security is primarily about technology". He further adds that it is a multi-disciplinary field, which comprises different disciplines such as sociology, economics, technology business and law. Conversely, Rhee *et al*., (2009:816) agree that technology plays an important role in information security. Bernard (2007:27) defines "information security" as a process, where information technology plays a major role and physical security application is merely limited to information system physical infrastructure. He further posits that even though physical security is part of information security standards, the majority of information security experts lack the required knowledge to implement physical controls for non-electronic forms of data. Bernard (2007:27) avers that in order to satisfy the definition of information security, all forms of data should be taken into consideration and be addressed by personnel that have the necessary knowledge.

According to Sveen *et al*., (2009:101), in order for these companies to achieve their goals in minimizing security breaches, the following three controls should be implemented:

- Technical controls - include hardware and software used to restrict and limit unathorised access to sensitive information. Some technical control examples include biometric devices, antivirus software, firewalls and intrusion detection devices.
- Formal controls - include policies and procedures that make sure that access and use of information are managed properly. Formal controls also include policies and measures to ensure that technical controls are best utilised.
- Informal controls - . includes steps taken in the company to build a security culture (Sveen *et al*. 2009:1).

2.3.2 Information security in SMEs

The application of ICT without proper measures can place a company's information resources at risk (Beranek, 2010:42; Morgan, 2006:1). Information security investment is not considered a priority amongst SMEs (Goucher, 2011:18). Most SMEs do not want to spend much on security applications as a result making them easy targets for hackers (Rachwald, 2011). Dimopoulos *et al*. (2005:73) contend that a lack of security measures has a negative impact on company information as this can lead to unnecessary loss. The authors reveal that in the UK and the USA, the universities of Plymouth and San Diego respectively are involved in research to determine SME attitude towards security (Dimopoulos *et al*., 2005, 76).

The increase in the usage of the Internet has also resulted in organisations trying to re-evaluate their views on information security regardless of their size (Dlamini *et al*., 2009:189; Tawileh, 2007). SMEs are facing similar security challenges to larger companies (Lee & Jang, 2009:84). Dynes, Brehcbuhl and Johnson (2005:2) assert that SMEs tend to make decisions, albeit with limited knowledge, about different threats that they face as well as the strengths of their systems to effectively deal with data breaches. In most cases, they rely on a few people or an individual that has limited knowledge in terms of information security (Park, Robles, Hong, Yeo & Kim, 2008:91). According to a survey by Dimopoulos *et al*. (2005, 76), SMEs' main form of security is anti-virus software, which is mainly used to keep their systems up-to-date and free from viruses. Even though viruses are considered to be one of the most worrying problems, the survey also proved that internal attack was the Achilles heel. That being the case, a study in Kenya revealed that half of SMEs do not have any measures in place to deal with internal attacks (Kimwele *et al*., 2012:9).

Another study by Tawileh *et al*. (2008:24) indicates that SMEs are not prepared to deal fully with security issues. Their study reveals that over a quarter of the respondents indicated that they do not have documented information security procedures in place to address security breaches. SMEs still believe that they are not susceptible to security threats because they believe that hackers are only targeting large companies (Millard, 2007; Morgan, 2006:3; Park *et al*., 2008: 92). This is no longer the case because many large companies have robust security measures in place as they are expected to abide by security laws (Park *et al*., 2008:92). Tawileh, *et al*. (2008:23) opine that 67 percent of large enterprises surveyed, compared to 17 percent of SMEs surveyed, indicated that they have implemented information security procedures.

There is evidence that cyber criminals are targeting SMEs as they tend to lack security measures (Morgan, 2006:3). In support of this, Kim, Ahn, Lee and Lee (2006) reveal that 74 percent of all hacking took places in SMEs. This being the case, SMEs are continuing to ignore computer security and usage precautions, leaving themselves vulnerable to these attacks (Kim *et al*., 2006). According to Bougaart and Kobe (2011:175) in Cape Town, most of the SMMEs tend to ignore security requirements. This is revealed by a mean score of 2.49 indicating a poor attitude to security requirements. Furthermore, the study reveals that inadequate knowledge of IT risks as well as computing applications were singled out as the main factors that hinder SMMEs from taking effective measures and monitoring of business operations (Bougaardt & Kyobe, 2011:175).

2.3.3 Information security in hospitality SMEs

The researcher finds studies on information security in the hospitality industry limited, verified by Kim, Lee & Ham (2012:1), but finds evidence of credit card fraud, systems compromise, out-dated systems and limiting budgets as being the causes of security compromise. It is evident that one of the challenges that the hospitality industry is facing is credit card fraud (Berezina *et al*., 2012:992; Lee *et al*., 2011:905; Percoco, 2010). According to further research by Trustwave, a PCI vendor and Qualified Incident Response Assessor issued a warning after investigating 75 cases of credit card compromises. In South Africa, EasyPay was hit by a scam whereby hackers managed to steal sensitive credit card information and made purchases of airtime, prepaid electricity and gift cards. EasyPay handles payments worth 120 million Rand a month, with the site growing at 10 percent a month. The hacking occurred over a two month period, and the company was forced to pay money back as rewards to

more than 180 000 customers, as a strategy to restore reputation and to try to regain customer's confidence (Fisher-French, 2011:8)

According to Ragan (2009) large numbers of accounts are under threat. Many of the hotels surveyed were found to have lost data that was stored on magnetic devices as well as out-dated processing systems and technologies. Because these out-dated systems are used to store personal information, it is easy for fraudsters to penetrate the systems and download stored files. Other problems that were revealed were weak passwords and improper firewall configurations, which could lead to possible security compromise (Ragan, 2009).

Hospitality SMEs seem to be in the dark when it comes to boosting security awareness, especially those connected to the Internet. They rely on limited resources and budgets and as a result, fail to protect their networks and customer information. To counter this type of intrusion, the government in Singapore for example, formed a Cyber Security Awareness Alliance in order to help hospitality SMEs address security breaches that were on the rise (IDA, 2008). Research conducted by Bedi and Warden (2009:11) indicates that SMMEs in the hospitality industry are still lagging behind on security applications. The majority of respondents indicated that they have either no or limited security measures in place to address escalating security threats. It is noted that some SMMEs indicated that they do not make use of any procedure to protect customer information leaving themselves vulnerable to attacks (Bedi & Warden, 2009:12).

2.4 HUMAN ASPECTS IN SECURITY

The aim of this section is to introduce some of the challenges experienced as a result of human aspects in information security. This section also explores information security training in hospitality SMEs. In this section, human aspects of both internal and external threats are discussed in sections 2.4.1 to 2.4.3. The reason why this discussion is important is to reveal that individuals, whether insiders or outsiders, can cause damage to the company's information assets

2.4.1 Introduction

Contrary to what is believed insiders are considered to pose a more serious threat than outsiders. Internal threats are more sophisticated than external threats making it difficult to detect them. These aspects are discussed in order to alert the reader on what the literature suggests in terms of addressing these attacks, whether internal or external.

Human aspects in security are threats that are initiated by individuals or a number of individuals who attempt to gain unauthorized entrance into computer systems, public switched telephone networks or other sources. In most cases, these attacks target security weakness in systems and most of the time such vulnerabilities are due to configuration errors (Sarkar, 2010:113). The main sources of human threat can be in the form of internal and external unsolicited information exposure (Goh, 2003:70).

A number of technologies are available to protect information such as firewalls and intrusion detection systems (Colwil, 2010:1). However, these technical devices cannot effectively deal with human security aspects (Rhee *et al*., 2009:816). One of the common ways in which intrusions access confidential information, is through end-user weak information security practices (Frauenstein & Von Solms, 2010:83). Cyber-attacks appear no longer as a result of bored individuals, but are perpetrated by nefarious individuals, including insiders, targeting important company information (Zhou, Leckie & Karunasekara, 2010:124). According to Colwill (2010:1), it is somewhat easier to deal with outside attacks than it is to deal with inside attacks. Tools that are used to address and deal with outside attacks cannot effectively address inside attacks (Colwill, 2010:1).

Zhou et al., (2010:124) assert that employees are important resources but can also be security threats to company information resources. It is indicated that most SMEs suffer from information security breaches, mainly as a result of internal threats than external threats. This insinuates that employees are threats to organisational information resources (Leach, 2003:685, Stanton, Stam, Mastragelo & Jeffrey, 2005:124; Dhilllon, 2001:165; Vroom & Von Solms, 2004:193). Stanton *et al*. (2005:124) opine that research by Ernst and Young reveals that more than three quarters of security breaches occur as a result of internal attacks. Even if organisations have adequate security policies and measures in place but employees are not willing to adjust their behaviour, these policies will be rendered useless (Leach, 2003:686; Tuyikize & Pottas, 2010:165). From this one could assert that information security is primarily a people problem. People are in control of technology and not the other way round. Companies invest time and money in technology but omit the most important aspect: the human aspect. This is an essential aspect that needs to be monitored if companies are to effectively deal with security issues (Dhillon, 2001:166).

2.4.2 External Threats

Walton (2006:8) and others however find that in most cases, people who are motivated to cause serious harm to company information resources are outsiders. Their actions range from stealing confidential information to simply causing havoc. External threats by outsiders are perpetrated mainly by competitive “scouters”, or hackers, “script kiddies”, external consultants or virus creators (Goh, 2003:71). In most cases attacks are carried out targeting particular companies. Outsiders actually have limited options to carry out subversive attacks and in most cases they rely on loopholes or weaknesses in networks to launch their attacks (Walton, 2006:8). It is evident that outsiders would have to do some research about specific or targeted companies to be attacked (Sarkar, 2010;114).

External threats from people such as hackers, bots and viruses can cripple company information resources, but in order to achieve that, they must first gain access to company resources (Shropshire, 2009:297). One of the ways outsiders can harm company information resources is using botnets, which is used to spread malware such as Trojans and spyware. This can be aided by using spam attachments or courtesy phishing emails which directs victims to infected web pages (Elliot, 2010:81).

External perpetrators can also gain access to company networks via hacking (Elliot, 2010:81). According to Trim (2005:494), external threats can be tricky to deal with because the perpetrators can easily relocate to another place at any time. This means that these criminals can operate from anywhere in the world and often disguise their identities. They often steal identities or create false identities. These actions give international criminal perpetrators platforms to launch different types of criminal activities. In summary, this means these types of criminals can utilise different forms of criminal activities as they like (Trim, 2005:494).

2.4.3 Internal Threats

Insider attacks have become emerging problems facing companies. It is noted that a CSI Computer Crime and Security Survey in 2008 reveals that 51 per cent of respondents believed that they would only suffer financial losses as a result of external attacks and not inside attacks (Kreicberga, 2010:1). Insiders have the potential to cause greater harm than outsiders simply because insiders have certain rights and often privileges to access resources, compared to outsiders.

Insiders are also more familiar with company details together with its processes, thus being well informed on how to access secure data. Malicious insiders know when, where and how to attack (Choo, 2010:107; Colwill, 2009:187). Generally, inside attacks have increased over the past few years as a result of a sudden surge in the value of information (Fyffe, 2008:11). A corrupt insider could deliberately sell important information to competitors – a common activity amongst companies these days (Walker, 2008:227). It is reported that confidential personal data stolen from databases could be sold for 4 to 8 USD per record (Fyffe, 2008:11). In other words, confidential data means profit for organised crime syndicates and immoral companies willing to pay huge sums of money for information they can obtain.

Examples of personal data that can be stolen include; credit card numbers, insurance numbers and bank account information (Fyffe, 2008:11). Serious cases of intentional information security breaches by insiders are common. However, it is not always advisable for companies to report security breaches (Shropshire, 2009:296). Security breaches as a result of insiders' actions are classified as a rational act because of personal factors, work situations and opportunities available (Theoharidou, *et al*., 2005:473).

Other categories of security breaches include IT espionage and IT sabotage carried out by insiders (Shropshire, 2009:297). This can take place when disgruntled employees plan to take revenge or when employees with malicious intentions are looking for financial gain (Sarkar, 2010:2; Walker, 2008:228). It can also be done as a way of retribution or reprisal for firing or dismissing employees, to impress a spouse or friend, or as a result of being under the influence of drugs or alcohol (Shropshire, 2009:297).

According to Kreicberga (2010:9) internal threats can be categorised in to three groups, based on the motive:

- Stealing or modifying information in order to benefit financially;
- Stealing information for business advantage;
- Information Technology sabotage.

Walker (2008:227) on the other hand, categorises security breaches into two groups; namely

- Malicious (e.g. intentional in nature)
- Non–malicious (accidental).

Malicious inside attack activities are carried out by individuals, groups, organisations and nations with the goal, motivation and capabilities to exploit companies with the aim of furthering their subversive objectives (Walker, 2008:227). According to Mubarak and Slay (2009:203), insider threats are more dangerous if influenced by outsiders, especially with the aid of technology which can open avenues for insiders to expose company information resources. Sankar (2010:113) discloses some of the possible inside attacks depicted in Figure 2.3. It is depicted in Figure 2.3 that network data breaches can take place in a number of ways. For example, there are a variety of practices in which personal information, patient information, or customer account can be disclosed (Bryce & Klang, 2009:160). Figure 2.3 shows that misuse of devices can also lead to breaches or loss of information. Devices such as flash drives, ipods and PDAs can carry viruses that can attack a company's information systems resources (Sankar, 2010:113).

It is also revealed in Figure 2.3 that lack of training can lead to social engineering. Since end-users will be poorly trained, they will activate the malware unknowingly and it will run in the system and will lead to data loss. The best remedy for dealing with social engineering is making use of email filtering devices and end-user training (Abraham & Chengalur-Smith, 2010:184).

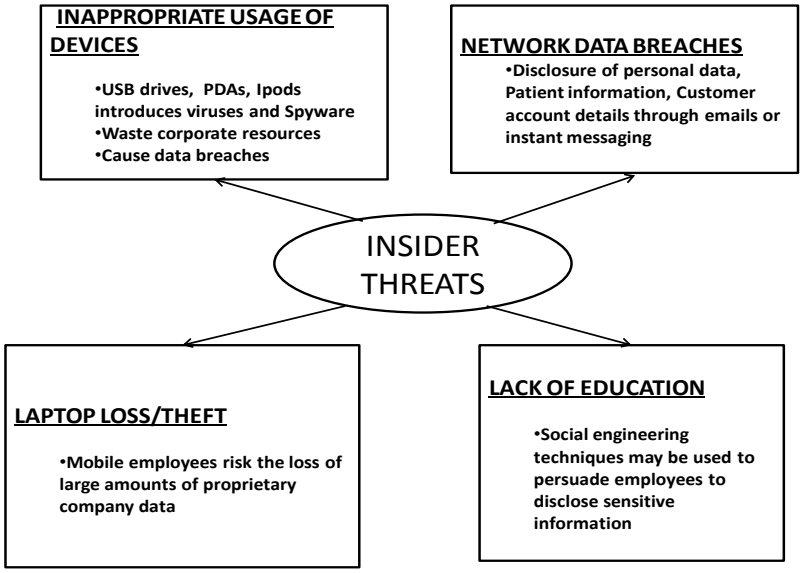

Figure 2.3: **Possible insider attacks (Adapted from Sankar, 2010:113)**

2.4.4 Summary – Human aspects in security

The aim of this section is to understand how internal and external threats can affect company's security breaches. Training as one way of addressing inside attacks, was also discussed. Literature reveals that companies find it common for inside attacks to overshadow outside attacks. Inside attacks are more difficult to detect and as a result, are more costly to solve.

2.5 INFORMATION SECURITY BREACHES

In this section information security breaches and their impact on SMEs are discussed in sections 2.5.1 and 2.5.2. Risk assessment in SMEs and data protection methods is also covered to understand measures that are put in place to assess network and system vulnerabilities. Risk assessment can help SMEs discover loopholes in the network before a breach takes place. The term information security breach refers to unauthorised access to data, or loss of data, which is stored in the computer or is transferred via communication channels. This data may include personal data or company data. In most cases these incidents take place because of the vulnerability of a company's network or loopholes in the company's information systems (Acquisti et al., 2006).

To further understand some issues related to information security breaches, types of breaches are also discussed. These aspects are essential because each and every company's success in information security depends on how it deals with security breaches. Security breaches are on the rise and companies need to put measures in place to address them. These measures can be in the form of data protection methods, hence the last section where these methods are discussed.

2.5.1 Introduction

Cavusoglu *et al*., (2004:72) avow that security breaches can be categorised into two groups; tangible and intangible costs. Tangible costs include costs that can easily be estimated or calculated such as lost sales, material costs and insurance expenses. Intangible costs include costs that cannot be calculated such as costs related to trust. These costs are still important because they are used to measure the overall cost of security breaches in companies (Cavusoglu *et al*., 2004:72). Security breaches do not only result in loss of customers or a competitive advantage, but can also lead to legal disputes (Liginlal, Sim, & Khansa, 2009:215). This could even lead to government sanctions (Campbell, Gordon, Loeb & Zhou,2003:432).

Information security breaches have been around for a while (Andoh-Baidoo & Osei-Bryson, 2007:703). There are many ways in which information breaches can occur (Cavusoglu, Mishra & Raghunathan, 2004:70). For example, it can be a result of lost or stolen computer hardware, media containing sensitive information, hacking, viruses, illegal sale of customer data and other means that involve technology (Federal Reserve Bank of Philadelphia, 2006:10; Acquisti, Friedman & Telang, 2006; Campbell 2003:432). A recent security breach in South Africa resulted in millions of Rand being stolen from Post Bank by a syndicate who were familiar with the office information technology system (SAPA, 2012).

Despite the fact that there is a rise in information security breaches, few studies have been carried out to investigate the real impact of online security breaches (Campbell*et al*., 2003:432; Garg *et al*., 2003:74). In most cases the studies have been based on self-reported cases (Garg *et al*., 2003:74). According to Campbell *et al.* (2003:432), one of the reasons why there has been limited research on information security breaches is due to either the unwillingness of companies to disclose this, or an inability to quantify losses that they have incurred. The authors opine that it is difficult to rely on this method for the full economic impact of information security breaches (especially in reference to indirect costs related to the effects on the value of security investments and other equipment) (Campbell *et al*., 2003:432).

Information security breaches do not only impact the increase of direct costs (repair costs, losses as a result of fraud or breach), but they also lead to an increase in indirect costs (costs incurred in the prevention of a breach). There are also other hidden costs (increases in lower productivity as a result of reduced trust in e-commerce) (Bauer & Van Eeten, 2009:706). Most security breaches result from human error, this is revealed by Linginlal *et al.,* (2009:215). These authors disclose that human error breaches account for 65 percent of all breaches. According to the Federal Bank of Philadelphia (2006:10), information security breaches can affect consumers in two ways; firstly, consumers will be confused and uncertain, which may cause them to lose confidence in the system that is used. If the breach is announced to them, they often fail to understand the situation and how much it can affect them. Sometimes this process might take a while and might result in anxiety. Secondly, consumers could be subjected to identity theft, which could lead to serious problems such as financial losses.

Linginlal *et al*., (2009:215) aver that security breaches can result in loss of consumer trust and confidence and ultimately, loss of business. Cavusoglu *et al*., (2004:72) assert that the cost of security can be divided into short-term cost (their impact is felt during the security breach), and permanent cost (long-term costs occur on a number of occasions). Examples of short-term costs include loss of business and decreased productivity as a result of unavailability of breached resources. Conversely, permanent costs have a long-term impact. These include loss of clients who might switch to competitors, inability to increase the number of customers as a result of perceived poor security, or even legal battles as a result of the breaches (Cavusoglu *et al*., 2004:72).

2.5.2 Security breaches in hospitality SMEs

Direct costs of security breaches in SMEs may not be as high as in large companies, but this still raises concern (DTI, 1997). SMEs may suffer losses which are heavier than losses incurred by larger companies (Moscaritolo, 2009). This is probably due to SMEs tending to lack necessary resources to effectively deal with security breaches (Lee & Jang, 2009:84). In most cases, SMEs make use of people who do not have sufficient experience when it comes to securing computers and networks. While large companies are sometimes facing difficult tasks of dealing with dispersed networks, SMEs have to deal with challenges of lack of dedicated IT personnel (Moscaritolo, 2009). According to research reported by PriceWaterhouseCoopers (2010), security breaches have been increasing since 2002.

Companies are losing money as a result of security breaches. This is not uncommon as it is reported that in the United Kingdom for example, 74 per cent of SMEs reported that they had been victims of security breaches during 2008. In Kenya 76.2 per cent of SMEs revealed that they were victims of security breaches (Kimwele, Mwangi & Kimani, 2012:9). The most common security breaches were infection by virus or malicious software, theft or fraud committed by insiders as well as attacks from outsiders who hacked into the company's network systems (Price Waterhouse Coopers, 2010).

The case of SMEs in the hospitality industry is not much different and they are therefore not immune to security breaches as noted by Bedi and Warden (2009:10). It was found that 83 percent of respondents indicated that they once experienced virus infection. In contrast, 32 percent indicated that they had lost data that was not backed up (Bedi & Warden, 2009:9).

2.6 TRENDS IN INFORMATION SECURITY

In this section the researcher explores some information security trends. According to the literature reviewed, the main aspects are; trends of information security introduction (section 2.6.1), focal areas in information security (section 2.6.2), secure network protocols (section 2.6.3) and risk analysis (section 2.6.4).

The aim is also to answer research sub-question 1, which is stated below.

What are the trends of information security both locally and internationally?

2.6.1 Introduction

Information security initially in the late 1960's consisted of basic access control features (Bella and Bistarelli, 2005: 322). Computers that were used at the time could only allow one person to work per machine (Thomson & Von Solms, 1998:167). It was easy to protect information by just restricting physical access to a computer room (Landwehr, 2001:3). Companies in the past did not have to worry about monitoring and controlling employee's actions because it was difficult for employees to use the information as they needed expensive devices to retrieve information. These conditions made it easy to deal with data security (Bella and Bistarelli, 2005: 322).

Technology advancement has led to a communication age where people can access their office systems via telecommunications lines but the data still remains within the boundaries of organisations. Although employees could access data remotely, it was difficult and cumbersome to download data (Bella & Bistarelli, 2005; 322). Maconachy *et al*. (2001:306) find that information security has evolved to form information assurance. The authors further add that information security is a term commonly used to differentiate between disciplines such as computer security, personnel security, operational security and communication security (Maconachy *et al*., 2001:306). As the 21st century approached, a change was detected. Hackers started attacking company systems in order to embezzle funds and not just to demonstrate their hacking skills. Company network systems became complicated and difficult to manage. The "e" word became a common adjective, for example; e-commerce, e-business, e-government and e-voting, denoting an increasingly electronic world. At that time a number of devices were introduced to the market such as personal digital assistants (PDAs), smart telephones, laptop and desktop computers making it difficult to deal with security issues. With the introduction of mobile computing devices, it became even more difficult to effectively deal with security breaches.

Online payment systems, web based applications as well as credit card usage became common activities (Dlamini *et al.,* 2009:191). Most companies depend on ICT for their daily business resulting in new emerging challenges (James, Khansa, Cook, Bruyaka, &Keeling, 2013: 49; Sarkar, 2010:112). For example, hackers have moved from a nuisance factor or being computer maniacs, to professional hackers. These hackers have become so knowledgeable that they can use their hacking skills to bypass authentication processes to access files that contain sensitive information. As a result, various threats have emerged such as, identity theft, social engineering, phishing and others (Dlamini *et al*., 2009:191). The high cost of maintaining and upgrading devices such as anti-virus software and firewalls makes it difficult for SMMEs to adopt effective security measures (EMW, 2005). In the next three sub-sections, an overview of some of the trends in information security is presented.

2.6.2 Focal areas in information security

For a universal overview of points of focus in information security, it is normal to concentrate on the CIA triad, which stands for confidentiality, integrity, and availability (James *et al*., 2013;49; Maconachy, Schou, Ragsdale & Welch, 2001:306; Walter & McKnight, 2002; Chiang and Huang, 2003:1; Kalla, Wong, Mikler and Elbert, 1999:167; Hutchinson and Warren 2003:68; Rosado and Gutierrez, 2006:521).

- **Confidentiality** - refers to preventing information from being disclosed to unauthorised individuals. Unauthorised disclosure of information may occur in several ways, such as, intentionally or unintentionally (Chiang & Huang, 2003:1).
- **Integrity** - is a concept that means that alteration or substitution of data and/or modifications of data are detected and provable (Clemer, 2010; Pasante, 2008:3; Flowerday & Von Solms, 2005:606).
- **Availability** - refers to information, the computing system which is used to process information, and security controls that are used to protect information; these are all available and function correctly when the information is required. In this way computing resources can be accessed by authorised personnel anytime (James *et al*., 2013:49; Posthumus & Von Solms, 2004:645). An additional two security requirements are often added to this list, being authentication and non-repudiation (Clemer, 2010; James *et al.,* 2013:49; Maconachy *et al.*, 2001:306). Authentication refers to the assurance that data was created or sent by the person it appears from (James *et al*., 2013:49). On the other hand, non-repudiation means that the person who is sending the information is who he or she claims to be (Pasante, 2008:3).

2.6.3 Secure network protocols

The Secure Sockets Layer (SSL) protocol which is an agreed upon format for transmitting information between two devices, was designed to ensure privacy and integrity over the Internet. SSL ensures security by using a personal key to encrypt data that is transmitted over the SSL connection, so that anyone who intercepts the data is unable to read it (Sarkar, 2010:135).The SSL protocol is made up of two phases. The first phase, server authentication, makes sure that authorised personnel can be sure that they have connected to the server they wanted to connect to. On the other hand, the second phase (client authentication) is optional (Seddingh, Pieda, Matrawy, Nandy, Lambadaris, Hatfield, 2012:3). The SSL protocol consequently ensures integrity and security of the transmission channel by making use of data encryption, server authentication, message integrity and optional client authentication (Smith & Eloff, 1999:45).

2.6.4 Risk Analysis in SMEs

It is accepted that information security devices cannot effectively deal with all security issues and therefore, companies must try to minimize the impact of risks rather than eliminate them. A risk assessment helps companies in the following ways:

- Checking and balancing the configurations and administrations of security networks that might not work as expected and might need to be monitored.
- Regular reviewing – in order for security to be effective, the configurations must be measured and adjusted according to the escalating threats.
- Allocation of resources based on the risk to be assessed – up until the company is aware of the risks it is facing, resources will be allocated to areas where they might not be needed (Sveen *et al*., 2009:104).

In the hospitality industry, a minor loss of information may result in serious loss (Sarkar, 2010:136). According to Comptia (2012) information security, like any other business problem, must include a measure of analysis to determine the risk and consequences. A typical threat to the hospitality industry is unauthorised access to credit card information (Smith & Eloff, 1999:45).

Risk management is one of the challenges that SMEs face because threats are evolving and security vulnerabilities keep on increasing (Beranek, 2010:43; Onwubiko & Lenaghan, 2007:6). The difficulties in conducting detailed analyses are diverse. According to Beachboard, Cole, Mellor, Hernandez & Aytes (2008:74) it is difficult to identify all the necessary threats and to estimate the probability of occurrences. For a risk assessment process to be successfully implemented, it requires an understanding of the concepts of security and their relationships.

This understanding could assist SMEs to gain knowledge to apply the right combination of protection controls as they try to categorize and mitigate both threats and weaknesses. It is therefore, imperative that SMEs protect their information by reducing the number of threats that might affect them. In order to effectively deal with these threats, SMEs should have some measures in place to curb them (Onwubiko & Lenaghan, 2007:6).

According to Onwubiko and Lenaghan (2007:6), a real challenge SMEs face in managing risks is the lack of finance. As mentioned before, SMEs rely on limited budgets to cater for their security needs, compared to larger companies. These authors indicate that it is pointless for SMEs to apply protection tools such as firewalls or intrusion detection systems if they do not consider the following:

- Identifying resources that need to be protected.
- Classifying the resources accordingly.
- Assessing the weaknesses in/within the identified assets.
- Identifying the weaknesses that might exploit the gaps in the network.
- Assess the associated risks to the resources as a result of threats and vulnerabilities.
- Establishing an effective combination of countermeasures (Onwubiko & Lenaghan, 2007:6).

According to Dimopoulos *et al*. (2005:74), risk assessment is not common amongst SMEs for several reasons. For example, some of their respondents indicate that risk assessment can disrupt management and employees (Dimopoulos *et al*., 2005:71). Simmons and Burgess (2000:5) advise SMEs to consider the following two stages when conducting risk assessment; the preparation and data collection stage, and analysis and results phase.

These are now briefly explained:

- The preparation and data collection stage is where data is identified and collected to be used at a later stage in a checklist;
- The analysis stage is where a checklist is used to identify risks, threats and vulnerabilities. Before the company embarks on a vulnerability assessment, it must be decided which assets need to be protected. The probability that certain assets are likely to be attacked should be determined. The goal of risk assessment is to determine and calculate the intensity of risks which face the company's information systems in order to select the right security safeguards (Spinellis *et al*., 1999:121).

According to Dimopoulos *et al*. (2005:78), 73 percent of SMEs in risk assessment research indicate that they conduct risk assessment in-house. Only 2 respondents out of 30 indicate that they make use of risk assessment tools and none of them used security guidelines such as ISO 17799 (Dimopoulis et al., 2005:78). Incidentally, this has been renamed ISO 27001 (Sveen *et al.,* 2009:99). Accepting these findings and considering the fact that most SMEs do not make use of specialists, raises questions regarding the effectiveness of their risk assessment program. According to Dimopoulos *et al*. (2005:78) SMEs perceive risk assessment complicated as they would have to hire a specialist to help them (Beranek, 2010:44). Dimopoulos *et al*. (2005:71) disclose that by failing to adopt such a procedure, SMEs render themselves vulnerable to exploitation by those with malicious intent. Simmons and Burgess (2000:6) indicate that vulnerability assessment is a route for SMEs to select the right method of data protection.

2.6.4.1 Summary – Risk analysis

Information security has existed for more than five decades. In the early stages of information security, restricting physical access to a computer room was enough to protect information. With technology advancement, it has become difficult for companies to effectively address information security. Hackers have become a problem and threat to companies as they no longer hack into the networks to demonstrate their capabilities but rather for monetary gain. Some of the trends of information security include a stress on focal areas in information security, secure network protocols and risk assessment. Focal areas of information security concentrate on the CIA triad. CIA represents confidentiality, integrity and availability. Authentication and non-repudiation have been added to this list.

These five factors have been singled out as the building blocks of information security. On the other hand, secure network protocols are some of the rules that were formulated to make sure that data can be transferred smoothly without any interference. Risk assessment ensures that analysis helps companies limit the number of breaches. It is an important procedure because it can help companies identify the risks they are facing and therefore mitigate them. SMEs seem to struggle to apply risk assessment as they do not have finances to hire specialists to address this. As a result, they are vulnerable to attacks because they do not know what to protect or the probability of a risk taking place.

2.7 MEASURES TO ENSURE CUSTOMER SECURITY

The aim of this section is to provide a background to research sub-question 2 which is stated below. Information management in SMEs is discussed in section 2.7.2.

What measures are in place for businesses to ensure customer security when conducting online business?

This section is needed in order to reveal to the reader how information security management can reduce information security threats. Information security management (ISM) in hospitality SMEs is also discussed to find out how hospitality SMEs are making use of it. As Saleh and Alfantookh (2011:107) disclose, one essential element of information security is information security management which aims at providing a safe and secure environment for e-business and e-commerce. SMEs that effectively manage information security will ensure that they select adequate and appropriate security controls that protect information assets and will gain confidence from third parties (Ashenden, 2008:195).

2.7.1 Introduction

Information security has matured over the years from a technical view to a more business focussed concern. ISM can be defined as the part of a management system that analyses business threats and formulates an approach to create, execute, operate, monitor, review, and maintain defences to improve information security. It is also one way of reducing risks to information within company environments by applying security technologies through the management process (Chang & Lin, 2007:440). A trusted security technology alone is not enough to protect company information without a good policy management and execution initiative (Chang & Ho, 2006:347).Given the important role played by IT, information security is an important aspect that modern enterprise planning and management has to consider (Chang & Lin, 2007:438). This is as a result of the rising growth of electronic transactions. Once companies are connected to the Internet, maintaining security becomes challenging. ISM is therefore used to protect information from a number of threats so that the company can continue with its daily business (Chang & Ho, 2006:346).

Organisations collaborate with their business partners and customers. Whenever there is information exchange via the Internet, there will be a measure of security risk (Von Solms, 1996:282, Yildrim *et al*., 2011:392). Previous studies indicate that ignorance plays a role in some security breaches. The main objective of ISM is to make sure that confidence and information effectiveness within the company, or

between the company and its stakeholders, is enhanced (Von Solms, 1996: 282). Security as a whole is a worrying problem for stakeholders and in order for companies to be successful in their quest to combat these threats, collaboration is needed to make sure that threats are mitigated (Tawileh, Hilton & McIntosh, 2007:2).

If information security is not properly managed, it is likely to result in confusion when it comes to the application thereof. A likely problem is that risks might not be addressed adequately or some controls may not be appropriate. It will thus be difficult to understand what has been done, by whom, for what reason and for what purpose without management's intervention or guidance. Management also needs to ensure that adequate and proper security measures or controls are selected. This would ensure that company information resources are protected (Ashenden, 2008:197).

2.7.2 Information security management (ISM) in hospitality SMEs

It is important for each organisation to define its security requirements (Yildrim *et al*., 2011:310). There appears to be a significant difference in the way SMEs manage their information (Tawileh *et al.,* 2007:2; Gupta & Hammond, 2005:299). This difference can be attributed to some operational limitations faced by SMEs which affect them as they try to apply security measures. For example, Sang and Jang (2009:84) opine that SMEs are aware of the importance of security but they lack the resources and technical knowhow to design proper Information Security Management Systems (ISMS). Security surveys reveal that there is poor security management amongst some Australian companies, especially SMEs (Sang &Jang, 2009:84). It is also found that SMEs do not have proper procedures and mechanisms in place to monitor their security in an online environment (Gupta & Hammond, 2005:300). Although ISM can help reduce security issues (Chang & Lin, 2007), SMEs in the hospitality industry reveal that they lack security awareness (Bedi & Warden, 2010:147). The study reveals that 34 per cent of the respondents indicate that they are not sure whether ISM can minimise information theft. Only 66 percent of the respondents indicate that they agree that ISM can minimise information theft (Bedi & Warden, 2010:147).

2.7.3 Information security policies

The aim of this section is to further answer sub-question 2. In this section, information security policies, their importance and implementation are discussed in sections 2.7.3 to 2.7.2. The reason that these aspects are included is to present to the reader how information security policies can help address security breaches. Through information security policies, the users' security awareness will be enhanced.

Information security policies are discussed since their successful application can contribute to a decline in data breaches. Information security policies implementation is also discussed in this section in order to reveal effective ways of implementing information security policies. Password policies are very crucial when it comes to authenticating legitimate users into the system, and are also discussed in this section. Considering that SMEs' main form of security are passwords and usernames, it is therefore appropriate to discuss password security in SMEs.

There is a trend for organisations to make more use of ICT if they are to survive competition regardless of their size. On the other hand, it is important that companies implement security controls that will ensure that information is properly secured. This is needed in order to maintain information confidentiality, integrity and availability (Tuyikeze & Pottas, 2010:165). The first thing that organisations should do to be safe-guarded against information security breaches, is to ensure that well documented and relevant policies are in place (Hone & Eloff, 2002:402; Wen & Tarn, 1998:179). A policy can be "classified as a communication tool from management as they attempt to convey a specific message to various parties" (Von Solms & Von Solms, 2004:276). The main goal of an information security policy is to guide users in terms of their responsibilities within the company, particularly with reference to information (Hong, Chi, Chao & Tang, 2006:105; Tuyikeze & Pottas, 2010:165). Doherty and Fulford (2005:57) further add that an information security policy includes "goals, objectives, beliefs, ethics and responsibilities". These authors point out that since availability, integrity and confidentiality of information need to be protected, security policies will be important in terms of defining network access, local and remote user authentication, service access, disk and data encryption, measures for virus protection and employee training (Wen & Tarn, 1998:179). An acceptable information security policy becomes the cornerstone of an organisation's information security regime (Baskerville & Siponen, 2002:337; Tuyikeze & Pottas, 2010:165).

Traditionally, the most common security policy is a privacy policy. Privacy policies indicate how personal information is handled (Peterson *et al*., 2007:658). Baskeville and Siponen (2002:337) indicate that not much has been done to create effective security policies. According to Olnes (1994:628), it is important to note that different companies have different policies, and much depends on the type of businesses that they are involved in. This is as a result of some companies requiring higher security measures compared to others who do not require as much. Companies that need high security measures require well detailed policies which do affect employees (Olnes, 1994:628).

An information security policy could be used to guide staff members on how to protect company information. If a policy is well written, it will provide an acceptable definition of what needs to be done and how it needs to be done (Tuyikeze & Pottas, 2010:166). Policies are important because they are a channel through which organisational goals are communicated effectively (Yildrim *et al*., 2011:360). They further guide employees and provide direction on how the organisation should be managed (Ward & Smith, 2002:361). According to Hone and Eloff (2002:15), effective information security policies are able to influence staff members to adjust their behaviour in order to make sure that the company information is kept secure. The authors further state that policies should consider both the users' and business needs in order to be effective. Users will be assured that information security is not a threat, but rather a procedure that is taken to make sure that the company's information is not compromised (Hone & Eloff, 2002:15). Hong et al. (2006:105) indicate that if a policy is understandable to end-users, they will always refer to it when they do not know what to do and, therefore, not waste time consulting continuously (Hong *et al*., 2006:105; Luzwick, 2001:16). It is indicated that a well documented security policy is one of the common ways of increasing information security awareness, and Chipperfield & Furnel (2010:14), for instance, find 88 percent of respondents agree with this. Information security policies can help define users' rights (Hong et al., 2006:105). If the policy is relevant or correct, it will address issues of concern and help in improving the overall security within the company and can also prove useful dealing with legal issues (Tuyikeze & Pottas, 2010:166).

Many European SMEs do not have security policies in place (Ferguson, 2007). According to Ferguson's research, most managers blame their employees for online security breaches even though they do not emphasise the importance of online security policies. The author finds that 23 percent of SMEs have security policies in place, but still they do not enforce them amongst employees. Additionally, research by Kyobe (2005:6) indicates that a majority (74 percent) of SMMEs in South Africa do not have security policies. Most respondents did not have guidelines that cover issues such as access rights, password formulations and, in some instances, roles and responsibilities were not properly defined. It is common that users have access to the Internet, but they do not have any policies to refer to in case a breach occurs. Kyobe (2000:143) also reveals that many SMMEs do not have measures in place to ensure secure transactions and minimize security compromises. A figure that indicates the possession of security policies in SMMEs is presented in Figure 2.4.

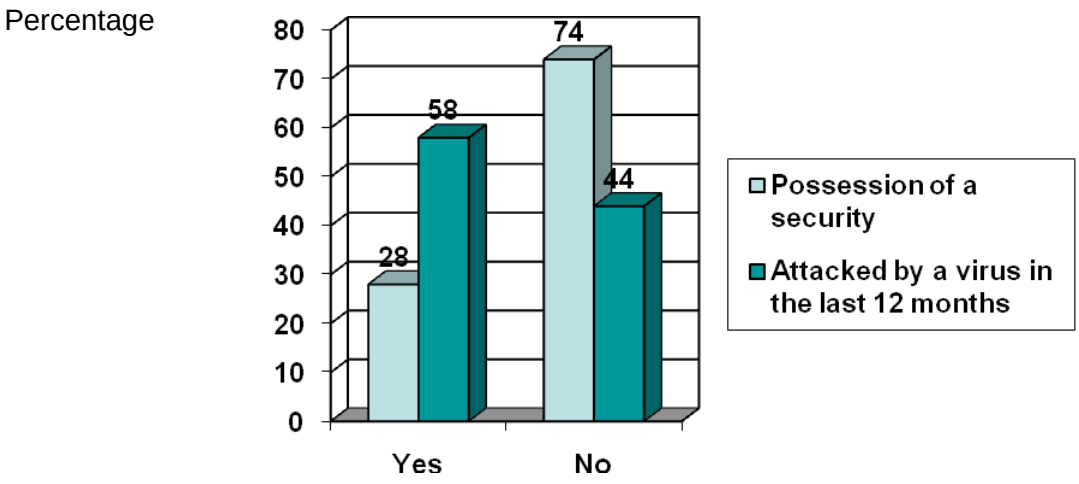

Figure 2.4Figure 2.4: Possession of a security policy vs. virus attacks (Adapted from: Kyobe, 2005:6)

From figure 2.4, it can be seen that 58 percent of respondents were attacked by viruses over a period of twelve months prior to the research. Of these, 74 percent did not have a security policy in place. Kyobe (2005:7) explains that a Chi square test was conducted to ascertain if lack of security policy and formation of virus attacks are linked to each other. The results reveal that a lack of policy and virus attacks are linked and depicted in Figure 2.4.

2.7.3.1 Information security policies in SMEs

According to Gupta and Hammond (2005), most SMEs lack policies and measures to deal with data breaches, and as a result these companies are vulnerable to attacks. In most cases they do not possess any documentation to guide users in terms of security (Park *et al*., 2008:92).

Upfold and Sewry (2005) agree with these authors indicating that it is surprising that a lack of policies is common amongst SMMEs even though it has been proved that security threats are on the rise. Research by Upfold and Sewry (2005) indicates that 82 percent of South African SMMEs do not make use of policies to minimize breaches. According to research conducted by Dojkovski, Lichstein and Warren (2007: 1566), most SMMEs believed that formal policies were not necessary. This is supported by research by Burns, Davies and Davies (2006) in Wales, indicating that most of SMEs indicated that they do not need such policies.

M2 Communications (2005) notes that in the UK, an ExoServer e-policy was launched to protect SMEs' online information which makes it easy to manage Internet and email activities, as well as to ensure that these companies abide by legal protocols that can prove to be costly if they are not followed. This policy is made to fit specific needs of SMEs, instead of instituting a total shut down of the Internet for their employees. Its flexibility to access allows employees to make use of the Internet with only minor restrictions, hence allowing employees and businesses to be productive. It makes sure that the Internet works securely and efficiently. As part of its daily duties, ExoServer manages the web browser and acts as an instant messenger and, as a result, produces reports on ongoing usage (M2 Communications, 2005).

2.7.3.2 Password policies for SMEs

Passwords are one of the common ways of ensuring that information assurance is kept intact (Vineyard, 2009:34; Siska, 2007). Some of the external threats such as trojans, other viruses, hackers and worms are exacerbated by poor behaviour such as poor choice of passwords or sharing of passwords (Doherty, Anastasakis & Fulford, and 2010:2). Passwords have long been used, but the way they are used is likely to change. Short and easy to crack passwords that do not expire are being replaced with passwords that include different characters with frequent expiration (Siska, 2007). Calder (2005:69) encourages SMEs to deploy password policies that will alert staff how often they should change their passwords. As more complex passwords are being used, users tend to re-use the same password, write them down or make them accessible to other people (Siska, 2007). A password policy is important because it guides staff members how to go about selecting passwords, sets out requirements for confidentiality and reminds them that temporary passwords are to be changed at the first logon (Duggan, Johnson & Grawemeyer, 2012:417). Olivier (2009) indicates that while SMEs in the UK understand the importance of information security, they still fail to realise that staff members can pose a threat to company information resources. Their research indicates that SMEs' security in the UK is so relaxed that over 60 percent of the respondents do not have any security policy in place, including password policies. While these SMEs admitted that they use passwords to authenticate users into the system, they fail to provide staff members with password policies to guide employees how to create passwords and when to change them (Olivier, 2009).

Ferguson (2007) indicates that IT managers in SMEs tend to blame their fellow employees for the security breaches even though most of the time their companies do not have password policies. Ferguson (2007) finds it worrying that close to three quarters of European SMEs' IT managers claim that employees are to blame for security problems, but still they fail to implement password policies. Cape Town hospitality SMMEs seem to be lagging behind when it comes to password policies, as revealed by Bedi and Warden (2009:11). Their research indicates that 53 percent of the respondents indicated that they do not have password policies (Bedi & Warden, 2009:11).

2.7.3.3 Summary – Security policies

Technology alone cannot effectively deal with security breaches. It is therefore important for SMEs to put measures in place that will address both inside and outside attack. ISM and information security policies can help in this regard. ISM management can help mitigate security breaches by making sure that security technologies are well managed. ISM can help SMEs select adequate and appropriate security controls that will help them protect information and avoid unnecessary breaches. Hospitality SMEs seem to be lagging behind when it comes to ISM. They seem to lack the technical knowhow and finance to effectively apply ISM. Policies on the other hand, can help SMEs deal with inside attacks. Policies can help communicate the company's goal. The main goal of an information security policy is to guide users in terms of their responsibilities within the company, particularly with reference to information. Information security policies help define users' roles. Despite all the benefits of the policies, they are not common amongst hospitality SMEs. Partly as a result of this, SMEs are vulnerable to attacks.

2.8 INFORMATION SECURITY TRAINING

In this section, an introduction to information security training and its importance to SMEs are discussed in section 2.8.1 and 2.8.2. This discussion is to provide background and gain understanding of the issues posed in research sub question 3. The empirical data in Chapter 4 will be used to answer this research question fully.

As revealed in the previous section, insiders are believed to be behind most attacks because they have the privilege of accessing company information resources. Through information security training end-users will be equipped to avoid some mistakes that contribute to some of the security breaches. This section also discusses some training procedures that are provided by SMEs and the frequencies of training programs in order to understand how seriously these companies value information

security. The aim of this section is to gain an understanding of research sub question 3 which is stated below.

To what extent is security training provided in hospitality SMMEs?

2.8.1 Introduction

Allam & Flowerday (2010:11) find employees do not take much care when handling information. Therefore, providing employee training makes them aware of security issues (Futcher, Schronder & Von Solms, 2010:216). One view expressed is if companies want to become successful, they need to become learning organisations (Trim, 2005:500). Awareness and culture are some of the contributing factors of information security performance in companies. To effectively deal with security incidents that involve human activities such as phishing or scams, ICT security awareness programs should be provided to employees (Kruger & Kearney, 2008:254). It is therefore imperative for companies to provide adequate training to improve user awareness and behaviour (Albrechtsen, 2010:432). Providing training to end-users highlighting their roles and responsibilities could curb security breaches (Ruighaver *et al*., 2007:60). In order for security standards to improve in an organization, security awareness training should be provided (Rezgui & Marks, 2008:244). Proper training can minimise unintentional disclosures of information to strangers and also lead to a security abiding culture (Ruighaver *et al*., 2007: 60). According to Chipperfield and Furnel (2010:14), it is revealed that the most effective method of increasing security awareness amongst employees is by training. Information security awareness plays an important role in curbing security breaches. New employees who might not be aware of company policies need some training to familiarise them with these policies. A frequent reminder should be provided to existing employees to reinforce security awareness (Allam & Flowerday, 2010:111). According to Rezgui and Marks (2008:244), training and education play an important role in defending information security. Information security training and awareness enforces the feeling of ownership and responsibility amongst employees (Ruighaver *et a*l., 2007:60).

2.8.2 Information security training in SMEs

Although training is indicated to be the most effective way of increasing security awareness, it is the least commonly used method in SMEs (Chipperfield & Furnel, 2010:14. Kelleher (2009) indicates that both large businesses and SMEs face the same threats, but SMEs tend to ignore this by failing to provide training for their employees. According to Lange, Ottens and Taylor (2000:5), a number of SMEs do

not provide regular training. They further reveal that SMEs are willing to participate in on-the-job training or informal training where there are no hidden costs. These authors assert that culture prevalence has a role in making SMEs not provide training. Stokes (2001:318) indicates that cultural barriers towards formal training are common amongst SMEs mainly due to some managers perceiving this as a waste of time.

SMEs singled out a lack of finance, awareness, access and provision as some of the obstacles which hinder them from providing security training (Tawileh *et al*.,2007:2). Stokes (2001:318) finds that there is an increase in temporary staff positions contributing to a lack of training within some SMEs as owners are less likely to invest in training temporary staff. Tawileh *et al*., (2007:2) further add that research indicates that some SMEs tend to encourage staff members, particularly new employees, to learn from others. Some SMEs believe in skill sharing, especially when it comes to information training related issues such as information security (Stokes, 2001:318). In South Africa, Bedi and Warden (2010:148) reveal that training of new employees is not common amongst hospitality SMMEs. This is based on a total of 15 percent of respondents indicating that they do not provide training to their employees, with 27 percent indicating that they are not sure if training is provided to employees. Only 58 percent of the respondents indicated that they provide security training to their employees (Bedi & Warden, 2010). Furthermore, regarding new employee training, participating SMEs in research by Kuusisto and Ilvonen (2003:236), indicate that one of the reasons for not having training programs is that they believe it is not necessary. SMEs only provide training to new employees. Only two SMEs out of fifteen indicated that security training was provided, although this training was not conducted regularly (Kuusisto & Ilvonen, 2003:437).

2.8.3 Summary – Information security training

Training can help address mistakes committed by staff members. Despite this, training is not common amongst hospitality SMES. They cite training costs as one of the main reasons for not providing training. This can cost these companies because a security abiding culture is enhanced by training staff members. One difficulty with addressing external attacks is that an attack can be launched from any part of the world.

2.9 ONLINE CUSTOMER PROTECTION

Security breaches are becoming more common and are threatening various business activities. The hospitality industry has adopted ICT and security for IS has become even more important, since the hospitality industry has to manage customer data in a broad customer database. The background to research sub question 4(stated below) is discussed.

What are hospitality SMMEs doing to protect customers in an online environment?

As a result of the rising number of clients who can access tourism establishments via the Internet and staff members who are allowed to access hotel information systems using external intranets, the importance of customer information security has become even more important (Kim, Lee & Ham, 2012:1). The hospitality industry has become more appealing to hackers because of the publicized poor network security by hospitality industry businesses. Some of the consequences of information security breach for hospitality industry customers include financial loss, loss of reputation and/or customer behaviour alterations (Berezina *et al*., 2010:992).

According to Goucher (2011:18) information security seems not to be a priority amongst SMEs, especially in those in the hospitality industry (Goucher, 2011:18). SMEs are more vulnerable to security breaches because they tend to lack the financial muscle and the necessary skills to effectively deal with them (Gupta & Hammond, 2005:298). Their IT technologies are either managed by one person or a few individuals, usually with limited knowledge (Park, Robles, Hong, Yeo & Kim, 2008:92). Adopting and implementing an effective new information security strategy is an uphill battle for hospitality SMEs. These companies might be tempted to cut corners (Gupta & Hammond, 2005:298). A recent study reveals that there was a 15 percent increase in security breaches amongst SMEs over the past year (Hubbard, 2013). In most cases these companies do not consider themselves to be the targets of hackers or intruders. As a result of this, they view security as a low priority, in the process exposing customers' confidential information (Park *et al*., 2008:92).

A majority of SMEs claim that protecting the customers' sensitive information, particularly credit card information, is a priority. However, if one investigates the subject in depth, there are indications that SMEs might not being doing enough to protect customers' information (Goucher, 2011:18). Hospitality SMEs tend to engage fewer deterrent measures compared to large hotels (Gupta & Hammond, 2005:298).

A great deal of time is needed to effectively address security concerns in the online environment and most SMEs are not prepared to do that (Barlette & Formin 2008:3).

2.9.1 Summary – Online customer protection

The hospitality industry deals with a great deal of customer information. Companies in this industry are expected to keep customer information secure. It seems hospitality SMEs are ill prepared to address security breaches in their networks to avoid loss of customer information. In most cases these companies tend to rely on one person or a few individuals who are not even qualified to address these issues. It seems hospitality SMEs are not doing enough to protect customers in an online environment.

2.10 CREDIT CARD FRAUD

Technological development has changed the way people view money, especially the way it is used, and methods of payment (Prabowo, 2011:371). It has evolved from being physical, such as notes and coins, to being a figure in an account. This change in framework has changed the way monetary policy is viewed on a large scale, and has had an impact on SMEs. Background to research sub question 5 is provided.

How is credit card fraud dealt with in hospitality SMMEs?

The use of credit cards has spread and increased around the world. As a result this has become a common means of paying in many countries (Parvia, Veres-Ferrer & Foix-Escura 2012:501). As a result of this credit card fraud has become common and it is estimated that billions of dollars are lost annually (Bhattacharyya, Jha, Tharakunnel & Westland, 2011:602). This type of fraud has become one of the most sophisticated crimes internationally (Prabowo, 2011:371). The biggest threat recently has been from organized groups (Williams, 2007:341). It is reported that total loss due to online fraud for the year 2008 was estimated to be around 4 billion dollars which is an increase of 11 per cent on year 2007 loss of around 3.6 billion dollars (Jha, Guillen &Westland, 2012:12650). According to Prabowo (2011:376), there are five common types of credit card fraud and they are; application fraud, card-not-received, skimming/counterfeiting and card-not-present fraud. A person who suffers credit card fraud has a lot to lose. In most cases, it takes time to restore the damage done to an individual's ruined credit card as a result of credit card fraud, not forgetting the unwelcome time needed to restore a good credit card standing (Barker, D'Amato & Sheridon, 2008:399).

According to Haasbroek (2013), the South African Banking Risk Information Centre (SABRIC) reported that credit card fraud stands at 18 percent for the year 2012 in South Africa. This amounted to a 306 million Rand loss. Syndicates target bars and tourism establishments' staff and provide them with electronic devices that can read the information off their card in a matter of seconds. This information will then be sent to the fraudsters and fraudulent activities will begin (Haasbroek, 2013). Most of the credit card fraud occurred in Gauteng, KwaZulu Natal and Western Cape with 91 percent of all the fraud having been reported in these three provinces (SABRIC, 2013). Credit card fraud as revealed in the financial statistics is the tip of the iceberg, if not taken seriously, may cause serious damage, even the loss of safety, and where it is used for terrorist financing, loss of lives (Prabowo, 2011:376). Credit card fraud is effective because the chances of being caught are slim and in developing countries the laws are still at a nascent stage with only a few cases brought to the courts (Williams, 2007:340). The hospitality industry has become a target of credit card fraud. Businesses in this field are at risk and must be concerned (Snyder, 2013).

2.10.1 Summary – Credit card fraud

Credit card fraud seems to be on the rise but hospitality SMEs are not doing enough to protect their clients in an online environment. The fact that these companies tend to make use of a few people who do not even have relevant experience proves that they are ill prepared. Considering that credit card fraud has become sophisticated, a lot of investment is needed to effectively address this problem but it seems SMEs are not prepared to invest in security, and as a result are putting their customers' confidential information at risk.

2.11 CONCLUSION

The Chapter 2 layout (Figure 2.1) presents a summary and groups together the main headings of this chapter to assist the reader in following the flow of literature discussed.

The Internet offers companies many opportunities. Costs have decreased and availability of Internet connections have increased in recent years and SMEs can now take advantage of this modern technology. The Internet also produces problems for companies that are not well guarded against cyber-crimes. The hospitality industry relies on the Internet for most business transactions. Literature reveals that credit card fraud in the hospitality industry is on the rise. Many of these companies make use of out-dated systems making it easy for hackers to steal information.

SMEs are not willing to invest in information security, which leaves them vulnerable to such attacks. It is evident that SMEs are not immune to information security breaches in contrast to what is perceived to be the case. SMEs' security management is lagging behind compared to multi-national companies and this makes them vulnerable to attacks. The objective of research sub-question one is to explore trends in information security.

According to the literature, it is no longer enough to restrict access to computer rooms as was the case in the past. Traditional security controls such as physical access control and use of security guards are no longer enough to ensure security of the organisation's information assets. Information security has escalated as a result of increased Internet usage and therefore companies are now more alert and do put measures in place to ensure that their networks are secure. Sub-question two aims to uncover what companies are doing to ensure secure transactions whenever customers are conducting online business. Considering that companies are dealing with confidential data, it is important for them to keep it secure. Companies are now relying on ICT to effectively provide service to their customers and to compete and this reliance on ICT has brought security challenges. Over the past few years, work has been done to develop a number of different ways of managing information systems. According to the literature, there are a number of ways in which breaches can take place. Some of the common security breaches include hacking, social engineering, phishing, viruses and others.

Companies have come up with different strategies to deal with these breaches. They have put technological devices in place as well as providing training to employees to make them aware of ways to ensure secure transactions. In most cases, large companies have information security experts that deal with security issues on a daily basis and, as a result, criminals are turning to SMMEs for easy targets. This is in agreement with the finding that SMMEs are lagging behind when it comes to information security. Information security breaches are increasing and companies that do not have counter-measures in place are likely to suffer the consequences. Security breaches can lead to loss of customers and sometimes result in law suits by victims. For example, hospitality SMMEs deal with client sensitive information and sometimes a breach can result in data being accessed by an unauthorized person, which can be negative for the company.

From previous research it is found that SMEs adopt ICTs but they fail to make use of security measure that will help them to address security breaches. It is futile for SMEs to connect to the Internet without putting the necessary security measures in place. They even fail to use basic information security facets such as anti-virus programs and firewalls, leaving them vulnerable. Even password usage is not common in SMMEs particularly in the hospitality industry, where they mostly rely on usernames and passwords as their security measure. Training is not common amongst SMMEs even though it has been indicated that hackers are constantly becoming more and more sophisticated. Finally, customers expect their information, especially credit card information which is commonly used in the hospitality industry, to be handled in a secure manner.

In Chapter 3 the research methodology and design is presented.

CHAPTER THREE
RESEARCH DESIGN AND METHODOLOGY

Research design and methodology are essential aspects of any research and are discussed in this chapter. The researcher discusses the research method and instruments used for data collection. Furthermore, the following topics are covered namely; research design used, its reliability, validity, selecting the research design, selection of the population, the Cape Metropole area, sampling method, sample size, response rate, data analysis and content analysis.

3.1 INTRODUCTION

Struwig and Stead (2001:44) indicate that research methodology governs the scientific method that should be followed for data collection, as well as analysis of data to produce results to find a solution to a stated problem. In Chapter 2, the researcher reviewed the literature pertaining to information security. As mentioned, in this chapter the research method followed for this research is discussed to correctly address the formulated research questions. The research problem, research question and sub questions were stated in Table 1.1.

The main research question is stated again:

What policies and measures do SMMEs use to protect their information as well as ensuring adequate customer information protection in an online environment?

This research question can be expanded into the following research sub-questions:

- What are the trends in online security both locally and internationally?
- What policies and measures are in place for businesses to ensure customer security when conducting online business?
- To what extent is security training provided in the hospitality SMMEs?
- What are hospitality SMMEs doing to protect customers in an online environment?
- How is credit card fraud dealt with in hospitality SMMEs?

The nature of the formulated research sub-questions requires the research design to facilitate a literature review and empirical work to answer the research sub-questions. Therefore, literature is used to answer the first research sub-question and also provides background to research sub-question 2 to 5. Research sub-questions 2 to 5 are answered as part of the empirical work discussed in Chapter 4 using both surveys and interviews.

Surveys will be used for research sub-questions 2, 3 and 4, whereas interviews will be used to collect data to answer sub-question 5. The literature review assisted the researcher in understanding some of the security procedures that are used by SMEs around the world and therefore the researcher gained insight into the challenges they face. The policies and procedures used by SMEs around the world and locally, will also be studied and will lead to the design of the structured questions used in the survey and interviews.

3.2 RESEARCH METHOD

Research methodology can be defined as steps that must to be followed when gathering and analysing data in order to address a particular problem (Struwig & Stead, 2001:44). Leedy (1997:104) avers that there are various research methods available. These methods can be grouped into three methods, namely quantitative, qualitative and mixed methods research. A method is selected based on the type of research questions that are to be answered. The research questions need to be taken into consideration when deciding on the research method because sometimes a combination of the methods would be required (Maree & Van Weisthuizen, 2007:34).

A quantitative research method is used mainly to answer questions that deal with relationships regarding variables that are measured with the aim of explaining, predicting and taking control of the phenomena (Leedy,1997:104). If the sample is selected properly, the results can be generalised for an entire population. Furthermore, quantitative data is mostly presented in number format (Bamberger, Rugh, & Mabry 2006:237). Teddlie and Tashakkori (2009:233) indicate that quantitative researchers make use of attitude scales where attitudes, beliefs, self perceptions, intentions aspirations and other related issues are measured. These attitude scales are questionnaires in the form of surveys (Teddlie & Tashakkori, 2009:233).

Qualitative research on the other hand, is a research methodology also referred to as “interpretivism” (Bamberger *et al*., 2006:268). It can be defined as a process whereby researchers enquire to understand the problem and form a picture by using detailed data, which is collected from participants. Qualitative researchers collect large amounts of data by using general questions that are posed usually to a smaller number of people or participants, compared to a quantitative method.

According to Ivankova, Creswell and Clark (2007:15), the research questions are general and not specific as they aim to understand participants' experiences of the problem under investigation. A qualitative research method is capable of analysing concrete cases in their "…temporal and local particularity…" (Flick, 2006:13). Another commonly used method is mixed methods. This method uses at least one quantitative method and one qualitative method, where none of the methods are inherently linked to any particular observation (Gravetter & Forzano, 2006:151). According to Gray (2009:204), mixed methods can be defined as "…the collection or analysis of both Quantitative and Qualitative data in a single method whereby data is collected concurrently or sequentially…"

3.2.1 Reliability

Reliability using quantitative research means how consistent the same results will be (Leedy, 1997:35). In other words, reliability is enhanced if the same (or similar) results are obtained if the research is repeated on the same sample (Maree & Pietersen, 2007:147). It can be added that the measuring instrument plays an important role in reliability. Reliability can be hindered by varying subjects' responses, differences in the way that the instrument is administered, and alterations or changes to what was initially measured over time (Leedy, 1997:34).

3.2.2 Validity

Validity can be described as the extent to which the instrument measures what it is intended to measure (Struwig & Stead, 2001:132). Validity can be enhanced in several ways, for example, a common method is to use a pilot study to check the legitimacy of the questions (Birley & Moreland, 1999:42). In this research questionnaires will be hand-delivered to appropriate personnel (managers and IT personnel). SMMEs will be contacted by telephone or email in order to make an appointment with the relevant individuals. This is to ascertain their willingness to participate in this research. In order to further enhance the validity of this research, the researcher will conduct a pilot study as Birley and Moreland (1999:42) suggest. The first few questionnaires will be used as a trial. A few respondents will be asked if they understand all the questions in the questionnaire. Appropriate adjustments will be made to the questionnaire if required. The questionnaires will then be distributed.

3.3 RESEARCH DESIGN

Research design is the overall procedure that will be followed when conducting research. As soon as the research problem is identified and properly formulated, the next step is to create detailed steps that should be followed in the research process (Leedy, 1997:93). There are a number of research designs available (Bamberger *et al.*, 2006:232). For example, survey research, correlation research, experimental research and causal-comparative research amongst others. A research design should be selected based on the kind of research questions that will be asked and how the combination of these methods can add weight to the research (Gray, 2009:205). For this research, a survey will be used initially, followed by a qualitative approach conducting interviews. This combination is to gain more clarification by the researcher about certain aspects posed by the research sub-questions.

3.3.1 Selecting the research design

Yin (2003:21) discloses that the research design must be able to allow or facilitate the researcher to obtain answers to the original question on which the study is based. In this case, the research design needs to facilitate or address the answer to the following research question **"**What policies and measures do SMMEs make use of to protect their information as well as ensure adequate customer protection in an online environment?"

A sequential explanatory strategy will be used for this research that specifies the collection and analysing of quantitative data followed by qualitative data in two consecutive phases within a single study. This method is preferred because it provides the researcher with an opportunity to use interviews to understand some of the decisions that are taken by SMMEs, revealed in the quantitative part of this research. According to Cresswell (2003:215), this method is commonly used where unexpected results are obtained through a quantitative method. This method is straightforward and it makes it easy to describe and report on findings.

3.3.2 Questionnaire Design

Delport (2005:159) discloses that quantitative data collection methods commonly make use of measuring instruments in the form of questionnaires. According to Krosnic and Presser (2010:263) questionnaires are the preferred form of data collection from people and can be used together with other techniques. When designing questionnaires, it is advisable to keep important points in mind in order to best meet the objectives of the research.

First of all, the type of information that is required needs to be considered to both achieve the objectives of the research and fulfil the purpose of the evaluation. Secondly, a decision needs to be made on the type of questions and responses which will best capture information that is sought (Colosi, 2006:1). As mentioned, validity and reliability needs to be considered by making sure that the measurement procedure and the measurement instrument used meet the acceptable levels of reliability and validity. There are a number of response systems or question types from which a researcher can select so that the desired goals are met. Examples of some of the question types are open questions, closed questions, dichotomous questions, scaled questions, statements and others.

The researcher will make use of closed-ended questions for this research. These questions are preferred because when using open questions, some answers might not be clear. If using closed questions, this problem is averted as respondents could choose from a list provided. Most importantly, the research objectives will be considered when deciding on the type of questions to use for this research. As Delport (2005:174) suggests, the researcher needs to make sure that all the possible theoretically appropriate answers to a question can be determined. These types of questions will allow the researcher to compare questions with one another and where respondents do not fully understand a question, the response choices could clarify this. Leading questions will be avoided in order to ensure that reliable data is collected. Questions in this questionnaire are structured in such a way that one issue per question is addressed. In order to avoid bias, the researcher will attempt to ensure that all the possible answers are provided as alternatives. To achieve this, a five point Likert scale is used. This type of question allows the "…respondents to rate their degree of agreement or disagreement with the provided opinion…" (Dunn, 2010:249). This type of scale is the most commonly used method. According to Colosi (2006:3) a five point Likert scale is an appropriate method and the choices range from "strongly agree" to "strongly disagree". The five point Likert scale also allows researchers to quickly tabulate responses and determine the percentage of the respondents who agree or disagree with a statement.

3.3.3 Semi Structured Interviews

It is common usage amongst researchers to utilise semi-structured interviews in order to clearly understand participant's beliefs about perceptions or accounts of particular topics. This method is flexible for both the researcher and participants (De Vos, Strydom, Fouche & Delport, 2005:296).

The researcher will prepare a number of questions to guide them during the interview process. These questions will be formulated in such a way as to address the scope of the interview. This type of interview is preferred because the interviewer can deviate from the sequence of the questions (Flick, 2011:112). In other words, the interviewer can always ask more probing questions for clarity. De Vos *et al*., (2005:297) disclose that semi-structured interviews can last for a prolonged time and can become intense and involved depending on the particular topic. The questions will be kept neutral instead of leading in order to enhance reliability. They will also focus on research questions to make sure that the participants provide the information that is required for this research (De Vos, 2005:397). The method used for the interviews will be face to face at the companies' premises. The interview duration could range from 10 to 30 minutes and will be recorded whenever possible. In some cases, relevant and important data will be written down, helping to generate ad hoc questions during the interview.

3.3.4 Transcribing interviews

After interviews, the data will be transcribed in order to present it as the interviewees answered the questions. Terre Blanche, Durrheim and Painter (2006:302) note that it is better to refer back and forth to different parts of an interview if it is on paper, than if it is on audio cassettes, hence the need for transcribing of the data. It is advisable to transcribe directly to a word processing document. This will make it convenient to edit and structure the data and search for key words at a later stage. It is also crucial to transcribe everything rather than trying to decide which data is relevant and which is not (Terre Blanche *et al*., 2006:302). The researcher will read and listen to the recorded data in order to check for reliability as suggested in the literature.

3.3.5 Data Analysis

One of the challenging tasks of mixed methods is how to analyse data collected from qualitative and quantitative research. In this method, because data is collected in phases, the analysis is easier to see and conduct than in a convergent design (Creswell, 2012:552). For this research, the companies not making use of information security will be identified via quantitative data and then be invited to take part in qualitative data collection.

3.4 SELECTION OF THE POPULATION

In this research participants will comprise of SMMEs in the hospitality industry that conduct their business in the Cape Metropole area (defined in section 3.5). The researcher will visit websites such asthose of the Cape Chamber of Commerce, South Africa Tourism and Cape Town Travel to select the SMMEs for this research.

3.5 DEFINITION OF THE CAPE METROPOLE AREA

The Cape Metropolitan Council (1999:4) states that the Cape Metropole is a unique area which is well known for its floral diversity. The Metropole is located in the southernmost part of the African continent and covers an area of 2 175 square kilometres. It is located between the famous Table Mountain and the Hottentonts Holland mountains and is surrounded by the Atlantic and Indian Oceans (Cape Metropolitan Council, 1999:4).

3.6 SAMPLING

Sampling can be defined as selecting a number of participants from a population in such a way that they reflect a true representation of the entire population (Petersen, Minkkinen & Ebensen, 2005:261). It is not always possible for a researcher to cover an entire population within the research (Vandersoep & Johnston, 2009:26); hence, when a population is large, sampling is used (Maree & Pitersen, 2007:172).

According to Teddlie and Tashakori (2009:181) the first thing that needs to be considered in developing a mixed method strategy is to consider what strategy will best address the research question. Generally, there are three types of units that can be sampled; case, materials and other elements in the social situation (Teddlie & Tashakori, 2009:181). For this research, case sampling is selected whereby individual groups or participants can be selected to participate. In this case, the participants should be owner managers or IT managers of hospitality SMMEs. These people were selected based on their expertise since information security is a technical topic.

3.6.1 Sampling method

According to Leedy (1997:204), the researcher should consider the nature, characteristics and quality of the data before choosing a method to use for sampling. In this way, the correct sampling method will be used (Leedy, 1997:204). The results from the first part, which in this case is a quantitative method, will be used to draft the questions for ensuing interviews. This sampling method provides the researcher with the opportunity to understand in detail why these hospitality SMMEs tend to take security breaches lightly. Considering that this topic is sensitive, this sampling method is preferred to dig out more pertinent details from the respondents.

3.6.2 Sample size

A mixed method approach is when two different types of sample sizes are used; larger quantitative samples rely on well-defined population and well informed selections of smaller qualitative samples. This is based on informal sampling frames (Teddlie & Tashakkori, 2009:182). The likely sampling error for any sampling method and survey population depends on the sample size for quantitative samples (Hoinville & Jowell, 1982:61). A larger sample size will enhance the accuracy (Descombe, 2008:26, Hoinville & Jowell, 1982:61). Hoinville and Jowell (1982:61) are of the opinion that selecting the sample size is mostly based on judgement rather than on calculations. Maree and Pietersen (2007:178) further elaborate that it can be worrying if the researcher realises that the sample size is too small after collecting data. In order to avoid this problem, the researcher should consider a few factors (Struwig & Stead, 2001:118). For example, the quality and general characteristics of the population need to be considered.

The researcher will be able to narrow down the population by selecting only SMMEs within the hospitality industry. SMMEs in the hospitality industry are likely to show the same characteristics, unlike respondents from different industries. Since SMMEs in the hospitality industry are eligible to participate in this research, the sample size will not be as extensive as a sample from a heterogeneous sample or from different industries. Maree and Pietersen (2007:178) indicate that time and the cost of research may also play a role in making a decision about the sample size, however these aspects were not considered by this researcher.

Descombe (2008:26) summarises factors that determine the sample size:

- accuracy of the results
- the likely response rate
- available resources
- number of subdivisions likely to be made within the data.

As for a qualitative sample size, Teddlie and Tashakkori (2009:183) suggest it is better for researchers to look at saturation of data, for example, using interviews. But if no new information is gained from conducting interviews, then it is pointless to continue with more interviews. A point of saturation would then be reached when no new information is gained from conducting more interviews. The general rule is that the researcher should plan four or five interviews and once they have been conducted, the researcher should determine if saturation has been reached (Teddlie & Tashakkori, 2009:183).

3.6.3 Response rate

Considering that this research deals with a sensitive issue, SMMEs will be guaranteed confidentiality. Hoinville and Jowell (1982:70) state that it is often difficult to obtain responses from all respondents. It is, therefore, advisable that the sample size is made large in order to accommodate the non-response rate (Struwig & Stead, 2001:122). The researcher should attempt to make a questionnaire user friendly in an effort to improve the response rate (Hoinville & Jowel 1982:70). The selected SMMEs will be contacted telephonically to make appointments to deliver a survey for completion. In order to maximise the response rate, the survey forms will be hand-delivered, as suggested by McBurney and White (2007:246). Interviews will be conducted for the qualitative part of data collection.

3.7 DATA ANALYSIS

Alreck and Settle (1985:287) indicate that it is important that the researcher makes use of the correct tools for data analysis. Quantitative research data is normally analysed using statistical software (Shuttleworth, 2008), hence the decision to use SPSS software. This software is designed specifically for data analysis, particularly survey data, and can also produce different reports (Alreck & Settle, 1985:51). It further allows creation of frequency tables and bar charts, which makes it easier to interpret data. Data analysis in qualitative research methods is in the inductive form where particular cases are observed in order to generalise to a number of cases (Leedy, 1997:105).

3.7.1 Content analysis

Content analysis is a commonly used procedure to analyse text material of whatever origin, from media products to interview data. This method is mainly derived from using categories derived from theoretical models. The researcher takes into consideration the categories of texts, instead of developing them from the material itself even though the researcher may revise the categories in the light of texts under analysis. Content analysis intends to classify the content of the texts by allocating statements, sentences or words to a system of categories (Flick, 2011:137).

The first thing that needs to be done is to define the material. After that, the researcher needs to analyse the situation of data collection (Flick, 2011137). In this research, the owner managers and IT managers in hospitality SMMEs will be interviewed and their responses recorded. For the interviews, structured content analysis will be used. According to Flick (2011:137) for this method, the researcher needs to look for the types or formal structures in the material. By doing so, the researcher may notice specific topics or domains which characterize text. This method allows researchers to group together phrases with the same meaning therefore making analysing of data simpler and more consistent.

3.8 CONCLUSION

The researcher identified the research method to be used and needs to support the research question. This chapter examines the research methodology to be followed to achieve the research objectives. Research methods are discussed in relation to the research question. The researcher highlights the route taken to conduct empirical research and how the survey and interviews are conducted. This includes, briefly mentioning aspects of the population for the quantitative part and the cases for the qualitative part of data collection.

The next chapter will discuss the data collection and presentation of the results.

CHAPTER FOUR
DATA COLLECTION AND ANALYSIS

4.1 INTRODUCTION

Following the research methodology and design discussed in Chapter 3, this chapter presents the procedures followed for the data collection and analysis in sections 4.2 and 4.3, respectively. The research sub-questions 2 to 4 are analysed in section 4.3 whereas research sub question 5 is discussed and analysed in section 4.4. A conclusion to both survey and semi-structured interviews is provided in section 4.5

4.2 DATA COLLECTION

In this section the researcher discuses both the quantitative and qualitative data collection processes. A questionnaire is used to collect quantitative data (section 3.32) while semi-structured interviews are used to collect qualitative data and are discussed in section 3.3.3.

4.2.1 Questionnaires

A trial run was conducted before the quantitative data collection commenced. This was done in order to refine and remove any ambiguities contained in the questionnaire. The questionnaires were then administered to hospitality SMMEs within the Cape Metropolitan area. In Appendix E, the researcher reports on the validation that the respondents were SMMEs according to the South African government specifications. Each questionnaire was accompanied by a letter of introduction stating the aims of the research (Appendix A). The letter was signed by the researcher and supervisor. A total of 120 questionnaires were distributed to these SMMEs over a period of five months. Of the questionnaires sent out, a total of 63 were returned of which 56 were completed correctly. This gives a response rate of 47 percent. According to McBurney and White (2007:246), a response rate of 47 percent is a fairly good response. Respondents who were interested in participating in the research were asked to provide their details so that the results could be sent to them afterwards. Struwig and Stead (2001:119) indicate that there may be constraints that limit data collection from a large sample. For example, time may not allow for an extended study, but the validity of the study is important and should not be compromised at the expense of expediency. The respondents were given sufficient time to avoid sacrificing the accuracy of the results.

4.2.2 Semi -structured interviews

The researcher conducted semi-structured interviews from a different group of respondents. A total of four in-depth interviews were conducted. The interviews were conducted at the respondents' premises and lasted for approximately 25 minutes. Only IT managers and SMMEs managers were eligible for the interviews.

4.3 DATA ANALYSIS

The quantitative data collected was entered into SPSS software for analysis to produce results (Appendix D). SPSS software was used to present the output. Some diagrams were used to present aspects of the findings. On the other hand, the semi-structured interviews were analysed through content analysis, since it allowed comparisons of the data collected. The data was then transcribed to make sense of it. Overall, the data is analysed according to the research sub questions. Research sub-questions 2 to 4 are analysed in section 4.3.1 and research sub question 5 analysed in section 4.3.2. The questionnaire was statistically checked for reliability and the result is .842 (Appendix B) which is above .700 which is the minimum, therefore indicating that the questionnaire was reliable.

4.3.1 Research sub-question 2

This section presents the data to answer research sub-question 2. A survey was used to address this research question. On the other hand, literature was used to provide background to the research sub-questions in Chapter 2, Section 2.7.

What policies and measures are in place for businesses to ensure customer security when conducting online business?

It appears that SMMEs understand the importance of putting measures in place. This is depicted in Figure 4.1. It is revealed that 19.6 percent of the respondents indicate that they strongly agree that end-users are encouraged to follow security measures in place. This is obtained from questionnaire question 9.19 (Appendix D). Respondents were asked if staff members are encouraged to follow security measures put in place. It is further depicted in Figure 4.1 that a total of 51.8 percent of the respondents indicate that they agree with the above statement.

A total of 10.7 percent indicate that they are not sure whether end-users are encouraged to follow security measures in place or not as depicted in Figure 4.1 below. Figure 4.1 further depicts that 17.9 percent of the respondents indicate that measures are in place but are not enforced on employees rendering them useless because they are not emphasized. A total of 10.7 percent of the respondents indicate that they are not sure whether there is a procedure to enforce information security in the hospitality industry

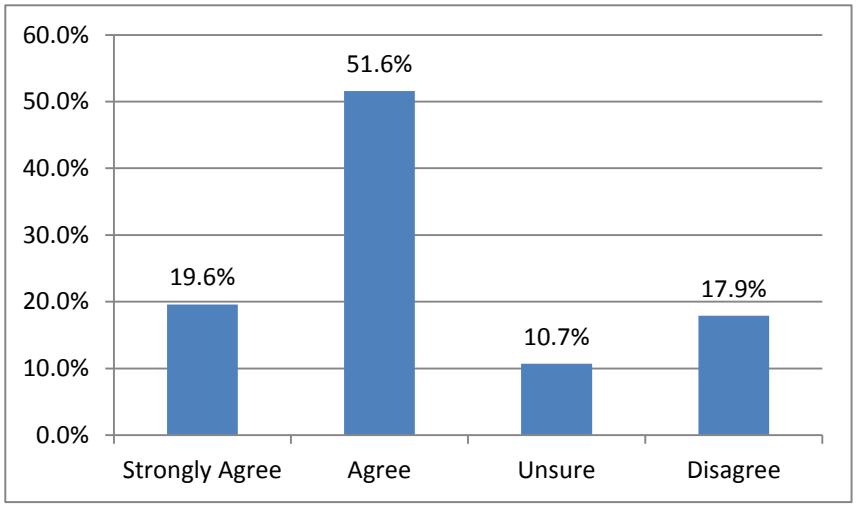

Figure 4.1: Security measure enforcement

Respondents were asked if they have security policies (Appendix D), question 9.18. Figure 4.2 depicts that a total of 7.3 percent of the respondents indicate that they strongly agree that their companies have information security policies in place to guide staff members while 40 percent agree.

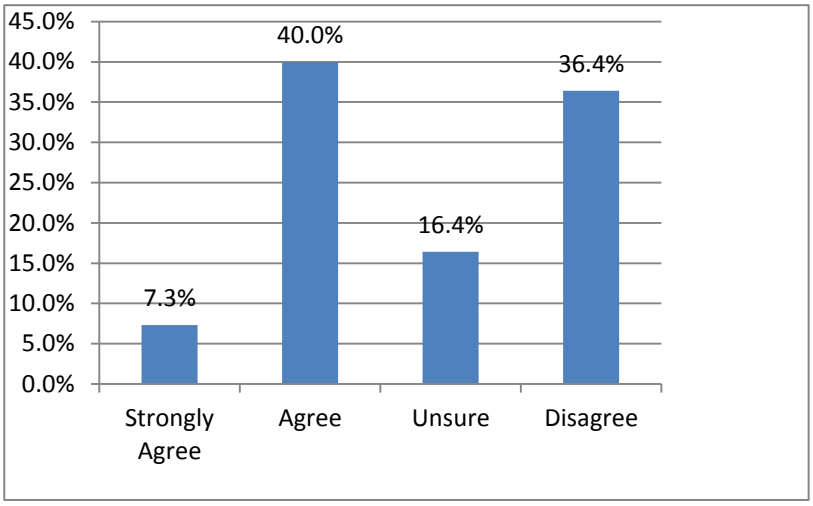

Figure 4.2: Information security policy possession

This shows that less than half of the respondents do not have policies to guide and advise staff members on security breach issues. Figure 4.2 further depicts that a total of 16.4 per cent of the respondents indicate that they are not sure whether their companies make use of security policies or not. On the other hand, a total 36.4 percent of the respondents disclose that their companies do not make use of security policies to address data breaches, as presented in Figure 4.2, despite handling sensitive customer data

When it comes to policy review, respondents were asked if their policies are reviewed on a regular basis or not, in question 9.22 (Appendix D), A total of 7.1 percent of the respondents indicate that they strongly agree that their security policies are reviewed on a regular basis while 26.8 per cent of the respondents agree proving that it is not common amongst SMMEs. A total of 21.4 percent of the respondents indicate that they are not sure whether their companies' information security policies are reviewed regularly or not. A total of 44.7 percent of the respondents indicate that they disagree that their security policies are reviewed regularly. As a result these companies' security policies can get outdated and this might have a negative impact on their security applications.

The following question was posed to the respondents "*Information security policies are accessible to staff members*", question 9.23 (Appendix D). It appears that security policies are inaccessible to staff members in most SMMEs with only 29.1 percent of the respondents indicating that they agree that information security policies are easily accessible. On the other hand, 27.3 percent of the respondents indicated they are not sure whether their security policies are accessible or not. At least 43.6 percent of the respondents indicate that they disagree that their security policies are accessible to staff members as a result leaving staff members in the dark because they do not have anything to refer to as a guideline for security procedures.

In question 9.24, (Appendix D), respondents were asked if their security policies are in line with their company's objectives. A total of 29.1 percent of the respondents indicate that they agree that their security policies are in line with their company's objectives. On the other hand, a total of 33 percent indicated that they are not sure whether their company's information security policies reflect the company's objectives or not. On the other hand, a total of 38.2 percent of the respondents indicated that they disagree that the company's policies reflect its objectives. This shows that these companies' security policies are in fact documents that are not relevant.

Considering that passwords are commonly used as a means of authentication in SMMEs, question 9.26 (Appendix D) assisted the researcher to find out if SMMEs have password policies. Figure 4.3 depicts that a total of 21.4 percent of the respondents indicated that they strongly agree that there is a password security policy in place while 17.9 percent agree that there is a password policy in place to guide staff members on its formulations.

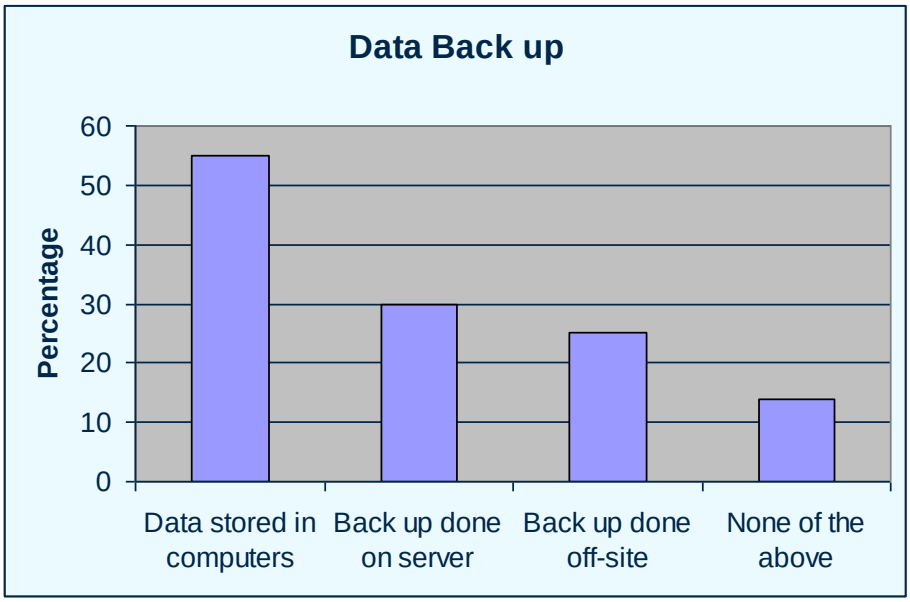

Figure 4.3: Data back-ups in SMMEs

Since unauthorized access has an ulterior motive, it is of concern to discover that a total of 10.7 per cent of the respondents disclose that they have been victims. Respondents were asked if they have been victims of information security breaches as a result of unauthorized access in question 9.14 (Appendix D). A total of 26.8 percent indicate that they were not sure whether their companies have been victims of unauthorized access or not. Even though a majority (62 per cent) of the respondents indicate that they have never been victims of unauthorized access, more needs to be done to avoid it considering the impact it can have on the company's information resources.

In order to find out if respondents have a procedure to address security breaches, question 9.2 was posed to the respondents in the questionnaire (Appendix D). Staff members should be aware of the steps to follow to report security breaches. Figure 4.5 depicts that a total of 44.6 percent of the respondents indicated that they agree that they have formal steps to report data breaches.

A total of 19.6 percent of the respondents indicated that they are not sure whether there is a procedure to report security breaches or not as depicted in Figure 4.4.Figure 4.5 further depicts that a total of 32.2 percent indicated that they disagree they have formal steps to report security breaches while 3.6 per cent strongly disagree. This might result in confusion of staff members about what to do if there is a breach

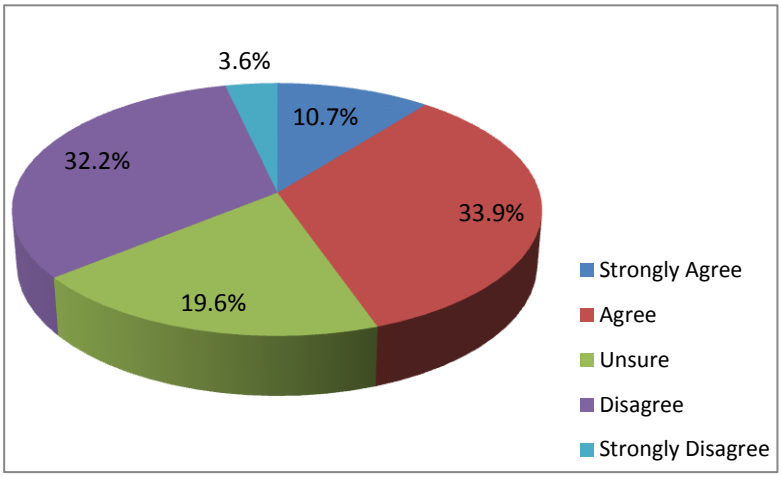

Figure 4.4: Formal steps to report breaches

In order to ascertain if respondents are making use of any devices to protect information, question 9.15 (Appendix D) was posed to them. SMMEs seem to understand the importance of putting measures in place such as anti-virus software, firewalls, encryption devices, and passwords, as revealed by 60.7 percent who agree and 19.6 percent who strongly agree. A total of 10.7 percent of respondents indicated that they are not sure whether they have devices in place to deal with security threats. A total of 8.9 percent of respondents indicate that they do not make use of any of the devices that are stated above, and as a result leaving themselves vulnerable to security breaches.

To find out how respondents maintain information security devices, especially anti-virus programs that need to be updated on a regular basis, a follow-up question to the above question was asked where respondents had to indicate how often they update (maintain) the devices (question 9.25, Appendix D).

The above stated security devices must be updated and monitored on a regular basis in order to keep up with the latest security developments in security. At least 18 percent of respondents indicate that they do not up-date their anti-virus device on a regular basis. A further 18 percent of respondents indicate that they are not sure whether their anti-virus devices are updated on a regular basis or not. Only 64 percent of the respondents seem to heed the call to maintain and update their security devices.

Posters can also help communicate the security message to staff members. At least 64 percent indicate that they disagree that their businesses use posters to communicate security messages. A further 14 percent of respondents indicate that they strongly disagree that their companies make use of posters. A total of 9 percent indicate that they are not sure whether their company makes use of posters or not while 7 percent of respondents indicate that they make use of posters to communicate information security messages, and 5 percent indicated that they strongly agree that they use posters to help communicate security messages. Considering that staff designing posters at SMMEs might not be conversant in the usage of polices, it was necessary to find out if posters are used to enforce information security in question 9.32 in Appendix D.

4.3.2 Research sub-question 3

This section presents the data to answer research sub-question 3. This research question was addressed through survey research. Literature was used to provide background to the research sub-question in Chapter 2, Section 2.8. In order to address this research sub-question questions from the questionnaire in Appendix D were used.

Research sub-question 3 is stated as:

To what extent is security training provided in hospitality SMMEs?

Figure 4.5 below depicts that a total of 58 percent of the respondents indicated that they provide training to their staff members while 12.7 percent indicated that they were not sure whether employees are provided with training or not. Question 9.28 in Appendix D was used to ask respondents to help the researcher gain an understanding of how new employees are recruited to ensure that they do not compromise the company's information resources. A total of 29.1 percent of the respondents indicated that they do not provide training to their staff members, thus as

a result making themselves vulnerable to security breaches as a result of staff members' mistakes.

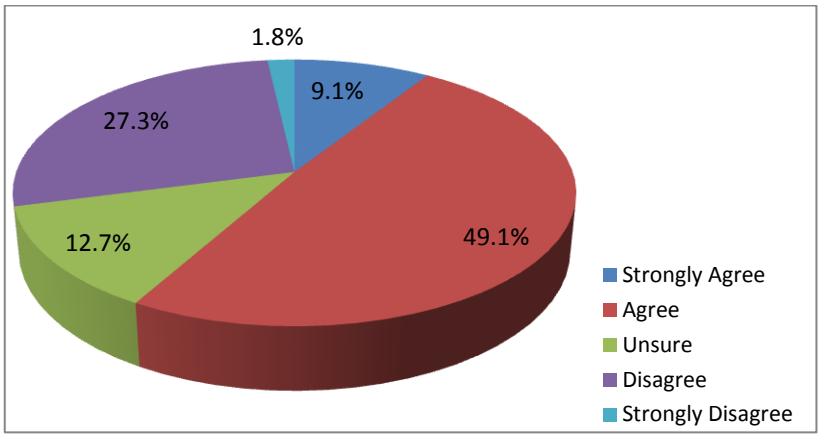

Figure 4.5: Induction of new employees

Respondents were asked if they provide training or promote awareness to staff members in question 10.1 (Appendix D). To understand how training is conducted in hospitality SMMEs, it was discovered that most (69.6 percent) of the respondents indicate that they neither possess nor provide security training to their employees as revealed in Figure 4.6. This can have a negative impact on these companies' security applications because without a training awareness program, the employees' security consciousness will not be enhanced. Only 25 percent of the respondents indicate that they possess a security awareness program to make staff aware of the importance of information security and their responsibilities to ensure that they exercise sufficient levels of security control. Figure 4.6 depicts that 5.4 percent of the respondents indicate that they are not sure whether their companies have a security program in place.

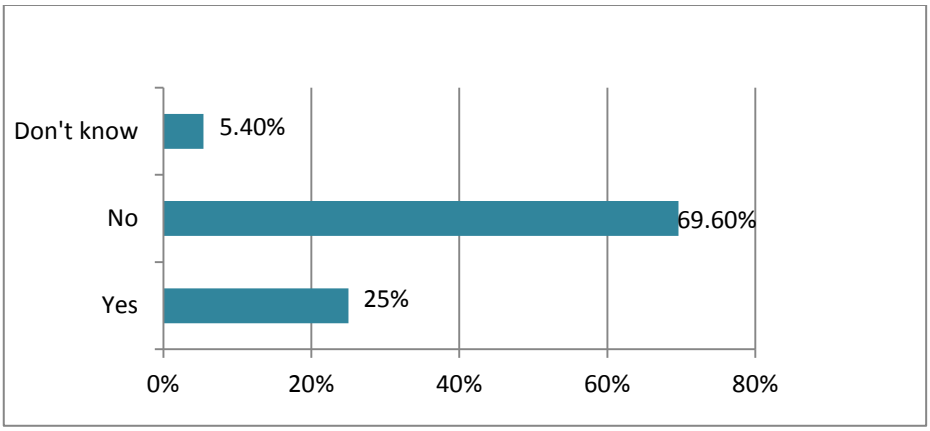

Figure 4.6: Training and awareness program possession

Employees' mistakes can have a negative impact on the company's information resources. It was therefore necessary to ask a question (question 9.27 Appendix D)to understand if hospitality SMMEs have previously been affected by employees' mistakes.

A total of 17.9 percent of the respondents indicate that they agree that they have suffered losses as a result of employee mistakes as depicted in Figure 4.7. Furthermore, Figure 4.7 shows that 3.6 percent of the respondents indicate that they strongly agree that they have suffered losses because of employee mistakes while 28.6 percent of respondents indicate that they were not sure whether they have previously suffered a loss because of employees' mistakes. It is further revealed in Figure 4.8 that a total of 32.1 percent indicate that they disagree that their businesses have been victims of security breaches as a result of employees' mistakes, while 17.9 percent indicate that they strongly disagree.

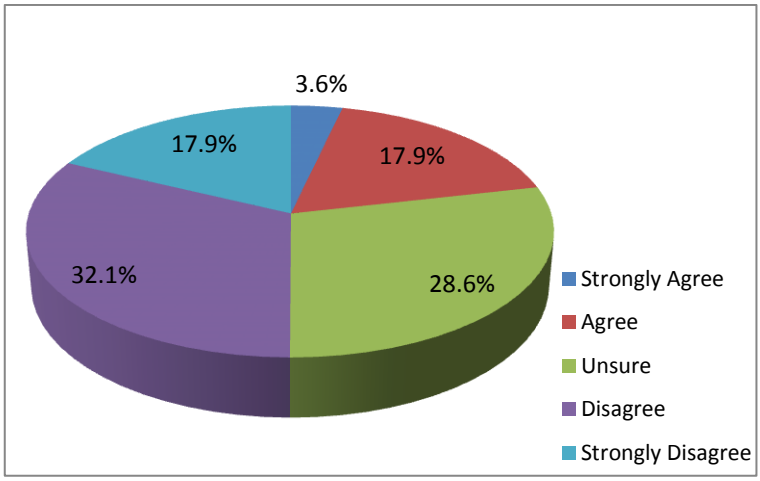

Figure 4.7: Security breaches as a result of employees' mistakes

Considering the fact that inside attack is common amongst companies, it is beneficial for SMMEs in the hospitality industry to prepare documents to be signed by staff members to discourage unwanted behaviour in security applications. It appears SMMEs do not heed this advice as 72.7 percent of the respondents indicate that they do not have any documents to be signed by new employees as depicted in Figure 4.8. Figure 4.8 further depicts that only 20 per cent of respondents understood the importance of making new employees sign documents while 7.3 percent indicate that they do not know whether a procedure exists within their companies. Question 10.2 (Appendix D) was therefore important to collect evidence of how internal attacks affect them.

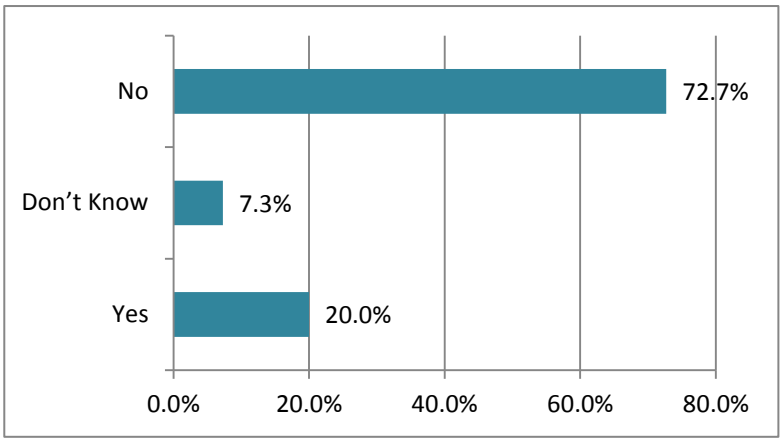

Figure 4.8: Possession of documents to be signed by employees

SMMEs are not immune to internal attacks and to verify this, question 9.29 (appendix D) was posed to the respondents. Figure 4.9 depicts that a total of 8.9 percent of the respondents indicated that they have been victims of internal attacks. A further 1.8 percent indicated that they strongly agree that they been victims of internal attacks. Figure 4.9 also depicts that 23 percent of the respondents indicated that they were not sure whether their companies have been victims of internal attacks or not, while a majority of the respondents indicated that they have never been victims of internal attacks as disclosed in Figure 4.9.

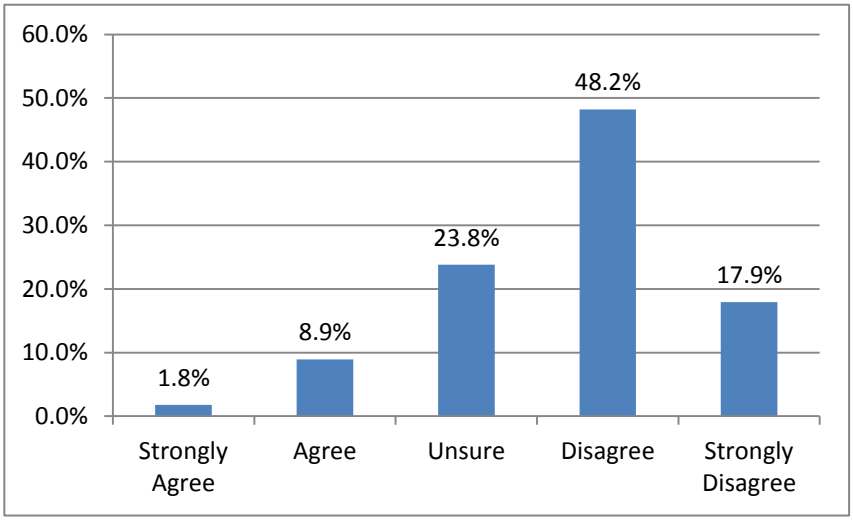

Figure 4.9: Internal attacks

It is also revealed in Figure 4.9 that a total of 48.2 percent of respondents indicated that they disagree that they have been a victim of internal attacks while 17.9 percent indicated that they strongly disagreed with the statement.

Considering that spam mail might have virus attachments, question 9.5 (Appendix D) asked respondents to comment. Concerning spam mail and attachments from unknown people, the data in Figure 4.10 above indicate that 54 percent of the respondents agreed that spam mail is not problematic for their companies while 14 percent of the respondents were not sure. It is further revealed in Figure 4.10 above that a total of 32 percent of the respondents indicate that they are experiencing spam mail problems and as a result these companies might lose money as a result of lost productivity.

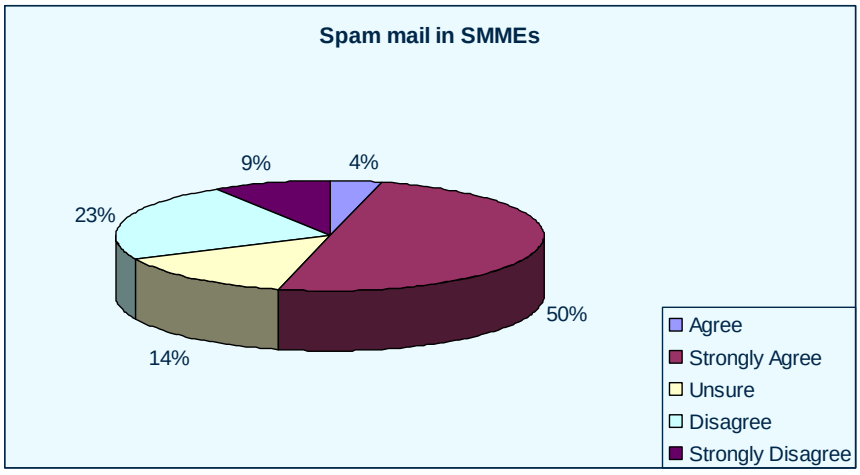

Figure 4.10: Spam mail in SMMEs

In a follow-up question to the previous question, the researcher wanted to find out how these companies address spam problems. It was therefore necessary to understand how the respondents address spam mail considering that some of them were experiencing problems in connection with spam, hence question 6 (Appendix D). A total of 45 percent of the respondents indicated that they encourage staff members to delete mail that has an attachment without opening it if they do not know the source while 23 percent indicated that staff members are encouraged to open the attachment. On the other hand 29 percent indicate that they do not encourage their staff members to follow either of the steps provided above. None of the respondents indicated that they encourage their staff members to email back the sender.

If employees are provided with proper training, they will be in a position to know what to do if they receive spam mail. Employees that are properly trained will be able to differentiate between spam mail and ordinary email. Even though a majority of respondents indicated that they do not have a problem with receiving spam mail, it is always better to put measures in place than to leave it until it is too late. They should provide their employees with training so that they can know what to do in case they receive spam mail. Anti-spam software should be used as well. Most SMMEs indicated that they are careful when it comes to email attachments.

4.3.3 Research sub-question 4

This section presents data to answer research sub-question 4. A survey was conducted to collect data to answer this research question.

What are hospitality SMMEs doing to protect customers in an online environment?

Each individual is entitled to privacy when conducting online business. It is therefore important for respondents to ensure security to customers hence question 9.17 (Appendix D) was posed to respondents where they were asked whether they ensure security to their customers whenever they do online business with them. Figure 4.11 depicts that 55.4 percent of respondents indicate that they agree that they guarantee their customers privacy whenever they conduct online business with them.

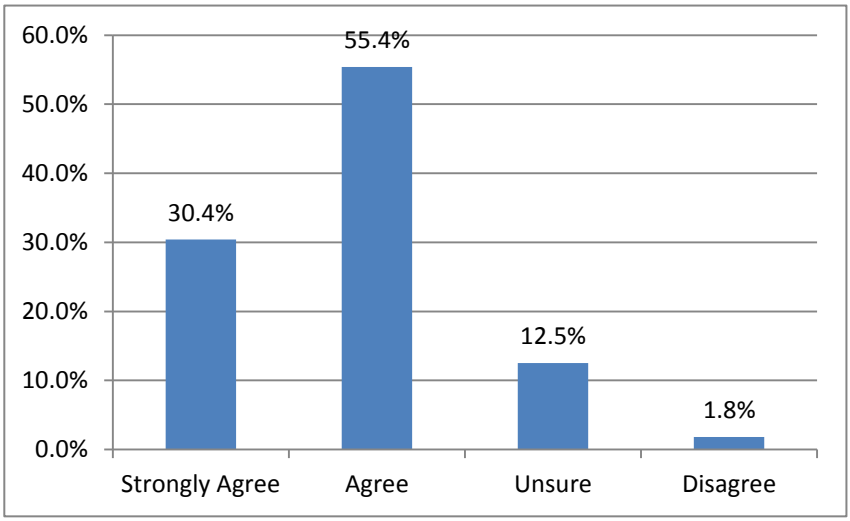

Figure 4.11: Customer privacy in SMMEs

A total of 30.4 percent indicate that they strongly agreed that customer privacy is guaranteed. This shows that these companies understand the importance of providing privacy to their clients. Figure 4.11 further reveals that a total of 12.5 percent indicate that they are not sure if their companies guarantee customers privacy whenever they conduct online business with them. Ironically, there were some respondents (1.8 per cent) who revealed that they do not guarantee their customers security when conducting online business.

In relation to client information security, it appears a majority of the SMMEs understand the importance of keeping client information secure as revealed in Figure 4.13 below where 90.7 percent (37 percent strongly agree and 53.7 percent agree) of the respondents indicate that they agree that credit card information is kept secure. This further shows that respondents value the customers' information and understand the consequences of losing customer data as a result of negligence. A total of 5.6 percent of the respondents indicate they were not sure whether credit card information is kept secure or not as revealed by Figure 4.12. Amazingly, some (1.9 percent) respondents revealed that they do not keep customer data secure as a result making it easy for fraudsters to steal information and use if for their own purposes as Figure 4.12 depicts. It was therefore necessary to understand whether respondents protect credit data that has become a target of hackers hence question 9.30 which reads "credit card information is kept confidential" was posed to the respondents.

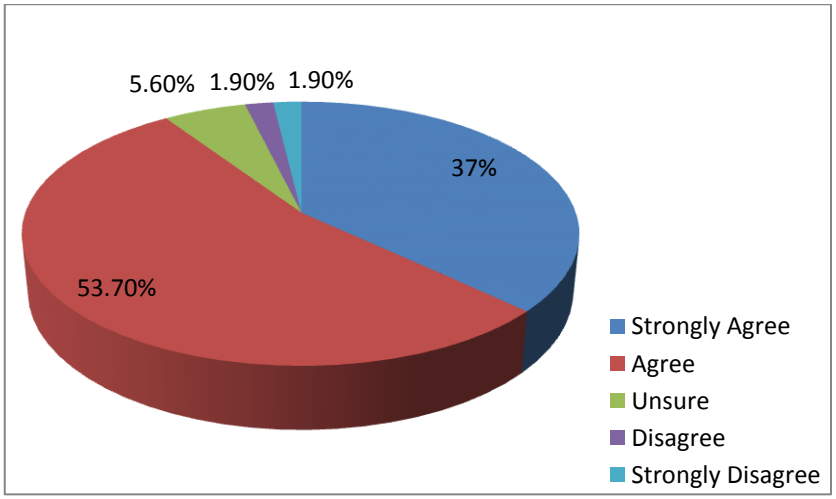

Figure 4.12: Customer data security

Figure 4.13 illustrates that even though most of the respondents indicate that there is strict control over the external and internal distribution of paper or removal media that contains client information, there are some who do not carry out this task as revealed by 26 percent of the respondents. This negligence by the companies can have a negative impact especially if breaches can occur as a result of this. Figure 4.13 further reveals that a total of 8.9 percent indicate that they don't know if there is strict monitoring of material with customer information. On the other hand, a total of 64.3 percent of the respondents indicate that there is control over external and internal distribution of paper or removal media that contains client information as depicted in Figure 4.13. This information reveals how important it is to protect media that contains client data, and the researcher asked the respondents whether there is strict control over paper or electronic media that contains client information as stated in question 10.3 (Appendix D).

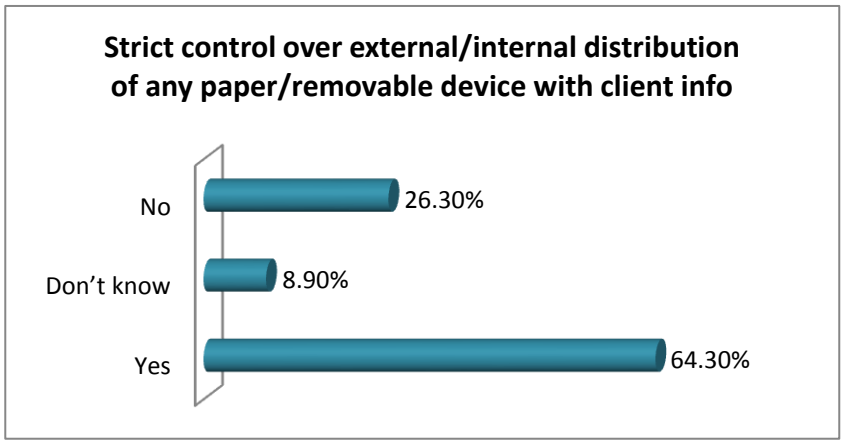

Figure 4.13: Media with client information control

To further understand how respondents value customer data, a follow up question (question 10.4) to find out if they protect any media that contains customer data or not was posed to the respondents in Appendix D. According to Figure 4.14, a total of 58.2 percent of the respondents indicate that they protect removal media that contains sensitive credit card information while 7.3 percent did not know whether media that contains sensitive data is protected or not. Despite admitting that they deal with sensitive client information, an incredible 34.5 percent of the respondents indicate that they do not take any precautions to protect media that contains client information as depicted in Figure 4.14.

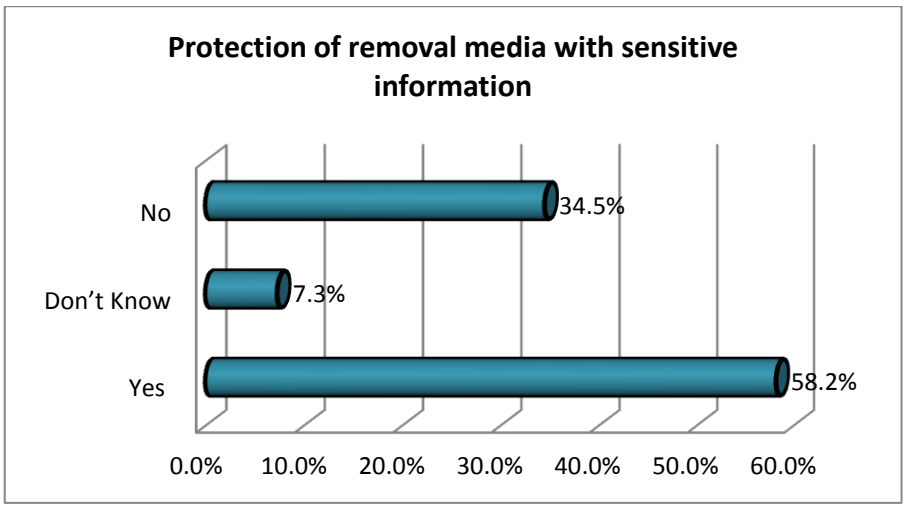

Figure 4.14: Protection of removable media

Respondents were then asked (question 9.31in Appendix D) if they conduct weakness assessment in their networks to minimize risks in their networks, Figure 4.15 depicts that 26 percent of respondents indicate that they agree that they conduct vulnerability assessment processes on the network on a regular basis while 4 percent indicate that they strongly agree. Figure 4.15 also indicates that a total of 25 percent of respondents indicate that they are not sure whether the company conducts weakness assessments on a regular basis.

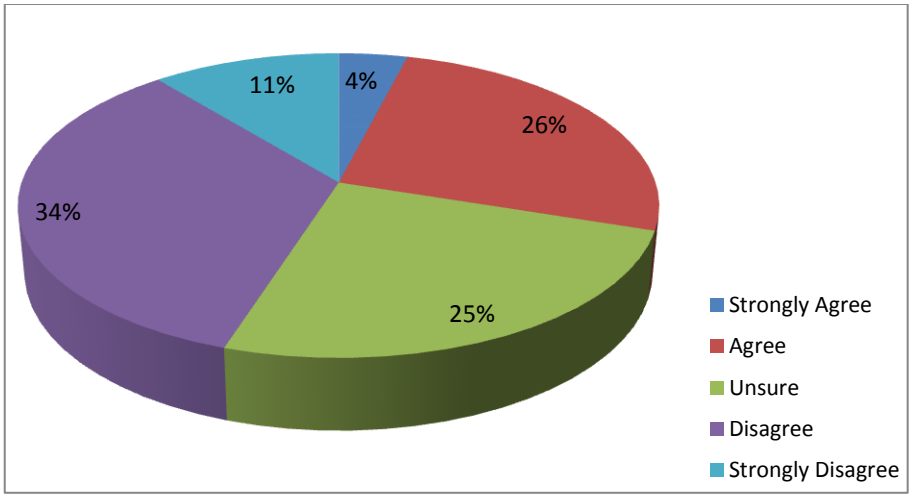

Figure 4.15: SMMEs vulnerability assessment

Respondents were asked if they have a weakness assessment procedure to minimise breaches (question 9.31) in Appendix D. A total of 33.9 percent of respondents indicated that they disagree that their companies conduct vulnerability assessment process on a regular basis, while total of 12.5 percent indicated that they

strongly disagreed that there is a weakness assessment program that is conducted regularly within their businesses. Only 28.6 percent of the respondents indicated that they carry out weakness assessment in their networks. A further 25 percent indicated that they are not sure if their companies carry out a weakness assessment program. This shows that vulnerability assessment is not common amongst hospitality SMMEs making them easy targets.

4.4 SEMI STRUCTURED INTERVIEWS

In this section the researcher analysis the qualitative data from the four respondents to answer research sub-question 5 (Appendix F to I). Semi structured interviews were conducted and the four interviews are summarised in sections 4.5.1 to 4.5.4.

Research sub question 5 is stated as:

How is credit card fraud dealt with in hospitality SMMEs?

4.4.1 Interview 1

The common security problem that is facing companies is attempted credit card fraud. In most cases, the culprits try to make use of fictitious credit card information. This shows that hospitality SMMEs are a target of credit card fraudsters. The company has never experienced a serious credit card scam since an administrator was hired on a permanent basis. This shows that the company values the customers' information. In most cases, the SMME is able to detect the breaches before they cause any harm. There was only one minor incident where a client accused the company of double charging him when he was paying for a flight. This problem was sorted out quickly. In order to address some of the security challenges that the SMME faces, it relies on the Internet Service Provider firewall. The administrator will then monitor the network as well as maintain the firewall.

The SMME makes use of external hard-drives which are stored both on-site and off-site to back up information. They also make use of cloud computing as a back-up procedure. According to the interviewee, should they lose data that was not backed up, they can request it from the Internet Service provider. Their Internet Service Provider (ISP) keeps the information for 365 days.

With regard to how users are authenticated into the system, the end-users make use of passwords and usernames. They use the person's surname as the username and passwords are personal. Passwords, which can be the easiest route by which fraudsters can gain access into a system, are changed regularly making it difficult for outsiders to crack passwords. Staff members are expected to change their passwords after 60 days. The SMME's system is programmed in such a way that each user will have to change his or her password after the first use.

Passwords are confidential and cannot be disclosed to anyone else except the user. The company also makes use of the ISP firewall to minimise the downloading of malicious software from the Internet by staff members. The company's firewall does not allow downloading of files from the Internet.

The SMME does not make use of guidelines like SABS and ISO 27001. A team of experts usually form rules that will drive the company forward. Even though the SMME understands that that these security standards are important, they believe they have a security team that can formulate rules and standards that are capable of addressing security breaches.

Employees are provided with training to deal with technological changes and security demands. Every three months, employees are sent for rotational training. Training normally ranges from three to six months. When it comes to new employees, they are provided with contracts that are expected to sign as soon as they join the company. This is to make sure that they do not violate the company's security rules.

In the case of a security breach, the employees are expected to report the breach to the network administrator as soon as they notice it. The network administrator will then deal with the problem. Regular checking of the network to determine if there are any breaches is commonly conducted. Employees are well informed about the acceptable and unacceptable behaviour when it comes to computer usage. The SMME also monitors each staff member's internet protocol in order to make sure that they do not violate the company's internet policies. Where employees are found to be violating the company's policies, they will be given warnings and should persist on doing that again, they will be fired. The SMME had one incident whereby an employee violated the company's policies. The employee was dismissed after it was discovered that it was a repeated offence. This proves that insiders can contribute to security breaches.

The SMME's security rules were formulated by management with the assistance of the Internet Service Provider. The Internet Service Provider came up with the rules and the management selected the policies that they believe can drive the company forward. Policies are updated once in a while in order to make sure that they keep up with security developments. Apart from security rules, the company makes use of contracts to dissuade employees from abusing the company's information systems. The contracts are normally signed at the beginning of employment. The SMME also relies on the anti-virus software which is updated daily to guard against virus attacks.

4.4.2 Interview 2

The company has outsourced IT services, including security issues, to an outside IT company. The SMME believes that by hiring an IT company the costs will be less. The IT company has been given a full mandate to take care of the network, which might be risky for the company considering that they deal with confidential information from time to time. Staff members are expected to report to the manager should they notice a security breach. Data is also backed up by the IT company. Data back-up is done on a daily basis to avoid losing important information. The system that is used by the company allows them to only back-up data for seven days. After seven days it will be deleted and new data will be backed up.

The SMME has never had a serious security breach before. Viruses are the only challenges that they have to deal with in most cases. Most of the time, computers that get infected by viruses are those that are used by clients. The SMME bought a licence for the whole year and the antivirus program updates itself every three months. Considering that viruses are becoming trickier, relying on an anti-virus program that updates itself every three months might prove ineffective. The SMME relies on the IT company to recover data should it happen that it is lost. The two companies signed an agreement that the IT company will receive a stable amount even if they do not service or fix any computer.

In order for users to gain access into the SMME's network, a password is required. However, staff members have two passwords. One password (personal) is used to authenticate them into the company's systems while the other one is used for accommodation bookings. The password used for accommodation does not change making it easy to access credit card data by former employees should they gain access into the system.

As for the personal password, it depends on the individual. Management trust that staff members will keep their passwords secure and therefore do not see the need to enforce regular password changes and this can be costly considering that staff members are poorly trained and as a result lack password management capabilities. The SMME system does not allow downloads from the Internet. On the other hand, staff members are encouraged to join social networks as they believe that it markets the company.

The SMME does not make or does not subscribe to any security standards. It believes that they do not need to follow security standards such as ISO 27001 because security is not their primary goal, a view which might have a negative impact considering that they deal with customer data on a daily basis. They have delegated the security mandate to the IT company. Nothing special is done to make sure that staff members do not abuse the company's resources and this can result in loss of information as a result Employees have signed the contracts and they are expected to abide by them. Contracts alone are not the best way of communicating security issues to staff members because they hardly refer to them for security advice. Other than that, the company has pinned its staff compliance to security on trust. Staff meetings are held whenever possible to discuss issues pertaining to information security. Staff members are informed about the importance of keeping data secure. In these meetings staff members are expected to raise issues that are bothering them.

4.4.3 Interview 3

There is nothing special done by the company to make sure that outsiders do not gain access to the documents that contain sensitive information, except limiting access to the room where the documents are kept. This means that as long as outsiders can gain access into the company's information systems, they can harvest as much confidential information as possible and use it for their own benefit. Important data is backed up through the usage of external hard drives. Each staff member has been given an external hard drive to use to back up information. The SMME has never had problems with information that is sent via networks and therefore does not see a need to guard against network intruders, relying on the fact that if it is not broken then don't fix it. Credit card fraud has never troubled this particular SMME. Viruses are the only challenges and the only persisting problems that they experience. In 2011, one of the company's computers crashed as a result of viruses and this shows that viruses have the capability to cause serious harm if no measures are put in place.

The company does not allow the use of memory sticks as they believe that these can expose their computers to viruses. The company's anti-virus is updated after a year. The SMME manager discloses that they do not assign much finance to computer security, even though they handle customer information on a daily basis. Their security budget varies from month to month because it depends on the number of times they have hired the consultant. It shows that these companies do not have people hired to take care of their security issues and they only call on consultants when there is a problem. IT consultants are hired on a temporary basis to fix any problems that the SMME might be experiencing.

The SMME does not make use of passwords to authenticate staff members into the system. They believe that because their workforce is small there is no need to use passwords. The company has a total of 14 employees. Passwords do not only minimize internal threats but they can also minimize external threat. The company manager believes that building trust amongst the staff members is the best recipe for dealing with information security threats. Staff members are allowed to download files from the Internet as long as it is work related material. Clients are only allowed to use basic Internet. That being the case, nothing has been put in place to stop clients downloading files from the Internet. The company does not make use of any guidelines to monitor their security standards as they believe that their workforce is too small.

Staff members are not provided with security training because the SMME manager believes that it is not worth it for the company to train employees and end up losing them to big companies. Considering that security problems are escalating, training can be a good platform to equip employees to be in a position to handle security issues. Staff members are expected to sign contracts when they join the company. An employee was given a warning after it was discovered that he gave a client permission to use one of the staff computers. Clients are not allowed to use staff computers as they store sensitive information. In the event of a security breach, staff members must phone one of the IT companies that normally help with IT issues to assist with the breach.

The SMME manager disclosed that they do not have security policies and rely on word of mouth rules. Where possible, meetings are organised to discuss pressing issues. In order to make sure that customer's details are kept secure, staff members are encouraged to keep client information secure especially seeing that online booking is conducted in the company. The clients are also assured of a secure

transaction whenever they conduct online bookings with the SMME as stated on the SMME website.

4.4.4 Interview 4

Credit card fraud which is reported to be experienced by hospitality companies has never troubled this company. The SMME has branches in other locations such as Johannesburg and the Kruger National Park. The SMME sets high standards and has put some measures in place to make sure that they do not become victims of security breaches. For example, this SMME has invested in the latest technology as well as engaging top consultants to take care of their IT issues including information security. In order to make sure that outsiders do not gain access to sensitive information, the SMME manager disclosed that they make use of a system that backs up information every two hours. The program is running on laptops as well and if there are any viruses, the user will be alerted. To further avoid risking the SMME information resources, the usage of memory sticks is not allowed. Computers that are used by clients allow them to only browse the Internet; no other applications such as Microsoft Word are installed on the computers

Every two hours data is transferred into external hard drives. This is done in order to minimize the number of people who have access to the backed-up data. In most cases, any branch that needs backed up information can request it from the Johannesburg branch because that is where data is controlled. The booking system is centralized and is controlled from Johannesburg. Should the company loose data, they always request it from the IT consultants since they have the expertise to recover lost data.

The Johannesburg branch, which is the headquarters, is the one that allocates funds for the different activities. The interviewee could not specify the percentage of the funds allocated to security relative to the overall budget since the budget was done in Johannesburg, but the company spends a lot of money on IT related issues. The staff members make use of usernames and passwords to log into the system. Passwords are personal though. Staff members are allowed to use the password for as long as they like and this can be the downfall of the company because passwords should be changed regularly. The staff members were advised to keep their passwords personal and avoid disclosing them to anyone. The company has installed a firewall that does not allow the downloading of files from the Internet. The interviewee makes it clear that downloading of documents is not permitted as indicated by the following quotation:

> "Users cannot download anything from the Internet. Remember we are not a research organisation where users spend most of their time looking for information on the Internet and downloading and saving information to use at a later stage. Even anti-virus that we use, is not downloaded from the Internet. Our anti-virus was not purchased on the shelves. We consulted the vendors to make sure that our anti-virus meets our expectations".

Since the SMME's booking system is centralised, new staff members are advised to be vigilant when dealing with client information. Users are not provided with training because the company recruits people who are capable of using the company's information systems. Investing in staff members training can help avoid costly mistakes. Staff members are expected to know the security concerns that are facing the hotel industry in general. In the event that there is a security breach, junior staff members must notify a senior staff member so that the breach can be dealt with quickly. Senior staff members are equipped enough to know what to do in cases of security breaches.

The company does not have information security policies but relies on rules that are mostly not written down. The SMME's only document that is used to alert staff members about security breaches is the contract that is signed when a new employee joins the company. Information security rules were mostly formulated by the management of the company after consulting with IT consultants. Most of these rules were formulated by the Johannesburg branch because that is the headquarters.

The anti-virus that is used by the SMME is updated on a monthly basis, but the IT consultant regularly visits the company to check if all computers are working well. The consultant will then scan the computers for viruses. The interviewee makes it clear that they rely on modern technology to effectively compete as a hospitality industry company. But in order to make sure that customers' sensitive information is not compromised, the company have made their systems secure. They did so by informing the staff members to be vigilant and cautious whenever they are helping clients with online booking. The SMME also made sure that only a few people from the management team can access sensitive clients' information.

4.5 CONCLUSION

Below are the summaries of the data presentation and analysis of the four research questions.

4.5.1 Research sub questions 2 to 4

This research has revealed some new insights. Even though the respondents are managers within their businesses, it seems some of them do not want to spend on security related issues, which might lead to their downfall. The other important aspect that was found is that SMMEs managers still believe that technology alone can solve security problems. They tend to overlook the human aspect of information security.

A few SMME managers indicated that their backups were done off-site. In most cases customers book accommodation online and if there is a computer crash, then SMMEs that do not back-up the information can have problems.

4.5.2 Research sub questions 5

The interviews revealed that SMMEs understand the importance of keeping client information secure. The SMME managers reveal that they outsourced the IT services to the consultants. One of the SMME managers indicated that they have had one computer crashed as a result of viruses. This particular SMME updates its anti-virus after 12 months. The SMMEs only hires consultants whenever they are experiencing technical problems. The other SMME managers revealed that attempted credit card fraud is troubling it. While the other SMME managers indicated that they have never experienced credit card fraud, they seem to have taken the wait and see approach.

In the next chapter the results are discussed as well as providing guidelines to use when trading online.

CHAPTER FIVE
DISCUSSION OF THE RESULTS AND GUIDELINES

5.1 INTRODUCTION

The aim of this chapter is to discuss the findings of this research followed by a conclusion. A research question and five research sub questions are proposed in Table 1.1. These research questions are answered first of all, using literature in Chapter 2 to explore the background to these research questions and to answer research sub question 1. Secondly, a quantitative method using a questionnaire is used to answer research sub questions 2 to 4. Finally, a qualitative research method using in-depth interviews is used to provide respondents the opportunity to explain in detail the challenges they face in their quest to address credit card fraud. This answers research sub question 5.

The findings in section 5.2 are structured in such a way that each research sub question is presented followed by a brief discussion. A conclusion follows each research sub question. An overall conclusion is presented in section 5.3

5.2 FINDINGS OF THE RESEARCH

The formulated research sub questions are:

- What are the trends of online security both, locally and internationally?
- What policies and measures are in place for businesses to ensure customer security when conducting online business?
- To what extent is security training provided in the hospitality SMMEs?
- What are hospitality SMMEs doing to protect customers in an online environment?
- How is credit card fraud dealt with by the hospitality SMMEs?

These five research sub-questions are discussed in sections 5.2.1 to 5.2.5.

5.2.1 Research sub-question 1- Trends of information security

As indicated earlier, literature was used to address this research question.

What are the trends of online security locally and internationally?

This research sub question 1 seeks to assist the researcher to explore security trends that have been developed, both locally and internationally. Literature is used to address this research sub question, discussed fully in Chapter 2 (section 2.6).

With the development of technology, users started accessing their office computer systems remotely via telecommunications lines, compared to previously physically locked computer rooms after hours, or specific access times. New challenges emerged in the 21st century as the value of information appreciated. Companies had to invest more in their networks and computer systems to protect information. Hackers became a threat to companies because they wanted to obtain information, especially details of customers and credit cards. This is even more prevalent in the hospitality industry. A number of threats also emerged making it difficult for companies to effectively deal with security breaches. This affected SMMEs leading to the emergence of information security trends. These are: focal areas in information security, secure network protocols and risk analysis.

- **Focal areas in information security:** Information security goes hand in hand with the CIA triad, which stands for confidentiality, integrity and availability. Two other security requirements have been added to this and they are authentication and non-repudiation. These five factors are key drivers to ensure information security.
- **Secure network protocols:** This is an agreed upon way of transmitting data between two devices. The protocol was designed to ensure privacy and integrity over the Internet. The secure network protocols play an important role in ensuring that information is protected by making use of data encryption, server authentication, message integrity and optional client authentication.
- **Risk analysis:** It is vital for companies to try and minimize threats as it is not an easy task to eliminate threats totally. Risk analysis can be used in this regard.

5.2.1.1 Research sub-question 1 summary

This research question assisted in showing that information security has evolved over time. At first information security was maintained by only restricting access to computer rooms, but with the connection of computers to the Internet, new challenges emerged. For example, restriction alone is not enough. Investing in intrusion detection devices is needed and companies must constantly monitor their networks. Trends of information security emerged. These trends are: focal areas in information security, secure networks protocols and risk analysis.

5.2.2 Research sub-question 2- Policies and measures

This research sub-question seeks to assist the researcher to explore what policies and measures have been put in place by hospitality SMMEs to ensure customer security. The empirical data results for this research sub question are discussed in Chapter 4 (Section 4.3.1).

What policies and measures are in place for businesses to ensure customer security when conducting online business?

This research sub question also assisted the researcher to explore what policies and measures have been put in place to curb security breaches. Considering that personal data is important to the hospitality industry, companies are expected to put measures in place to ensure security. Even though the majority of the respondents indicate that they understand the importance of policies, a considerable percentage of the respondents do not have these in place. Without security policies, there will not be a document available to specify how to safeguard confidentiality, integrity and availability of information. Technology alone cannot effectively address security breaches, these SMMEs are thus putting customers' information at risk. A combination of both technology and human aspects can assist in dealing with security issues effectively. Some respondents indicated that they have policies but they are not enforced. This makes security policies somewhat useless. Surprisingly, some respondents indicate that they do not have any security measures in place to minimise security breaches, as a result making it easy to compromise their information. It is noted that the majority of respondents indicate that they encourage their employees to follow provided guidelines. Considering the importance of information security policies, it is of paramount importance to ensure that these documents reach their target audience. Some respondents admit that even though they have security policies, they are not presented to employees who are sometimes the targets. As a result, staff members struggle to effectively deal with breaches without any documentation. On the other hand, some SMMEs do not take precautions to avoid data loss.

Fifty percent of the respondents indicate that they do not have password policies. According to Bafna and Kumar (2012:130), in order to enhance the security of passwords, SMMEs must make use of a set of rules, commonly known as password policies. These findings indicate that these respondents' information resources are at risk because staff members may not be aware of how to keep passwords secure.

Without password policies, staff members will in the dark on how to formulate passwords that cannot be cracked easily. They also would not know that they are not supposed to share passwords with anyone. Considering that phishing is on the rise, respondents who indicate that they do not have password policies are putting their information resources at risk because staff members may end up revealing their passwords to strangers.

Unauthorised access, which has the capability to cripple a company's information systems, appears not to be given the attention it deserves. Considering that unauthorised access is carried out by people with a motive of taking subversive action, it needs to be minimised at all cost. The lack of procedures to deal with unauthorised access is tantamount to disaster. It equates to the lack of measures to address rising security breaches, which can result in loss of critical data. Unauthorised access can also be as a result of both inside or outside attacks. These companies are not immune to unauthorised access, as some respondents reveal that they have been victims of such attacks. It is of great concern, considering the impact that can be caused by unauthorised access.

Insider attacks appear to be common amongst hospitality SMMEs. For example, 10.7 per cent (section 4.3.1) of respondents disclose that they have been victims of insider attacks. This indicates that hospitality SMMEs are not immune to such attacks as it was previously thought. It is probable that some insider attacks might go unnoticed because insiders are familiar with company's information systems.

Theft of computers appears to be another problem that is a concern for hospitality SMMEs. A total of 35 per cent (section 4.3.1) of respondents indicate that they have been victims of computer theft. Considering that computers and laptops are used to store data, losing these can have serious consequences to the business.

Virus attacks are common amongst SMMEs in the hospitality industry. As long as this problem persists, there is always a risk of losing information. Virus attacks have the capability of causing damage to company resources, especially those companies that deal with confidential data. It is found that some respondents fail to update their anti-virus software. The lack of updated anti-virus software will leave company information systems vulnerable to virus attacks. For example, close to half of the respondents (section 4.3.1) reveal that they have previously lost data that was not backed-up before, due to virus attacks.

It is evident that SMMEs are aware of the implications of exposing confidential information, especially client information, but they tend to fail where it matters most, putting measures in place. For example, some respondents indicate that they do not make use of devices to minimise security breaches. Considering that all respondents are connected to the Internet and deal with confidential data on a daily basis, they are taking a serious risk by not making use of any device. Hospitality SMMEs deal with confidential customer data that needs to be protected. Although these companies are aware that it is their responsibility to ensure that they monitor all external and internal distribution of paper work, and removal of media that contains client information, some companies however, still fail in this regard. This can have serious implications for the company should a breach occur as a result of this type of negligence.

5.2.2.1 Research sub-question 2 summary

Respondents appear to understand the importance of putting security measures in place to address security breaches. However, they tend to be slow to put this into practice. Information security policies can play an important role in addressing internal attacks but it appears that many hospitality SMMEs are not making use of this. Some of the respondents have policies in place but they do not enforce them, rendering them useless. In some instances, security policies are not properly distributed making them inaccessible to staff members. Even though passwords are commonly used by SMMEs, the majority of respondents fail to implement password policies. As a result, staff members might not know the details of password control. Virus attacks appear to be common amongst SMMEs but some respondents fail to update their anti-virus software on a regular basis. Unauthorised access which can also contribute to loss of information is not properly addressed. Respondents appear to understand the importance of keeping customer information secure as a majority of the respondents disclose that they have a procedure to make sure that customer information is kept secure. Customers are the reason why these companies are in business and therefore they cannot afford to expose their customer information.

5.2.3 Research sub-question 3-Information security training

This research question seeks to assist the researcher to investigate if hospitality SMMEs provide security training and if they do, what type of training is done. This research reveals that close to a third (section 4.3.2) of the respondents indicate that they do not provide security training to new employees.

To what extent is security training provided in the hospitality SMMEs?

By failing to provide security training to new employees, companies are putting themselves at risk. Companies that provide training to their staff members, help in internalising knowledge and skill so that employees take decisions that are in line with company objectives. Without training, employee mistakes will persist and some mistakes can be costly. It is known that fraudsters are becoming more sophisticated and poor training or the lack of it, can lead to security breaches that can cost companies dearly. Equipped with a security program, staff members will know their roles and be aware of their responsibilities and as a result, will assist IT personnel in minimising security breaches. This program can reduce losses as a result of intentional or accidental disclosure or modification of information.

A total of 69.6 percent (section 4.3.2) indicate that they do not have security awareness programs to help employees keep up with security developments. Knapp *et al.,* (2009:499) indicate that and awareness are intertwined when applied to security. The fact that most of these companies do not have awareness and training programs in place, results in security breaches and employee mistakes will persist. Considering that some respondents disclosed that their networks are regularly being tampered with, it therefore makes sense to provide training and awareness programs for staff members. This will equip them to effectively deal with attacks that may confront their companies.

It is revealed that spam mail is common amongst these companies. Training can help reducing security because it alerts employees to a number of issues. This includes information security, including spam mail. It is revealed that fraudsters make use of phishing which can be in the form of spam mail to trick users into revealing sensitive information. Employees will be able to differentiate between spam mail and legitimate mail if they are provided with suitable training.

5.2.3.1 Research sub-question 3 summary

Training appears to be alien to some hospitality SMMEs. Some respondents indicate that they do not provide training or induction to new employees. Considering that employees' mistakes are costing companies in monetary terms, it is of concern that some respondents indicate they do not provide training to new staff members. Security awareness programs can also assist companies to address security breaches as well as helping them to keep up with new security developments.

Hackers have become sophisticated and use various techniques such as social engineering to coerce users into revealing their log-in details. It is therefore, crucial to empower employees to ensure they do not fall into the trap of hackers. Trained staff members will understand how to deal with spam mail.

5.2.4 Research sub-question 4 customer protection in an online environment

This research question below is aimed at assisting the researcher to understand some of the procedures that have been put in place by hospitality SMMEs to ensure customer security.

What are hospitality SMMEs doing to protect customers in an online environment?

The results for this section are discussed in Chapter 4 (Section 4.3.3). Considering that SMMEs in the hospitality industry tend to deal with sensitive customer data, one would expect them to emphasise information security. It is evident that information security is not given the attention it deserves by hospitality SMMEs as significant number of respondents reveal that it is not emphasised in their company. As a result, this puts customers' data at risk. Where customer information is handled, measures should be put in place to minimise attacks to customer data

Even though most respondents disclose that they ensure customer privacy whenever they conduct online business a lot still needs to be done. Some respondents reveal that they do not guarantee customer privacy whenever they do business with them as a result putting the customer's information at risk. Some of the respondents disclose that it is not their responsibility to monitor customer data whenever they do business with them. This can have a negative impact on the company especially if a breach occurs as a result of negligence. It is evident from this research that SMMEs understand the importance of keeping client information secure, as the majority of the respondents indicate that they keep credit card information secure.

On the other hand, a majority of the respondents reveal that they do not have any strict regulations to monitor the distribution of material that contains client information. This puts clients' information at risk because their information is not being monitored. Should clients notice that their information is not being kept secure, the company is likely to lose customers and its reputation could be at stake. Lawsuits could even incur from affected clients (Tuyikize & Pottas, 2010:166).

Sometimes it might take time for companies to recover from such loss especially SMMEs. SMMEs appear to be unaware of the repercussions of failing to keep customer data secure as more than one third (section 4.3.3) of the respondents indicate that they do not guarantee privacy against unauthorised access to media containing client information.

Some respondents indicate that they do not carry out any weakness assessments in their networks. Risk assessment can help hospitality SMMEs avert breaches. It is evident that Cape Town hospitality SMME's risk assessment is too low (28.6 percent) compared to UK SMEs, where 75 per cent of respondents carry out risk assessments (PricewaterhouseCoopers, 2010:4). This shows that Cape Town SMMEs are lagging when it comes to the implementation of weakness assessment procedure. It appears these local companies apply a wait and see approach, waiting for incidents to take place before acting.

5.2.4.1 Research sub-question 4 summary

It is found that SMMEs understand the importance of keeping customer data secure. The majority of respondents reveal that they keep customer information secure. Even though, they indicated that they keep customer data secure, their actions reveal the opposite. Keeping customer information secure should include all the devices that contain client information and it should be a priority.

5.2.5 Research sub-question 5-Credit card fraud

This section summarises answering research sub question 5. As discussed in Chapter 4 (section 4.4.1), interviews were conducted to collect data to answer the research question stated below.

How is credit card dealt with in hospitality SMMEs?

For ethical reasons the names of SMMEs are not revealed. Considering that hospitality SMMEs are expected to make use of online business to cater for their clients, they are expected to keep client information secure. Credit card payment transactions are essential in the hospitality industry. It is therefore important for hospitality SMMEs to put measures in place to make sure that their security is not compromised. That being the case, SMMEs appear not to be heeding this call. The manager of SMME 3 argues that because they are a small company, they do not see the need to allocate large amounts of money to maintain security, let alone having a budget for this.

Only two SMMEs (SMME1 and 4) show dedication to addressing security breaches as they provide budgets for their security demands. By failing to provide sufficient budget for security needs, these SMMEs will be putting their customers' information at risk because they will not be able to put the necessary measures in place. This concurs with Ragan (2009) who revealed that customers' confidential information is under threat because hospitality companies rely on outdated processing systems. Hospitality SMEs lack of budget for security related issues will make them vulnerable to attacks because they will put minimal security applications in place. Hospitality companies tend to lose data stored in their systems because of unauthorised access.

A study by GFK[1] reveals that SMMEs tend to spend more cash on coffee and tea for their staff members, than on information security (Goodwill, 2012). Despite admitting that they deal with sensitive information, they still fail to provide a sufficient budget to address their security demands. Their reasoning being that security is not their concern since they are tourism companies. Both SMMEs (1 and 4), rely on external companies (as consultants) to deal with their security needs. However, SMME 1 is the only company that hires a network administrator on a permanent basis to address security breaches. The other three rely solely on consultants to provide information security issues.

> "I personally believe that it is useless for small companies to send employees to training and end up losing them to big companies. Big companies are always waiting to pounce and we can't compete with them in terms of salaries".

The above quotation indicates that SMME 3 does not intend to provide training for staff members to enlighten them about possible credit card fraud. This would affect their business and the industry at large. Employees will also understand how to avoid credit card fraud if they are provided with training. Training can also equip the staff members to know what to do when handling customer's sensitive information

5.2.5.1 Research sub-question 5 summary

The study reveals that companies that provide budgets for information security are capable of addressing data breaches much better. None of the companies that indicated that they have budget was a victim of serious data breaches. Most of them were able to curb the breaches before they took place. On the other hand, SMME 3 that did not budget for information security had one of their computers crash, as a result of virus attacks.

[1]A Global Research Company (Goodwill, 2011)

The SMMEs admit that they deal with sensitive client information, but they fail to maintain a sufficient budget to take care of their security needs. Relying on external consultants can be costly. In addition, there is a risk especially if they come into contact with confidential data. It is advisable to sign confidentiality agreement with these companies so that they will be aware of the repercussions. The companies still rely on outdated ways of storing data making use of external hard drives as back-ups.

SMMEs that lack information security policies, are also making themselves vulnerable to both employee mistakes and internal attacks because employees do not have documentation to refer to, when dealing with credit card fraud. Their lack of security policies can expose their client information. Even password security policies can assist SMMEs to reduce unauthorised access which can lead to credit card fraud. Considering that passwords are used to authenticate users onto systems, users must be well informed how to keep them secure. This is to avoid unauthorised personnel accessing customer data such as credit card information. Firewalls should also be maintained and updated at all times to hamper intruders from accessing sensitive information. SMMEs could hire IT experts on a more permanent basis to make sure that they take care of their networks and systems. Such a person can also conduct risk assessments to check the vulnerability of their networks. Virus attacks appear to be an issue for most SMMEs. The SMMEs questioned appeared to be reluctant to send staff members for training. Training can provide employees with the necessary knowledge to understand how to avoid credit card fraud

5.3 PROPOSING THE GUIDELINES

These guidelines reflect the outcome of this research specifically pertaining to SMMEs in the hospitality industry. Although not verified, many of these guidelines could apply to other industries as well or at least, be used as a starting point.

5.3.1 Necessity for policy adoption and enforcement

Information security policies should be implemented so that employees can have some documentation to refer to whenever they are handling sensitive data. Once policies are in place, they need to be enforced in order to be effective. It is senseless having policies and then failing to enforce them. This, in the light of the fact that that some respondents admit that they have information security policies but they fail to enforce them. Some respondents indicate that they do not even have password policies, despite passwords and usernames being the most common forms of authentication, amongst others. Another group indicated that policies are not even accessible to end-users.

5.3.2 Provision of training and awareness programs

Training is important in addressing information security problems. Training would enable SMMEs to influence their staff members and thereby alerting them, to issues pertaining to information security. Training and awareness drives are important in information security and are linked to some extent. Training will internalize knowledge and skill to enable employees to make decisions that are consistent with the company's goals. Considering that training is not common amongst hospitality SMMEs, a staff members' way of doing things may not be consistent with the company's objectives.

While employee awareness has been cited as one of the biggest challenges achieving the goals of information security, SMMEs can make use of training to make them aware of security challenges. Considering that new security breaches are emerging regularly, one of the easiest ways of averting them is the introduction of training and awareness programs to equip staff members to effectively address these breaches. However, information security training and awareness may never be totally sufficient considering the rapid change of technology. Training can also assist employees to avoid accidental mistakes that can be costly because it has been shown that some internal breaches might occur as a result of mistakes.

5.3.3 Governance of information security

One way in which SMMEs can improve their security compliance is through governance. Governance of information security can help SMMEs cope with data breaches because they would accept it as an integral part of information security management. Information security can be regarded as corporate governance which involves controlling a set of rules, policies and procedures. Considering that respondents are all connected to the Internet, risks are always emerging. Information security governance can therefore help create a wide range of policies and procedures pertaining to the use of IT resources by staff members. Information security governance will help SMMEs understand that information security needs a holistic approach and not to only put technology in place and hope for the best. Worse still, some of the respondents do not even update their technology making themselves easy targets. By adopting governance, hospitality SMMEs will come up with procedures and policies that will protect the customer's data both in the online and offline environment. It is found that governance minimises security breaches. SMMEs failing to establish adequate governance in an online environment could most likely result in an infective process, leading to diminished organisational security.

5.3.4 Mitigating both internal and external breaches

Both inside and outside threats have the capability to cause harm to a company's information system resources. Previous studies reveal that insiders pose more threat than outsiders, but outsider threats should not be underestimated. SMMEs must address both internal and external attacks to effectively protect their information. Thus, they must ensure secure transactions. While insiders can easily execute their attacks without being noticed, outsiders spend most of their time trying to find loopholes in networks to execute their attacks. Insiders have the advantage over outsiders by having direct access to information. Outsiders must first gain access to a company's system, while an insider can just target information directly without any barriers to overcome. It is found insider threats are mostly carried out by disgruntled employees who are embarking on revenge missions. Malicious staff members are financially motivated to steal information, especially customer data, in the hospitality industry. It is important to indicate that some internal breaches might be as a result of mistakes by staff members. However, some of these mistakes can be costly to a company.

Table 5.1 is structured to summarise the guidelines that can be used by SMMEs to address security breaches

Table 5.1: Information security guidelines for SMMEs

Table 5.1: Information security guideline	Necessity for policy adoption and implementation	Provision of training and awareness programs	Governance of information security	Mitigating both internal and external breaches
	• Policies instill policy procedures in the minds of employees • They can help curb internal attacks. • Can help SMMEs curb internal abuse, misuse or destruction of the company's resources. • Policies must be enforced to be effective. • If security policies are not enforced, employees will not strive to satisfy what has been stated in the policy. • A policy that is not enforced is like a useless document. • By enforcing security policies, SMMEs will fend off potential abuse especially if offenders are punished or sanctioned.	• Training can help SMMEs address security problems. • Training equips and alerts staff members to be proactive when dealing with sensitive information. • Training can help staff members internalize knowledge and skill and as a result, make decisions that are in line with the company's objectives. • Training will prepare staff members to accept security concepts easily. • Training and awareness programs can help staff members to become aware of security developments. • Training can also help minimize accidental breaches by staff members.	• Governance can also help SMMEs comply with security procedures. • Governance is important because SMMEs will be able to take information security management as an integral part of their daily activities. • Through information security governance a wide range of policies and procedures pertaining to the use of IT resources by staff members will be created to ensure secure transactions. • Governance could assist help SMMEs come up with procedures and policies that will protect the customer data.	• Both insider and outsider attacks have the capability to cause harm to the company's information resources. • SMMEs must address both internal and outsider attacks to protect information as well as ensure secure transactions. • It is easy for insiders to execute their attacks while outsiders must first gain access into the company's network or information systems. • In most cases, insiders consist of disgruntled staff members embarking on revenge missions or who are financially motivated to steal information.

5.4 CONCLUSION

In this chapter, the researcher discusses findings from the previous chapters and discusses this in relation to the research sub questions. The guidelines are discussed and summarised in a table to provide assistance to SMMEs in an effort to cope with online transactions.

In the next chapter the researcher presents the conclusion. SMMEs will be advised how they can make use of the model that has been adopted to address their security challenges.

CHAPTER SIX
CONCLUSION AND RECOMMENDATIONS

6.1 INTRODUCTION

This chapter covers conclusions and recommendations of this research. Furthermore, this chapter endeavors to demonstrate that the research problem is satisfactorily addressed. To effectively answer the research problem and the research questions both Quantitative and Qualitative research methods were used. The research question and sub-questions are also stated for completeness. The conclusions of both chapters (4 and 5) are revisited to present a more focused and comprehensive conclusion. Thereafter, recommendations are given and future research proposed.

6.2 RESEARCH PROBLEM

The research problem formulated in Chapter 1 for this research is:

"*SMMEs within the hospitality industry do not have sufficient procedures to protect their information as well as customer information in an online environment*".

The findings of this research ascertain that SMMEs in the hospitality industry are lagging in using information security applications. The literature reveals that SMMEs generally do not have policies in place to enforce information security. In some developed countries regular studies are conducted to determine the extent to which SMEs emphasize information security. This type of action would assist South African SMMEs in future

6.2.1 Research question and sub questions

The research question used in this study in order to address the research problem reads:

"What policies and measures do SMMEs use to protect their information as well as ensuring adequate customer information protection in an online environment?"

It is evident from the literature review that SMMEs tend to underestimate the impact of information security breaches. The empirical data indicates that SMMEs in Cape Town, do not make use of information security policies as a means to guard against security breaches. From the empirical work it is also noted that SMMEs in Cape Town face several challenges when it comes to information security, discussed in Section 4.4. Hospitality SMMEs deal with confidential customer information such as credit card data that needs protection.

As stated in Chapter 1, the research sub questions are:

What are the trends of online security locally and internationally?

- What policies and measures are in place for businesses to ensure customer security when conducting online business?
- To what extent is security training provided in the hospitality SMMEs?
- What are hospitality SMMEs doing to protect customers in an online environment?
- How is credit card fraud dealt with in hospitality SMMEs?

6.3 CONCLUSION

Research sub question one is addressed using the literature review in Chapter 2. Empirical data in the form of survey and interviews is used to collect data to address research sub question two to five. More importantly, research sub question two, three and four are addressed using a survey while interviews are used to address research sub-question five.

Information security has escalated over the years. Previously, computers were physically large and only one person worked per machine and therefore the system was easy to protect physically as well as the information contained in it. Restricting physical access to the computer room was often sufficient to protect information. The communication age has come with many challenges as computers are connected to each other via telecommunications lines. Companies now have to ensure that their networks are well maintained to ensure error-free and smooth transactions. There is an essential need to protect internal as well as customer information. Many challenges have since emerged as a result of increasing Internet connections. For example, hackers have become sophisticated and credit card fraud is rife.

Some of the trends that have emerged are:

- Focal areas in information security
- Secure Networks Protocols
- Risk analysis

The conclusion reached for research sub-question 2 dealing with policies and measures, is of paramount importance in curbing breaches and instilling a culture that is security abiding. SMME's lack of policies does not only make them vulnerable to attacks, but can also result in financial loss. Technology alone cannot provide sufficient protection as some respondents believe. Some respondents admit that they have been victims of internal attacks, and these attacks cannot only be addressed through technological measures. In some instances respondents possess information security policies but fail to enforce them. Despite experiencing virus attacks, SMMEs still fail to implement information security policies that will inculcate information security amongst the staff members who are chief culprits when it comes to spreading viruses.

Where information security policies are not enforced, security breaches will persist especially as a result of employee action. Considering that respondents rely on consultants for their information security needs, information security policies can help enforce information security with regard to the staff members as well as the consultants. While respondents' preferred form of authentication is by using passwords and usernames, password policies were not formulated to guide users, giving them guidelines for password usage. Lack of password policy can make it easy for outsiders to gain access into company networks and steal data that is valuable. Despite the fact that cyber-attacks are on the rise, SMMEs seem to be slow to sensitize employees about the effects of data breaches. SMMEs cannot afford to lose customer data as a result of negligence.

The conclusion reached for sub-question 3 dealing with training, finds that despite considering training as an important aspect in averting security breaches, SMMEs appear to be reluctant to provide staff training. SMMEs goals of trying to avoid breaches will never succeed if staff members are not provided with information security training. Considering that SMMEs rely on limited finances, these companies must send their staff members to short courses to update them on security issues. In some cases SMMEs fail to provide training for new staff members, as a result exposing themselves because new staff members need some form of induction to make them aware of what is expected from them. Without training security awareness will not be enhanced and mistakes will persist.

Some mistakes as a result of insiders can be costly. Respondents seem to lack having awareness programs which makes them vulnerable to attacks. This is due to staff members not being provided with necessary programs to make them aware of breaches experienced by hospitality companies.

The conclusion reached for research sub-question 4 dealing with online protection, finds that although SMMEs indicate that they ensure customer privacy whenever they conduct online business with them, their actions are not supportive of this. Most of the respondents did not provide training to staff members to make them aware of some of the new breaches that are taking place. The respondents were all connected to the Internet and therefore it is important for them to be vigilant about online breaches. Customers are central to the success of the SMMEs and therefore they cannot afford to be negligent when dealing with customers. Hospitality SMMEs deal with sensitive customer data in most cases and should institute necessary measures to protect it.

Lastly the conclusion reached for research sub-question 5 dealing with credit card fraud is presented. Hospitality SMMEs being connected to the Internet are also exposing themselves to credit card fraud. It is therefore important for hospitality SMMEs to put measures in place to avert credit card fraud. SMMEs understand the implications of credit card fraud and indicate that they ensure credit card security. The respondents did not have a dedicated IT or information security specialist to deal with such fraud save for one company. While information security is not their main goal, their networks should be guarded to avoid credit card fraud. Considering that credit card fraud can be a result of internal attacks as well, SMMEs must be wary of internal attacks. While none of the SMMEs has been a victim of credit card fraud, they must put measures in place to curb this. Similarly to research sub question three, staff members need training to be aware of security breaches due to credit card fraud.

6.4 RECOMMENDATIONS

While some recommendations have been dealt with as part of the guidelines (section 5.3), these are expanded in this section. It has been indicated that there are always new security attacks emerging and in order for SMMEs to avoid being victims, they should hire specialists` (or have access to specialists) that could address these problems. By hiring specialists, SMMEs will be able to address security breaches as soon as they take place therefore avoiding breaches that could be more costly. If SMMEs do not have qualified technicians, they could outsource training to a consultant.

Contracts must be signed between the two companies clarifying how they are going to deal with information security. Programs such as SETA (Security Education, Training and Awareness) can assist SMMEs to instill security awareness in the minds of employees. These programs can help make employees aware of their responsibilities in terms of security. Considering that these companies rely on limited budgets, staff members can be sent for short courses so as to sensitize them with some security developments.

Managers and end-users are important to information security. It is important for a dialogue to exist between managers and users. It is also advisable that information security is addressed at three levels: during recruitment, employment and when the contract is terminated. When a new employee is hired, the SMME manager must explain what is expected from the new employee and a thorough induction must be conducted so that he or she can know what to do when handling personal data. In the same breath, if an employee leaves a company for a specific reason, SMMEs should make that particular employee sign a non-disclosure agreement.

SMMEs that are connected to the Internet will always be under threat of being attacked by intruders. Security breaches are on the rise and SMMEs are not immune to these cyber threats. Some SMMEs indicated that there are regular attempts to breach their networks. In one incident, one of the employees managed to bypass the firewall of the SMME to download files from the Internet. In order to avoid these breaches, SMMEs should make use of intrusion detection systems as well as hire IT personnel on a full time basis. This program notifies the administrator if there is any interference in the network. Anti-viruses should also be updated on a regular basis so that they can keep up with the latest developments regarding viruses.

Considering that SMMEs mostly rely on consultants to monitor and ensure secure networks, they should make use of security standards such as ISO 27001 so that they can meet the minimum security demands in the hospitality industry. Considering that each company's security requirements are different, SMMEs will be committing a serious mistake if they are only going to rely on consultants for their security demands. By failing to make use of these security standards, SMMEs will not know whether their security practices meet the minimum standards. Considering that these companies deal with confidential information, their security policies should mainly concentrate on non-disclosure agreement. Without information security policies, staff members will not know what the company's goals are in terms of information security.

Information security policies act as rules relating to access of resources and information such as systems and applications and therefore can act as a deterrent to breaches by insiders. It is important for policies to be visible and understandable to employees. SMMEs should avoid copying policies from the Internet and pasting them onto their notice boards. Every company has a different way of doing business and its policies should reflect this. Policies should take into consideration the roles and responsibilities of users and indicate that all staff members are expected to sign a confidentiality agreement. A password policy should be emphasized in SMMEs because this will enforce employees to be aware of how often they need to change passwords, as well as the number of characters that is needed to form an effective password. They will also be aware that they cannot use sequential letters or numbers. They will also be advised about the consequences of sharing passwords and using the same password twice. SMMEs systems should regulate the number of times that a person can log on so that fraudulent people cannot try the password several times.

6.4 FUTURE RESEARCH

Information security in the hospitality industry is still in its early stages especially when it comes to SMMEs. Further studies should be conducted to determine the preparedness of SMMEs in South Africa. The following research areas could be conducted in the future:

- A full assessment of barriers to information security in the hospitality industry with a reference to SMMEs.
- A comparative study to determine how SMMEs in the hospitality industry perform in comparison with SMMEs from other industries in terms of information security.
- A thorough study to quantify financial losses in SMMEs as a result of information security breaches.

REFERENCES

Abraham, S. & Chengalur-Smith, I. 2010. An overview of social engineering malware: Trends, tactics and implications. *Technology in Society,* 32(2010):183-196.

Acquisti, A., Friedman, A. & Telang, R. 2006. Is there a cost to privacy breaches? An event study.*Proceedings of the International conference of Information Systems (ICIS)*.Milwaukee, Wisconsin, 10 -13 December.

Alifri, H.A., Pons, A. & Collins, D. 2003. Global e-commerce: a framework for understanding and overcoming the trust barrier. *Information Management and Computer Security,* 11(3):130-138.

Allan, G. 2003. A critique of using grounded theory as a research method. *Electronic Journal of Business Research Methods*, 2(1):1-10.

Allam, S. & Flowerday, S. 2010. A model to measure the maturity of smart phone security at software consultancies.*Proceedings of the South African Information Security Multi Conference*. Port Elizabeth, 17-18 May.

Alreck, P. L. & Settle, R.B. 1985.*The Survey research handbook*. Illinois: Irwin.

Ashenden, D. 2008. Information security management: A human challenge? Information security technical report, 13(4):195-201.

Ayyagari, M., Beck, T. & Dermiguc-Kunt, A. 2007.Small and medium enterprises across the globe.*Small business economics*, 29 (4):415-434.

Babbie, E. & Mouton, J. 2001.*The practice of social research*. Cape Town: Oxford University Press.

Bagchi, K. & Udo, G. 2003. An analysis of growth of computer and Internet breaches. *Communications of the associations for information systems*, 12(2003):684-700.

Bahmanziari, T., Odom, M.T. & Ugrin, J.C. 2009.An experimental evaluation of the effects of internal and external e-Assurance on initial trust formation in B2C e-Commerce. *International journal of accounting information systems*, 10(2009):152-170.

Barker, K. J., D'Almato, J. & Sheridon, P. 2008. Credit card fraud: awareness and prevention. *Journal of financial crime*, 15(4):398-410.

Barlette, Y., & Formin, V.V. 2008. Exploring the suitability of IS security management standards for SMEs. *Proceedings of the 41st Hawaii International Conference on Systems Sciences.* Waikoloa, Big Island. 7- 10 January. Hawaii.

Baskerville, R. & Siponen, M. 2002.An information meta-policy for emergent organisations. *Logistics and information management,* 15(5):337-446.

Bauer, J. & Van Eeeten, M. 2009. Cybersecurity: Stakeholder incentives, externalities and policy options. *Telecommunications policy,* 33(10):706-719.

Beachboard, J., Cole, A., Mellor, Hernandez, S. & Aytes, K. 2008. Improving information security risk analysis, practices for small and Medium sized enterprises: A research agenda. *Informing science and information technology*, 5(2008):73-85.

Bedi, D.S. & Warden, S. 2009. Web security in hospitality SMMEs: investigating policies and measures in the Cape Metropole area. *Proceedings of the 11th Annual World Wide Web Applications*. Port Elizabeth: 2-4 September.

Bedi, D. S. & Warden, S. 2010. Web security in the hospitality SMMEs: Investigating policies and measures in the Cape Metropole area. *Proceedings of the South African Information Security Multi Conference*. Port Elizabeth: 17-18 May.

Bella, G. & Bistarelli, S. 2005.Information assurance for security protocols.*Computers and security*. 24(4):322-333, June.

Beranek, L. 2010. Risk analysis methodology used in small and medium enterprises in the Czech Republic. *Information management and computer security*, 19(1):42-52.

Berezina, K., Cobanoglu, C., Miller, B.L., & Kwansa, F. 2012. The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word of mouth. International journal of contemporary hospitality management, 24(7):991-1010.

Bernard, R. 2007. Information lifecycle security assessment: A tool for closing security gaps. *Computers and security,* 26(1):26-30.

Berry, A., Von Blotnitz, M., Cassim, R., Kesper, A., Rajaratnan, B., & Van Seventer, D.E. 2002.The economics of SMMEs in South Africa.http://www.edgegrowth.com/Portals/0/Documents/Seminal%20Docs/THE%20ECONOMICS%20OF%20SMMES%20IN%20SOUTH%20AFRICA.pdf [12 July 2008].

Bharadwaj, P.N. & Soni, R.G. 2007. E-commerce usage and perception of e-commerce issues among small firms: results and implications from an empirical study. *Journal of small business management*, 45(4):501-521.

Birley, G. & Moreland, N. 1999.*A practical guide to Academic Research*. London: Kogan Page Limited.

Bojanc, R. & Jerman-Blazic, B. 2008.Towards a standard approach for quantifying ICT security investment. *Computer standards and interfaces,* 30(4):216-222, May.

Bougaardt, G. & Kyobe, M. 2011.Investigating the factors inhibiting SMEs from recognising and measuring losses from cyber-crime in South Africa. Electronic journal of information systems evaluation, 14(2):167-178.

Bryce, J. & Klang, M. 2009. Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information security technical report*, 14(2009):160-166.

Burdon, M., Lane, B. & Von Nessen, P. 2010. The mandatory notification of data breaches: Issues arising for Australian and EU legal developments. *Computer law and security review*, 26(2010):115-129.

Burns.A,, Davies AJ. & Beynon-Davies P. 2006. A study of the uptake of information security policies by small and medium sized businesses in Wales; *In: ICEB & eBRF 2006 conference*, Tampere, Finland, November 28–December 2.

Calder, A. 2005.*A business guide to Information Security: how to protect your company's IT assets, reduce risks and understand the law*. 2nd ed. London: Kogan Page Limited.

Campbell, K. Gordon., L.A. Loeb, M. P. & Zhou, L. 2003. The economic cost of publicly announced security breaches: empirical evidence from the stock market. *Journal of computer security*, 11(3):431-448.

Caralli, A. W. & Wilson, R. W. 2004. The challenges of information security: Survival enterprise management team. www.cert.org/archive/pdf/ESMchallenges.pdf [20 March 2007].

Carron, M.P., Lund-Thompsen, P. Chan, A. Muro, A. & Bhushan, C. 2006. Critical perspectives on CSR development: what we know, what we don't know, and what we need to know. *International affairs*, 82(5):977-987.

Cavusoglu, H., Mishra. B. & Raghunathan, S. 2004. The effect of Internet security breach announcement on Market Value: Capital market reactions for breached firms and internet security Developers. *International journal of electronic commerce*, 9(1):69-104.

Chang, E.C. & Lin, C.S.2007.Exploring organisational culture for information security management.*Industrial management and data systems,* 107(3):438-458.

Chang, E.S., & Ho, C.B. 2006. Organisational factors to the effectiveness of implementing information security management. *Industrial management and data systems,* 106(3):345-361.

Chau, S. 2003. The use of ecommerce amongst thirty four Australian SME: An experiment of strategic business too. *Journal of systems and information,* 7(1): 46-66.

Chiang, T.C. & Huang, Y.M. 2003.Group keys and the multicast security in Ad Hoc networks.Proceedings of the 2003 International Conference on Parallel Processing Workshops. Kaohsiung, 06 -09 October. Taiwan.

Choo, K.R. 2010.High tech criminal threats to the national security infrastructure. Information security technical report, 15(2010):104-11.

Clear, F. 2007. SMEs electronically-mediated working and data security: cause for concern? *International journal of business science and applied management,* 2(2):1-19.

Cobanoglu, C. & DeMico, F.J. 2007. To be secure or not to be: Isn't this the question? A critical look at hotel's network security: *International journal of hospitality and tourism administration*, 8 (1):43-55.

Coertze, J., Van Niekerk, J. & Von Solms R. 2011. A web based information security governance toolbox for Small-to-medium Enterprises in Southern Africa.*Proceedings of the 10th Information Security South Africa (ISSA) Conference*. Johannesburg: South Africa. 15-17 August.

Colwill, C. 2010. Human factors in information security: The insider threat-who can you trust these days? Information security technical report, 14(4):186-196.

Comptia. 2012. Employee empowering technologies raise security stakes for organisations. http://www.comptia.org/news/pressreleases/12-11-14/Employee-Empowering_Technologies_Raise_Security_Stakes_for_Organizations_New_CompTIA_Study_Reveals.aspx [12 December 2013].

Creswell. W. J. 2003. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. 2nd Ed. California: Sage Publications.

Creswell, W. J. 2009. Research *Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 3rd Ed. California: Sage Publications.

Dallago, B. 2004.The importance of SMEs in transitional economies.http://www.humancapitalinstitute.org/hci/tracks_small_medium_enterprises.guid?_currentTab=_researchTab [09 September 2008].

Damanpour, F. & Madison, J. 2001.e-Business e-Commerce Evolution: Perspective and strategy. *Managerial finance*, 27 (7);16-33.

Desouki, H. & Amstrong, H. 2010. Security and quality issues in IT projects. *Proceedings of the South African Multi Conference*. Port Elizabeth, 7- 8 May.

De Vos, A.S., Strydom, H., Fouche, C.B. & Delport, CSL. 2005. *Research at grass roots for the social sciences and human service professions.* Pretoria: Van Schaik Publishers.

Dhillon, G. 2001. Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and security,* 20(2):165-172, April.

Dimopoulos, V., Furnel, S.M., Jennex, I. & Kritharas, I. 2005. Approaches to IT security in Small and medium enterprises. *Proceedings of the 2nd Australian information security management conference*, Perth. Australia.

Dlamini, M.T., Eloff, J.H.P. & Eloff,M.M. 2009. Information security: the moving target. *Computer security*, 28(2009):189-198.

Doherty, N.F., Anastasakis, L. & Fulford, H. 2010.Reinforcing the security of corporate resources: A critical review of the role of the acceptable use policy.*International journal of information management*, 31(3):201-209.

Doherty, N.F & Ellis-Chadwick, F.E. 2009.Exploring the drivers, scope and perceived success of e-commerce strategies in the UK retail sector. *European Journal of Marketing*, 43 (9-10):1246-62.

Doherty, N.F. & Fulford, H. Aligning the information security policy with the strategic information systems plan.*Computer and security*, 25(1):55-63, February.

Dojkovski, S., Lichstein, S. & Warren, M. 2007. Developing information security culture in Small and Medium size Enterprises. *Proceedings of the 6th European Conference on information Warfare and Security*, Shrivenham, 2-3 July 2007.Defence College of Management and Technology.

Drew, S. 2003. Strategic use of e-Commerce by SMEs in the east of England.*European management journal,* 21(1):71-88 February.

Driscoll, D.L., Appiah-Yeboah, Salib, & Rupert, 2011. Merging qualitative and Quantitative Data in Mixed Methods Research: How to and Why Not. *Ecological and environmental anthropology*, 3(1):19-28.

Duggan, G.B., Johnson, H. & Grawemeyer, B. 2012. Rational security: Modeling everyday password use. *International journal of human-computer studies*, 70(6):415-431.

Dunn, D.S. 2010. The Practical Researcher: A student guide to conducting psychological research. 2nd Ed. West Sussex: Wiley Blackwell.

Dynes, S., Brechbuhl, H. & Johnson, E. M (2005). Information security in the extended enterprise: Some initial results from the field study of an industrial firm http://mba.tuck.dartmouth.edu/digital/Research/AcademicPublications/InfoSecurity.pdf [24 September 2008].

Elliot, C. 2010. To what extent are they a threat to information security? *Information security technical repor*t, 15(2010):79-103.

EMW. South Africa. 2005. Cost Effective, Secure, Internet Access Control and Reporting for the SME. http://www.itweb.co.za/office/emw/0506090933.htm [13 April 2007].

Federal Reserve Bank of Philadelphia.2006. http://www.phil.frb.org/payment-cards-center/events/conferences/2007/C2006SeptInfoSecuritySummary.pdf [10 October 2008].

Feng, N., Wang, H.J. & Li, M. 2014. A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, 256(2014):57-73.

Ferguson, C., Fin, F., Hall, J. & Pinnuck, M. 2010.The long and the short of IT. International journal of accounting systems, 11(2):79-104.

Ferguson, T. 2007. Staff blamed for security breaches; but is it a matter of policy? http://management.silicon.com/smedirector/0,39024679,39168237,00.htm [10 October 2009].

Fillis, I., Johannson, U. & Wagner,B. 2004. Factors impacting on e-Business adoption and development in the smaller firm.*International journal of entrepreneurial behaviour and research*. 10(3):178-191.

Fisher-French, M. 2011. EasyPay fights back after fraud. *Mail and Guardian*, 11-16 November.

Flick, U. 2011.Introducing Research Methodology.2nd Ed. Sage Publications. California.

Flink, F. 2002. Who holds the key to IT security? *Information security technical report*, 7(4):10-22.

Flowerday, S. & Von Solms, R. 2005. Real time information integrity = systems integrity +data integrity + continuous assurances. *Computers and security*, 24(8):604-613, October.

Fulford, H. & Doherty, N.F. 2003. The application of information security policies in UK based organisations: an exploratory investigation. *Information management and computer security,* 11(3):106-114.

Furnell, S. & Thomson, K. L. 2009. Recognising and addressing security fatigue. *Computer fraud and security*, 2009(11):7-11.

Futcher, L., Schroder, C. 2010. Information security education in South Africa. *Information management and computer security*, 18(5): 214-229.

Fyffe, G. 2008. Addressing the insider threat. *Network security*, 2008(3):11-14.

Garg, A., Curtis, J. & Halper, H. 2003. Quantifying the financial impact of IT security breaches. *Information management and computer security,* 11(2):74-83.

George, R. 2010. Visitors' perceptions of crime safety and attitude towards risk: The case of Table Mountain National Park, Cape Town. *Tourism Management*, 31(2010):806-815.

Gerber, M. & Von Solms, R. 2001. From risk analysis to security requirements. *Computers and security*, 20(7):577-584, October.

Gerber, M., Von Solms, R. & Overbeek, P. 2001. Formalizing information security requirements. *Information management and computer security,* 9(1):32-37.

Gerber, M. &von Solms, R. 2008. Information security requirements - Interpreting the legal aspects. *Computers & Security, 27*(6):124-135.

Goh, R. 2003. Importance of information security: The importance of the human element. Unpublished dissertation, Preston University: Singapore.

Gordon, G. 2011. Online boom set boost SA commerce. *Sunday Times*:30, August 7.

Goucher, W. 2011. Do SMEs have the right attitude to security? *Computer fraud and security*: 18-20.

Gravetter, F.J. & Forzano, L.B. 2006. Research Methods for the Behavioural Sciences. 3rd Ed. Wadsworth Cenage Learning. Belmont, USA.

Gupta, A & Hammond, R. 2005. Information systems security issues and decisions for small businesses. *Information management and computer security,* 13 (4):297-310.

Haasbroek, J. D. 2013. Credit card fraud in restaurants. http://eatout.co.za/News/2619/Credit-card-fraud-in-restaurants. [02 August 2013].

Helokunnas, T. & Ilvonen, I. 2003. Information security culture in small and medium size enterprises. http://www.ebrc.info/kuvat/2034.pdf [20 March 2009].

Hoinville, G. & Jowell,R. 1982. Survey research practice.2nd ed. London:Heinnemann Educational Books Ltd.

Hone, K. & Eloff, J.H.P. 2002. What makes an Effective Information Security Policy. *Network Security*, 20(6):14-16.

Hong, K.S., Chi, Y.P., Chao, L.R. & Tang, J.S. 2006. An empirical study of information security on security elevation in Taiwan. *Information management and computer security,* 14(2):104-115.

Householder, A., Houle, K. & Dougherty, C. 2002. Computer attack trends challenge Internet Security. *Computer*, 35(4):5-7, April.

Huang, C.D., Hu, Q. & Behara, R.S. 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International journal of production economics*, 114(2008):793-804.

Hubbard, J. 2013. SMEs: Staff buy-in essential to SMEs security. http://finweek.com/2013/07/25/smes-staff-buy-in-essential-to-sme-security/. [06 August 2013].

Hutchinson, D. & Warren,M. 2003. Security for Internet banking: A framework. *Logistics information management*, 16(1):64-73.

Isomaki, H. & Bilozerov, O. 2011. Information security culture in Russian ICT small and medium sized enterprises. *Proceedings of IRIS 2011 Conference, Turku,* 16-19 August. University of Turku, Finland.

Ivankova, N.V., Cresswel, J.W. & Clark, V. L. *Designing and conducting mixed methods research*. Thousand Oaks: Sage.

Jamaluddin, N. 2013. Adoption of e-commerce practices amongst Indian farmers, a survey of Trichy District in in the state of Tamilnadu, India. *Procedia economics and finance,* 7(2013):140-149.

James, T.J., Khansa, L., Cook, D.F., Bruyaka, O. & Keeling, K.B. 2013. Using network based text analysis to analyze trends in Microsoft's security innovations. *Computers and security,* 36(2013):49-67.

Jha, S., Gullien, M. & Westland, J.C. 2012. Employing Transaction aggregation strategy to detect credit card fraud. *Expert systems with applications*, 39(2012):12650-12657.

Jirasek, V. 2012. Practical application of information security models*. Information security technical report*, 17(2012):1-8.

Johnston, D. A. & Wright, L. 2004. The e-business capability of small and medium sized firms in international supply chains. *Information systems and e-business management*, 2(2):223-240.

Kalla, M., Wong, J.S.K., Mikler, A.R. & Elbert, S. 1999. Achieving Non-repudiation of Web based transactions. *Journal of systems and software*, 48(1999):165-175, October.

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

Kelleher, D. 2009. SME security: SME mindset must change. http://www.scmagazineus.com/sme-security-sme-mindset-must-change/article/136052/ [21 June 2009]

Kesper, A. 2001. Failing or not aiming to grow? Manufacturing SMMEs and their contribution to employment growth in South Africa. *Urban forum*, 12(2):171-203.

Kim, H.S. Ahn, MH. Lee, G.S. & Lee, J. 2006. The information security guideline for SMEs in Korea. http://ww1.ucmss.com/books/LFS/CSREA2006/SAM3066.pdf [22 January 2009].

Kim.J., Chung, N. & Lee, C.K. 2011. The effects of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. *Tourism management*, 32(2011):256-265.

Kim, W.G. & Kim, J.K. 2004. Factors affecting online hotel reservation intention between online and non-online customers*. Hospitality management*, 23(2004):381-395.

Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs). *International journal of computer science and security*, 5(1): 9-29.

Knapp, K.J., Morris, F.R., Marshall, E.T. & Byrd, T. A.2009. Information security policy: An organisational level process model. *Computer security,* 28(2009):493-508.

Kortjan, N. & Von Solms, R. 2012. Fostering a cyber-security culture: A case of South Africa. *Proceedings of the 14th Annual Conference on World Wide Web applications*, Durban. 7-9 November 2012, Mangosuthu University of Technology.

Kovavich, G. 2001. Protecting 21st century information – its time for a change: *Computers and security*, 20(3):207-213.

Kraemar, S. Carayon, P. & Clem, J. 2009. Human and organisational factors in computer and information security: Pathways to vulnerabilities. *Computer and security*, 28(2009):509-520, April.

Kreicberga, L. 2010. Internal threat to information security – Countermeasures and human factor within SME. Unpublished Master Thesis, Lulea University of Technology.

Kritzinger, E. & Smith, E. 2008. Information security management: An information security retrieval and awareness model for industry. *Computers and security*, 27(2008):224-231.

Kruger, H.A. & Kearney, W.D. 2008. Consensus ranking – an ICT security awareness case study. *Computers and Security*, 27(7-8):254-259.

Kshetri, N. 2007. Barriers to e-commerce and competitive business models in developing countries: a case study. *Electronic commerce research and applications,* 6(2007):443-552.

Kuusisto, T. and Ilvonen, I. 2003. Information security culture in small and medium size enterprises. http://www.ebrc.info/kuvat/431-439.pdf *[05 March 2009].*

Kyobe, M. 2005. Addressing E-crime and computer security issues in homes and small organisations in South Africa. http://icsa.cs.up.ac.za/issa/2005/Proceedings/Poster/071_Article.pdf [17 March 2009].

Landwehr, C.L. 2001. Computer security. *International journal of information security,* 1(1):3-13.

Lange, T. Ottens, M. & Taylor, A. 2000. SMEs and barriers to skills development: a Scottish perspective. *Journal of European industrial training*, 24(1):5-11.

Lawson, R., Alcock, C., Cooper, J. & Burgess, L. 2003. Factors affecting electronic Commerce by SMEs: An Australian study. *Journal of small business and enterprise development,* 10 (3) 265-276.

Leach, J. 2003. Improving user security behaviour. *Computers and security,* 22(8):685-692, December.

Lee, Y. J., Kauffman, R. J., Sougstad, R. 2011. Profit maximizing firm investment in customer information security. Decision support systems, 51(2011):904:920.

Lee, W. S. & Jang, S.S. 2009. A study on information security management system model for small and medium enterprises. *Proceedings of the 11th WSEAS conference*. Timisora, Romania. 27-29 May.

Leedy, P. D,, Newby, T.J. & Ertmer, P.A. 1996. *Practical research planning and design.* Upper Saddle River, NJ: Merrill.

Leedy, P.D. 1997. *Practical research: Planning and design*. Upper Saddle River,NJ: Prentice Hall.

Le Vine, R. 2005. Technology evolution drives need for greater information security. *Computers and security*, 24(5):359-361, August.

Luzwick, P. 2001. If information warfare attacks are common, then evaluate the security policy. *Computer fraud and security*, 2001(9):16-19, September.

Lybaert, N. 1998. The information use in SMEs: its importance and some elements of influence. *Small business economics*, 10(2):171-191.

M2 Communications. 2005. Lack of document disposal policy puts SMEs at risk of corporate ID fraud. http://web.ebscohost.com/ehost/detail?vid=14&hid=12&sid=4e377a67-c37b-4439-ba98-e42882a78b63%40sessionmgr4&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=nfh&AN=16PU4246419902 [23 February 2009].

Maconachy, W.V. Corey, D. Schou, C.D. Ragsdale, D. & Welch, D. 2001. A model for information assurance: an integrated approach. *Proceedings of 2001 IEEE workshop on information assurance and security*, West Point, 5-6 June. New York: 306-310.

Mapheshoane, T.J. & Pather, S. 2012. Adoption of e-Commerce in typical developing country context: Lesotho tourism industry. *Proceedings of the 14th annual conference on World Wide Web applications.* Durban. 7-9 November.

Maree, K. & Pietersen, J, 2007. Sampling. In Maree,K. (ed). *First steps in research*. Pretoria: Van Schaik Publishers:171-181.

Maree, K. & Pietersen, J. 2007. Surveys and the use of questionnaires. In Maree, K. (ed*) First steps in research*. Pretoria: Van Schaik Publishers: 155-169.

Maree, K. & Pietersen,J. 2007. The quantitative research process. In Maree, K. (ed). *First steps in research.* Pretoria: Van Schaik Publishers:144-153.

Maree, K. & Van Der Weistheuizen. 2007. Planning a research proposal. In Maree, K. First steps in research. Pretoria: Van Schaik Publishers: 23-47.

Mashanda, P., Cloete, E. & Tanner, M. 2012. An analysis of factors affecting the adoption of business to consumer e-commerce in developing countries – a case of Zimbabwe. Proceedings of the 14th annual Conference on World Wide Web Applications. Durban. 7-9 November. Mangosuthu University of Technology

Maswera, T., Dawson, R. & Edwards, J. 2008. E-Commerce of travel and tourism organisations in South Africa, Kenya, Zimbabwe and Uganda. *Telematics and informatics.* 25(3):187-200.

Maswera, T., Edwards, J. & Dawson, R. 2008. Recommendation for e-commerce systems in the tourism industry of sub-Saharan Africa. *Telematics and informatics*: 26 (1):12-16 , February.

McBurney, D.H. & White, L. 2007. *Research methods*. 7th ed. Massachusetts: Thomson Wadsworth.

McKnight, W.L. 2002. What is information assurance? http://www.stsc.hill.af.mil/crosstalk/2002/07/mcknight.html [27 October 2009].

Millard, E. 2007. How vulnerable is your SME? http://www.processor.com/editorial/article.asp?article=articles/P2922/20p22/20p22.asp [22 November 2008].

Moertini, V. S. Small and Medium Enterprises: On utilizing Business-to-Business e-commerce to global. *Procedia economics and finance*, 4(2012):13-22.

Morgan, A., Colebourne, D. & Thomas, B. 2006. The development of ICT advisors for SME businesses: An innovative approach. *Technovation,* 26(8):980-998.

Morgan, B. 2004. 2010: Real benefits off the field. http://www.southafrica.info/2010/2010_wc_thoughts.htm [21 August 2007].

Morgan, R. 2006. Information Security for small businesses. http://www.infosecwriters.com/text_resources/pdf/Information_Security_for_Small_Businesses.pdf [20 July 2008].

Moreira, E.D.S.,, Martimiano, L.A.F., Brandao, A.J. & Bernandes, M.C. 2008. Ontologies for information security management and governance. *Information management and computer security*, 16(2):150 -165.

Moscaritolo, S. 2009. SME security: Sizeable differences. http://www.scmagazineus.com/sme-security-sizable-differences/article/136042/ [12 April 2009].

Mubarak, S. & Slay, J. Protecting clients from insider attack. *Information security technical report*, 14(2009)

Nakayama, Y. 2009. The impact of e-Commerce: It always benefits consumers, but may reduce social welfare. *Japan and the world economy*, 21(2009):239-247.

Navarro, L. 2001. Information security risks and managed security services, *Information security technical report*, 6(3):28-36, October.

Ngai, E.W.T & Wat, F.K.T. 2002. A literature review and classification of electronic commerce research. Information management, 39(5):415-429.

Nkwe, N. 2012. Role of SMEs in Botswana. American International Journal of contemporary research, 2(8):29-37.

Olivier, G.B. 2009. UK SMEs underestimate the danger posed by employees. http://www.gfi.com/blog/uk- [21 October 2009].

Olnes, J. 1994. Development of security policies. *Computers and security*, 13:628-636.

Onwubiko, C. & Lenaghan, A.P. 2007. Managing security threats and vulnerabilities for small to medium enterprises. *Proceedings of the of the 2007 IEEE International conference on Intelligence and Security Informatics*. New Brunswick, May 23-24. New Jersey.

Park, J. Y. Robles, J. R. Hong, C.H. Yeo, S.S. & Kim, T. 2008. IT security strategies for SMEs. *International journal of software engineering and its applications,* 2(3):91-98.

Pasante, L. 2008. Introduction to information security. http://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf [11 June 2013]

Petersen, L., Minkkinen, P. & Esbensen, K.M. 2005. Representative sampling for reliable data analysis: Theory of sampling. *Chemometrics and intelligent laboratory systems*, 77(2005):261-277.

Peterson, D., Meinert, D., Criswell, J. & Crossland, M. 2007. Consumer trust : privacy policies and third-party seals. *Journal of small business and enterprise development*. 14(4):654-669.

Posthumus, S & Von Solms, R. 2004. A framework for the governance of information security. *Computers and security,* 23 (8):638-646, October.

Pozzi, A. E-commerce as a stockpiling technology: implications for consumers. Kim, Lee & Ham, 2013:369, 31(2013):677-689.

Prabowo, H.Y. 2011. Building our defence against credit card fraud: A strategic view. Journal of money laundering, 14(4):371-386.

Pricewaterhousecoopers. 2010. Information security breaches survey 2010: Technical Report. http://www.pwc.co.uk/audit-assurance/publications/isbs-survey-2010.jhtml [10 January 2010].

Qian, Y., Fang, Y. & Gonzalez, J.S. 2012. Managing information security risk during new technology adoption. *Computers and security*, 31(2012):859-869.

Rachwald, R. 2011. Why are SMBs attractive to hackers?http://securitysa.com/article.aspx?pklarticle=7237[18January 2011].

Ragan, S. 2009. Security vulnerabilities persist in hospitality industry. http://www.thetechherald.com/articles/Security-vulnerabilities-persist-in-hospitality-industry/5987/ [20 January 2009].

Rao, S.S. 2000. E-Commerce: the medium is the mart. *New Library world*. 101(2):53-59.

Rezgui, Y. and Marks, A. (2008) Information security awareness in higher education: An exploratory study. *Computers & security*, 27(3):241-253

Riberio, D. 2012. Sophisticated security threats target SMEs. http://www.entrepreneurmag.co.za/advice/business-leadership/risk-management/sophisticated-security-threats-target-smes/ [11 June 2013).

Rhee, H.S., Kim, C.T. & Ryu. Y.U. 2009. Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & Security*, 28(8)-816-826.

Robinson, F. 2001. High end IT security: No longer a distant pipe dream for SMEs. Computer fraud and security, 6(2001):12-14.

Rosado, D.G., Gutierrez, E.F. & Piattini, M. 2006. Security patterns and requirements for internet based applications. *Internet research*,16(5):519-536.

Saleh, M.S. & Alfantook, A. 2011. A new comprehensive framework for enterprise information security risk management. *Applied computing and informatics,* 9(2)107:118.

Santarelli, E & D'Altri, S. 2003. The diffusion of e-Commerce amongst SMEs: Theoretical implications and empirical evidence. *Small business economics,* 21(3):273-283.

Sapa. 2012. Millions stolen in PostBank cyber hacking. *Cape Times*, January 16

Sarkar, K. 2010. Assessing insider threats to information security using technical behavioural and organisational measures*. Information security technical report*, (2010)4:1-22.

Senol, H., Akturk, S. & Demirel, S. 2008. Position of small and medium sized enterprises (SMEs) in transition economies within context of financial globalization, financial problems and solution proposals. http://ces.epoka.edu.al/icme/Pos_SME_Fin_Glob_prob.pdf [26 February 2013]

Sharma, M. L. & Bhagwat, R. 2006. Practice of information systems: Evidence from select Indian SMEs. *Journal of manufacturing technology management*, 17(2):199-223.

Sharma, V. 2013. Information security in Hospitality. http://infosecblogg.wordpress.com/2013/05/06/information-security-in-hospitality/ [11 June 2013].

Shoniregun A. C., Nwanko, S., Imafidon, C. & Wynarczyk, P. 2005. Information security challenges facing TEISME business operations in the UK: *International journal for infonomics,* No Volume (1):66-68.

Shropshire, J. 2009. A canonical analysis of intentional information security breaches by insiders. *Information management and computer security,* 17(4):296-310.

Shuttleworth, M. 2008. Quantitative research design. http://www.experiment-resources.com/quantitative-research-design.html [06 June 2009].

Simmons, C. & Burgess, L. 2000. Internet Commerce, security risk analysis and small to medium enterprises. http://www.collecter.org/archives/2000_December/06.PDF [23 *March 2009].*

Siponen, M. T. 2000. A conceptual foundation for organizational information security awareness. *Information management and computer security*, 8(1):31-41.

Siponen, M., Mahmood, M. A. & Pahnila, S. 2013. Employees adherence to information security policies: An exploratory field study. *Information and management*, 51(2014):217-224.

Sinogoj, A. 2004. The importance of e-Security in the overall e-Strategy of an organization. *Proceedings of the 17th e-Commerce conference*, Bled, 21-23 June.

Smallbone, D., Welter, F., Isakova, N & Slonimski, A. 2001.contribution of small and medium enterprises to Economic development in Ukraine and Belarus: Some policy perspectives. *MOCT-MOST: Economic policy in transitional economies,* 11(3):253-273.

Smith, A.D. 2004. Information exchanges associated with the internet travel marketplaces. *Online information review*, 28(4):292-300.

Smith, A.D. 2004. e-Secutity issues and policy development in and information sharing and networked environment. *New information perspectives*, 56(5):272-285.

Smith, E. & J. H. P. Eloff, 1999. Security in health-care information systems--current trends. *International Journal of Medical Informatics,*54 (1):39-54.

Snyder, N. 2013. Eyes on tourism-Beware of travel scams. http://www.thenorwester.ca/Columnists/Nola-Snyder/2013-03-22/article-3205798/Eyes-on-Tourism---Beware-of-travel-scams/1 [03 August 2013].

South African Business Directory. 2007. The Cape Business news. http://www.myprofile.co.za/directory/business/cape_business_news/review/ [17June 2007].

South Africa. 2003. National Small Business Amendment Act. Notice 26 of 2003. *Government gazette*. 461:1-10.

Spinellis, D., Kolakis, S. & Gritzalis, S. 1999. Security requirements, risks and recommendations for small enterprise and home-office environments*. Information management and computer security*, 7(3):121-128.

Stanton, J.M. Stam, K.R. Mastrangelo, P. & Jolton, J. 2005. Analysis of end user security behaviors. *Computer and security*, 24(2):124-133, July.

Stewart, A. 2005. Information security technologies as a commodity input. *Information management and computer security.* 13(1):5-15.

Stokes, A. 2001. Using telementoring to deliver training to SMEs: a pilot study*. Education and training*, 43(6):317-324.

Struwig, F.W. & Stead, G. B. 2001. *Planning, designing and reporting research*, Cape Town: Pearson Education.

Sveen, M.O., Torres, J.M. & Sarriegi, J.M. 2009. Blind information security strategy. *International journal of critical infrastructure protection*, 2(3):95-109.

Tawileh, A., Hilton, J. & McIntosh, S. 2007. Managing information security in Small and Medium Sized Enterprises: A holistic approach. www.tawileh.net/anas/?q=en/disknode/get/691/InfoSec-SME *[7 November 2009].*

Teddlie, C. & Tashakkori, A. 2009. *Foundations of Mixed methods*. California: Sage Publications.

Terre-Blanche, K., Durrheim, K. & Painter, D. 2006. *Research in practice: Applied Methods for the Social sciences*. Cape Town: University of Cape Town Press.

Theoharidou,M. Kokolakis, S. Karyda, M. & Kiountouzis, E. 2005. The insider threat to information and the effectiveness of ISO17799. *computers and security*, 24(26):472-482.

Thomson, K. & Von Solms, R. 2003. Integrating information security into corporate culture. Unpublished Masters Dissertation, Nelson Mandela Metropolitan University, Port Elizabeth.

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

Thompson, K. & Von Solms, R. 2006. Cultivating an organisational informattion security culture. *Computer fraud and security,* 2006(10):7-11, October.

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

Thurik, R. & Wennekers, S. 2004. Entrepreneurship, small businesses and economic growth. *Journal of small business and enterprise development*, 11(1):140-149.

Trim, P.R.J. 2005. Managing computer security issues. Preventing and limiting future threats. *Disaster prevention and management*, 14(4):493-505.

Upfold, C.T. & Sewry, D.A. 2005. An investigation of information security in small and medium enterprises in Eastern Cape. Unpublished Master's dissertation. University of Pretoria. Pretoria.

Vandersoep, S.C. & Johnston,D.D. 2009. *Research Methods for everyday life: Blending qualitative research and Quantitative Approaches*. San Francisco: John Wiley & Sons.

Venesaar, U. & Loomets, P. 2006. The role of entrepreneurship and in economic development and implications for SME policy in Estonia. *Proceedings of 2006 14th conference on Small business research*. 11-13 May. Stockholm:1-17.

Von Solms, R. 1996. Information Security Management: The Second Generation. *Computer & Security,* 15 (1):281-288.

Von Solms, R. & Van Niekerk, J. 2013. From information security to cyber security. *Computers and security*, 38(2013):97-102.

Von Solms, R. & Von Solms, B. 2004. From policies to culture. *Computers and security*, 23(4): 275-279, June.

Vroom, C. & Von Solms, R. 2004. Towards information security behavioural compliance. *Computers and security*, 23(3):191-198, May.

Walker, T. 2008. Prcatical management of malicious insider threat – an enterprise CSIRT perspective*. Information security technical report*, 13(2008):225-234.

Walter, L. & Mcknight, D. L. n,d. What is information assurance? http://www.stsc.hill.af.mil/crosstalk/2002/07/mcknight.html [03 September 2007].

Walton, R. 2006. Balancing the inside and outside threat. *Computer fraud and security*, 2006(11):8-11.

Wang, Y. & Ahmend, P. K. 2009. The moderating effect of the business strategic orientation e-Commerce adoption: Evidence from UK family run SMEs. *Journal of strategic information systems*, 18(2009):16-30, January.

Ward, P. & Smith, C.L. 2002. The development of access control policies for information technology systems. Computers and security 21(4):356-371, August.

Warden, S.C. 2007. E-commerce adoption by SMMEs-How to optimize the prospects of success. Unpublished Doctor's dissertation. Cape Peninsula University of Technology. Cape Town.

Wen, H.J. & Tarn, J.H.M. 1998. Internet security: a case study of firewall selection. *Information management and computer security*, 6(4):178-184.

Whittman, M.E. and Matford, H.J. 2005. *Principles of Information security*. 2nd Ed. Canada: Thompson Course Technology.

Wiant, T. 2005. Information security policy's impact on reporting security incidents. *Computer and security*, 24(6):448-459, September.

Willliams, D.A. 2007. Credit card fraud in Trinidad and Tobago. Journal of financial crime, 14(3):340-359.

Xu, S.X., Yan, X. & Zheng, X. 2008. Communication platforms in electronic commerce: a three dimension analysis*. Info,* 10(2):47-56.

Yao, J. 2004. Ecommerce adoption of insurance companies in New Zealand. *Journal of electronic commerce research*, 5(1):54-61.

Yildrim, E.Y., Akalp, G., Aytac, S. & Bayram, N. 2010. Factors influencing information security in small and medium-sized enterprises: A case from Turkey. *International journal of information management,* 31(4):360-365.

Zheng, J., Caldwell, N., Harland, C., Powell, P., Woerndl, M. and Xu, S. 2004. Small firms and e-business: cautiousness, contingency and cost benefits. *Journal of purchasing and supply management*, 10(1):27-39, January.

Zindiye, S. & Mwangolela,T.F. 2007. Entrepreneurship a key to poverty reduction and socio-economic development. *Proceedings of the 2007 Conference : On SMMEs development: an African perspective: 12-14 September 2007.* Pretoria: 88-98.

Zuccato, A. 2007. Holistic security management for framework applied in electronic commerce. *Computers and security*, 26(3):256-265, May.

Zulu, J. 2007. *Folding the sleeves for the MDGs* http://www.hpgworks.co.za/SARPN/mail/2nd%20Edition/Main.html#DOWNSTREAM [10Nov 2007].

APPENDICES

APPENDIX A: COVER LETTER

21 November 2010

Dear Sir/Madam

Research Project on information security in SMMEs

I am a registered Master's degree student in Office Management and Technology at the Cape Peninsula University of Technology. The title of my research is "*Information security in the hospitality SMMEs in the Cape Metropole area: Policies and measures in the online environment".* The research aims to find out how SMMEs are handling information security issues especially in the online environment.

As part of my research, I will be sending out questionnaires to SMMEs in the hospitality industry who are conducting their business in the Cape Metropole area. The information that will be collected will be kept confidential and it will not be divulged to any third party.

The study will benefit SMMEs because it will indicate if SMMEs in South Africa are on the right track in terms of information security as well as ensuring the smooth transaction of online transactions. Your cooperation is appreciated.

Should you need any clarification, please do not hesitate to contact me or my supervisor at the email address listed below.

Yours faithfully

David Bedi
Ds.beddy@gmail.com Tel: 072-4179970

Dr Stuart Warden (Study Supervisor)
wardens@cput.ac.za

APPENDIX B: Reliability Test Results

[DataSet5] C:\@Data\Research\Research PostGraduate\MTech\CPUT\BediDavid\MTechData new.sav

Scale: Question 9

Case Processing Summary

		N	%
Cases	Valid	51	91.1
	Excluded[a]	5	8.9
	Total	56	100.0

a. List wise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.842	33

APPENDIX C: QUESTIONNAIRE

Questionnaire

Part 1:

Online Trading

1. What are the reasons for e-commerce adoption in your company?

Reason	Option
Provides a competitive advantage	1
Helps in the reduction of costs	2
Provides an opportunity to increase our customer base	3
Helps to improve customer service	4
Convenient-assists in creating a paperless office	5
Provides an opportunity to trade at international level	6
Avails information that we could not access previously	7
Provides timely information	8

Other (Specify) _____

Online Security: Please tick the option that best describes security precautions in your company. You may tick more than one option.

2. Some of the risks that can be associated with e-commerce adoption include

Lack of privacy	1
Vulnerability to information theft	2
Technical failures (example: Software bugs)	3
Loss of finance as a result of theft, virus attacks, fraud and others	4
Challenges to comply with e-commerce requirements	5

*Other (specify)*_____

3. The company IT maintenance and website up-dating is done by….

in-house IT department	1
a third party (outsourced)	2
hiring IT specialists (could be on a temporary basis)	3
permanent employee in the company	4

*Other (specify)*_____

4. Have you or your company suffered from any of the following? (NB, you can choose more than one option).

Computer theft	1
Loss of important data not backed up before	2
Virus infection	3
Any kind of hacking or electronic intrusion	4
Unauthorised disclosure of information by staff or outsiders	5

*Other (Specify)*_____

5. Data back up: Which of the following measures do you take regularly to protect and back up your data? (You may select more than one option).

Staff/employees conduct back-up on their computers	1
Back up of data is done on the server	2
Back up is done off-site in storage media	3
None of the above	4

Other (Specify) _____

6. If employees receive some attachments via their emails, they are encouraged to…..

Delete it without opening it	1
Open it to find out what it is	2
Email the sender back to tell her/him not to email again	3
None of the above	4

*Other (specify*_____

7. The challenges facing my company in the application of information security include:

Shortage of IT staff	1
Government legislation and industry regulations (e.g Cyber laws)	2
E-commerce requirements (always to be alert about security)	3
Lack of finance to adopt appropriate security measures	4
The constant growth and complexity of security attacks	5

Other (specify)

_____

8. How does the company ensure that the employees adhere to the security procedures?

Employees are provided with some training	1
New employees are provided with thorough training	2
Whenever employees breach security they are reprimanded	3
Employees are encouraged to ask when they are not sure about security matters	4
Employees are encouraged to report any suspicious security incidents	5

*Other (Specify)*_____

Part Two:

INFORMATION SECURITY ISSUES

The table below indicates some of the security and human issues that are experienced by companies that conduct online business. Please indicate to what extent you agree or disagree with the statements below. Please (√) the appropriate option

	Strongly agree	Agree	Unsure	Disagree	Strongly Disagree
9.1 Information security should be regarded as a technical issue					
9.2 The information security policy reflects the company's objectives					
9.3 The company has formal procedures indicating how to report information security incidents					
9.4 Internet security is a worrying factor in our company					
9.5 There are regular attempts to breach our security					
9. 6 Spam is not a problem to our company					
9.7 It is important to determine the company's information security needs					
9.8 Information security governance is emphasized in the company					
8.9 Governance of information security minimises risks such as information theft					
9.10 Accountability plays a big role in information security governance					
9.11 Governance of information security improves business operations					
9.12 Only staff in the IT department should carry out the risk assessment task					
9.13 End-users play an important role in information security					
9.14 Managers must make all decisions concerning information security					
9.15 The company has suffered losses as a result of unauthorised access					
9.16 The company employs various means of information security (firewalls, digital signatures)					
9.17 investing in information security should be considered as a future investment					
9.18 The company ensures adequate customer privacy when conducting online business					
9.19 The company deploys adequate information security policies					
9.20 Management emphasize adherence to information security policy					
9.21 All the stakeholders (employees and Management) took part in the implementation of information security policy					
9.22 Policies are made clear and understandable to employees					
9.23 Information security policies are reviewed on a regular basis					
9.24 Information security policies are easily accessible					
9.25Confidentiality of information is emphasized in the company					
9.26 Anti-viruses- are (firewalls) updated/managed on a regular basis?					

9.27 Passwords are changed regularly (what about enquiring about a password policy)					
9.28 The company has suffered loss before as a result of employee mistakes (actions).					
9.29 New employees are provided with training to familiarise them with company security policies					
9.30The company has been a victim of information security breach as a result of employees actions					
9.31 Credit card information is kept confidential					
9.32 The company carries out a weakness assessment on a regular basis to determine the weakest link in the network (why network?)					
9.33 The company makes use of posters as well to communicate a security message					

Part Three – Please select the option that best describes how your company emphasizes security.

10.1 The company has a security training and awareness program in place.
Yes☐ No☐ Don't know☐

10.2 Employees are required to sign an agreement to verify that they have read and understood the policies and procedures. Yes☐ No☐ Don't know ☐

10.3 Strict control is maintained over the internal and external distribution of any paper or electronic media containing client information. Yes☐ No☐ Don't know ☐

10.4 Removable media (e.g. flash drives) containing sensitive information is properly labelled and protected against unauthorized access at all time. Yes ☐ No☐ Don't know☐

10.5 The roles and responsibilities for information security have been clearly defined within the company. Yes☐ No☐ Don't know☐

Part Four – COMPANY BACKGROUND

11.1 Name of Company: _____

11.2 Number of employees: { }

11.3 Company age: { }

11.4 Please tick the relevant one

11.4.1 Are you the: Owner ☐ Owner and Manager ☐ Manager ☐

11.4.2 How long have you been an Owner or Manager?

0 – 5 years ☐ 6 – 10 years ☐ More than 11 years ☐

Optional

11. 5 What is the annual turnover (R)? *(Optional) Please tick the relevant one*

0 – 100 000	☐	100 001 – 500 000	☐
500 001 – 1 200 000	☐	1 200 001 – 2 000 000	☐
More than 2 000 000	☐		

Optional

10.6 The company gross asset is (R)…Please tick the relevant one

0 – 100 000	☐	101 000 - 1, 000 000	☐
1, 000 001 - 2 000 000	☐	More than 2, 000 000	☐

THANK YOU FOR COMPLETING THIS QUESTIONNAIRE…

APPENDIX D: FREQUENCIES

Frequency Table

Q1Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		54	96.4	96.4	96.4
	Do not use e-commerce	1	1.8	1.8	98.2
	Speeds up booking process	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Q2Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		52	92.9	92.9	92.9
	Impersonal	1	1.8	1.8	94.6
	None	1	1.8	1.8	96.4
	Not sure	1	1.8	1.8	98.2
	Time based technical support or know how when the systems go down	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Q3Other

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	56	100.0	100.0	100.0

Q4Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		48	85.7	85.7	85.7
	Loss of data that was stored in an external hard drive, lost data due to guests using the main computer	1	1.8	1.8	87.5
	None	5	8.9	8.9	96.4
	None of the above	1	1.8	1.8	98.2
	Not applicable	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Q5Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		51	91.1	91.1	91.1
	Also done on external hard drive	1	1.8	1.8	92.9
	External hard drive usage	1	1.8	1.8	94.6
	External hard drive usage as well	1	1.8	1.8	96.4
	None	1	1.8	1.8	98.2
	Remote external hard drive	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Q6Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		44	78.6	78.6	78.6
	Applies to all suspicious emails	1	1.8	1.8	80.4
	Block the sender	1	1.8	1.8	82.1
	Check sender first	1	1.8	1.8	83.9
	Delete unless the sender is known	1	1.8	1.8	85.7
	No employees using IT	1	1.8	1.8	87.5
	Of it is from unknown source-it is deleted	1	1.8	1.8	89.3
	Open only if from trusted sources	1	1.8	1.8	91.1
	Open only if the sender is known	1	1.8	1.8	92.9
	Question the sender about attachment	1	1.8	1.8	94.6
	Scan the email for virus first	1	1.8	1.8	96.4
	Taught what to open and what not to open	1	1.8	1.8	98.2
	Unless the attached Items have been cleared through anti-virus	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Q7Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		52	92.9	92.9	92.9
	Labour and knowledge updating and development as well as hardware and software updating	1	1.8	1.8	94.6
	None	1	1.8	1.8	96.4
	None of the above	1	1.8	1.8	98.2
	Not applicable	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Q8Other

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		45	80.4	80.4	80.4
	As IT expert -responsible for admin of security and translate safety to staff as appropriate (usually daily)	1	1.8	1.8	82.1
	Doesn't apply	1	1.8	1.8	83.9
	Not applicable	1	1.8	1.8	85.7
	None	3	5.4	5.4	91.1
	None of the above	2	3.6	3.6	94.6
	Not applicable	1	1.8	1.8	96.4
	Not applicable- computers used by guests only	1	1.8	1.8	98.2
	Owner run establishment	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

9.1 Our company emphasizes information security in order to avoid information loss

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	21	37.5	37.5	37.5
	Agree	21	37.5	37.5	75.0
	Unsure	9	16.1	16.1	91.1
	Disagree	4	7.1	7.1	98.2
	Strongly Disagree	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

There are formal steps outlining the necessary procedure to report information security incidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	6	10.7	10.7	10.7
	Agree	19	33.9	33.9	44.6
	Unsure	11	19.6	19.6	64.3
	Disagree	18	32.1	32.1	96.4
	Strongly Disagree	2	3.6	3.6	100.0
	Total	56	100.0	100.0	

9.3 Internet security is a worrying factor in our company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	5.4	5.4	5.4
	Agree	23	41.1	41.1	46.4
	Unsure	7	12.5	12.5	58.9
	Disagree	19	33.9	33.9	92.9
	Strongly Disagree	4	7.1	7.1	100.0
	Total	56	100.0	100.0	

9.4 There are regular attempts to breach our security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	9	16.1	16.1	16.1
	Unsure	11	19.6	19.6	35.7
	Disagree	26	46.4	46.4	82.1
	Strongly Disagree	10	17.9	17.9	100.0
	Total	56	100.0	100.0	

9.5 Spam is not a problem to our company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	2	3.6	3.6	3.6
	Agree	28	50.0	50.0	53.6
	Unsure	8	14.3	14.3	67.9
	Disagree	13	23.2	23.2	91.1
	Strongly Disagree	5	8.9	8.9	100.0
	Total	56	100.0	100.0	

9.6 It is important to determine our company's information needs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	7	12.5	12.5	12.5
	Agree	34	60.7	60.7	73.2
	Unsure	10	17.9	17.9	91.1
	Disagree	5	8.9	8.9	100.0
	Total	56	100.0	100.0	

9.7 Information security is emphasized in our company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	7.1	7.1	7.1
	Agree	24	42.9	42.9	50.0
	Unsure	15	26.8	26.8	76.8
	Disagree	13	23.2	23.2	100.0
	Total	56	100.0	100.0	

9.8 Information security governance minimises information theft

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	7	12.5	12.5	12.5
	Agree	30	53.6	53.6	66.1
	Unsure	19	33.9	33.9	100.0
	Total	56	100.0	100.0	

9.9 Accountability plays a big role in information security governance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	6	10.7	10.7	10.7
	Agree	33	58.9	58.9	69.6
	Unsure	17	30.4	30.4	100.0
	Total	56	100.0	100.0	

9.10 Governance of information security improves business operations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	8	14.3	14.3	14.3
	Agree	35	62.5	62.5	76.8
	Unsure	12	21.4	21.4	98.2
	Disagree	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

9.11 Only people with IT background are allowed to carry risk assessment in our company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	16.1	16.1	16.1
	Agree	34	60.7	60.7	76.8
	Unsure	7	12.5	12.5	89.3
	Disagree	6	10.7	10.7	100.0
	Total	56	100.0	100.0	

9.12 End-users play an important role in information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	5	8.9	8.9	8.9
	Agree	21	37.5	37.5	46.4
	Unsure	9	16.1	16.1	62.5
	Disagree	20	35.7	35.7	98.2
	Strongly Disagree	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

9.13 Managers must make all decisions concerning information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	14	25.0	25.0	25.0
	Agree	32	57.1	57.1	82.1
	Unsure	1	1.8	1.8	83.9
	Disagree	9	16.1	16.1	100.0
	Total	56	100.0	100.0	

9.14 Our company has previously suffered losses as a result of unauthorized access

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	1.8	1.8	1.8
	Agree	5	8.9	8.9	10.7
	Unsure	15	26.8	26.8	37.5
	Disagree	27	48.2	48.2	85.7
	Strongly Disagree	8	14.3	14.3	100.0
	Total	56	100.0	100.0	

9.15 Our company makes use of various means of information security measures such as firewalls, digital singtures, anti-viruses etc.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	11	19.6	19.6	19.6
	Agree	34	60.7	60.7	80.4
	Unsure	6	10.7	10.7	91.1
	Disagree	5	8.9	8.9	100.0
	Total	56	100.0	100.0	

9.16 Investing in information security can be considered as a future investment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	16.1	16.4	16.4
	Agree	27	48.2	49.1	65.5
	Unsure	17	30.4	30.9	96.4
	Disagree	1	1.8	1.8	98.2
	Strongly Disagree	1	1.8	1.8	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

9.17 Our company ensures adequate customer privacy when conducting online business

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	17	30.4	30.4	30.4
	Agree	31	55.4	55.4	85.7
	Unsure	7	12.5	12.5	98.2
	Disagree	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

9.18 The company deploys adequate information security policies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	7.1	7.3	7.3
	Agree	22	39.3	40.0	47.3
	Unsure	9	16.1	16.4	63.6
	Disagree	20	35.7	36.4	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

9.19 Staff members are encouraged to follow security measures in place to protect information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	11	19.6	19.6	19.6
	Agree	29	51.8	51.8	71.4
	Unsure	6	10.7	10.7	82.1
	Disagree	10	17.9	17.9	100.0
	Total	56	100.0	100.0	

9.20 End-users (Staff members) contributed to the implementation of information security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	1.8	1.8	1.8
	Agree	18	32.1	32.1	33.9
	Unsure	5	8.9	8.9	42.9
	Disagree	30	53.6	53.6	96.4
	Strongly Disagree	2	3.6	3.6	100.0
	Total	56	100.0	100.0	

9.21 Policies are made clear and understandable to employees

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	5	8.9	8.9	8.9
	Agree	23	41.1	41.1	50.0
	Unsure	9	16.1	16.1	66.1
	Disagree	17	30.4	30.4	96.4
	Strongly Disagree	2	3.6	3.6	100.0
	Total	56	100.0	100.0	

9.22 Information security policies are reviewed on a regular basis

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	7.1	7.1	7.1
	Agree	15	26.8	26.8	33.9
	Unsure	12	21.4	21.4	55.4
	Disagree	24	42.9	42.9	98.2
	Strongly Disagree	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

9.23 Information security policies are easily accessible

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	1.8	1.8	1.8
	Agree	15	26.8	27.3	29.1
	Unsure	15	26.8	27.3	56.4
	Disagree	24	42.9	43.6	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

9.24 The information security policies reflects our company's objectives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	5.4	5.5	5.5
	Agree	13	23.2	23.6	29.1
	Unsure	18	32.1	32.7	61.8
	Disagree	21	37.5	38.2	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

9.25 Anti-viruses (firewalls) are updated on a regular basis

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	13	23.2	23.2	23.2
	Agree	23	41.1	41.1	64.3
	Unsure	10	17.9	17.9	82.1
	Disagree	10	17.9	17.9	100.0
	Total	56	100.0	100.0	

9.26 The company has a password policy in place

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	12	21.4	21.4	21.4
	Agree	10	17.9	17.9	39.3
	Unsure	6	10.7	10.7	50.0
	Disagree	24	42.9	42.9	92.9
	Strongly Disagree	4	7.1	7.1	100.0
	Total	56	100.0	100.0	

9.27 Our company has suffered loss before as a result of employee mistakes (actions)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	2	3.6	3.6	3.6
	Agree	10	17.9	17.9	21.4
	Unsure	16	28.6	28.6	50.0
	Disagree	18	32.1	32.1	82.1
	Strongly Disagree	10	17.9	17.9	100.0
	Total	56	100.0	100.0	

9.28 New employees are provided with training to familiarise them with the company security policies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	5	8.9	9.1	9.1
	Agree	27	48.2	49.1	58.2
	Unsure	7	12.5	12.7	70.9
	Disagree	15	26.8	27.3	98.2
	Strongly Disagree	1	1.8	1.8	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

9.29 Our company has been a victim of an information security breach as a result of employees actions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	1.8	1.8	1.8
	Agree	5	8.9	8.9	10.7
	Unsure	13	23.2	23.2	33.9
	Disagree	27	48.2	48.2	82.1
	Strongly Disagree	10	17.9	17.9	100.0
	Total	56	100.0	100.0	

9.30 Credit card information is kept confidential

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	20	35.7	37.0	37.0
	Agree	29	51.8	53.7	90.7
	Unsure	3	5.4	5.6	96.3
	Disagree	1	1.8	1.9	98.1
	Strongly Disagree	1	1.8	1.9	100.0
	Total	54	96.4	100.0	
Missing	System	2	3.6		
Total		56	100.0		

9.31 Our company carries out a weakness assessment on a regular basis to determine the weakest link

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	2	3.6	3.6	3.6
	Agree	14	25.0	25.0	28.6
	Unsure	14	25.0	25.0	53.6
	Disagree	19	33.9	33.9	87.5
	Strongly Disagree	7	12.5	12.5	100.0
	Total	56	100.0	100.0	

9.32 Our company makes use of posters as well to communicate security message

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	5.4	5.4	5.4
	Agree	4	7.1	7.1	12.5
	Unsure	5	8.9	8.9	21.4
	Disagree	36	64.3	64.3	85.7
	Strongly Disagree	8	14.3	14.3	100.0
	Total	56	100.0	100.0	

9.33 Information security should be regarded as a technical issue

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	16.1	16.1	16.1
	Agree	34	60.7	60.7	76.8
	Unsure	8	14.3	14.3	91.1
	Disagree	4	7.1	7.1	98.2
	Strongly Disagree	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

10.1 The company has a security training and awareness program in place

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	14	25.0	25.0	25.0
	No	39	69.6	69.6	94.6
	Don't know	3	5.4	5.4	100.0
	Total	56	100.0	100.0	

10.2 Employees are required to sign an agreement to verify that they have read and understood the policies and procedures

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	11	19.6	20.0	20.0
	No	40	71.4	72.7	92.7
	Don't know	4	7.1	7.3	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

10.3 Strict control is maintained over the internal and external distribution of any paper or electronic media containing client information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	36	64.3	64.3	64.3
	No	15	26.8	26.8	91.1
	Don't know	5	8.9	8.9	100.0
	Total	56	100.0	100.0	

10.4 Removable media (e.g. flash drives) containing sensitive information is properly labelled and protected against unauthorized access at all times

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	32	57.1	58.2	58.2
	No	19	33.9	34.5	92.7
	Don't know	4	7.1	7.3	100.0
	Total	55	98.2	100.0	
Missing	System	1	1.8		
Total		56	100.0		

The roles and responsibilities for information security have been clearly defined within the company

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	28.6	28.6	28.6
	No	33	58.9	58.9	87.5
	Don't know	7	12.5	12.5	100.0
	Total	56	100.0	100.0	

Number of Employees

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	3	5.4	5.4	5.4
	3	3	5.4	5.4	10.7
	4	5	8.9	8.9	19.6
	5	4	7.1	7.1	26.8
	6	4	7.1	7.1	33.9
	7	4	7.1	7.1	41.1
	8	2	3.6	3.6	44.6
	9	5	8.9	8.9	53.6
	10	1	1.8	1.8	55.4
	12	2	3.6	3.6	58.9
	13	4	7.1	7.1	66.1
	14	2	3.6	3.6	69.6
	16	1	1.8	1.8	71.4
	18	2	3.6	3.6	75.0
	19	1	1.8	1.8	76.8
	20	3	5.4	5.4	82.1
	21	1	1.8	1.8	83.9
	23	1	1.8	1.8	85.7
	25	2	3.6	3.6	89.3
	27	2	3.6	3.6	92.9
	30	1	1.8	1.8	94.6
	31	1	1.8	1.8	96.4
	40	1	1.8	1.8	98.2
	100	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Company Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	5.4	5.4	5.4
	2	4	7.1	7.1	12.5
	3	4	7.1	7.1	19.6
	4	5	8.9	8.9	28.6
	5	7	12.5	12.5	41.1
	6	5	8.9	8.9	50.0
	7	1	1.8	1.8	51.8
	8	4	7.1	7.1	58.9
	9	3	5.4	5.4	64.3
	10	3	5.4	5.4	69.6
	11	4	7.1	7.1	76.8
	12	3	5.4	5.4	82.1
	14	2	3.6	3.6	85.7
	15	5	8.9	8.9	94.6
	20	2	3.6	3.6	98.2
	30	1	1.8	1.8	100.0
	Total	56	100.0	100.0	

Owner/Manager

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Owner	7	12.5	12.5	12.5
	Owner and Manager	24	42.9	42.9	55.4
	Manager	25	44.6	44.6	100.0
	Total	56	100.0	100.0	

How long have you been the owner/manager

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	o - 5 years	34	60.7	60.7	60.7
	6 - 10 years	15	26.8	26.8	87.5
	11 or more years	7	12.5	12.5	100.0
	Total	56	100.0	100.0	

Annual Turnover

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	R100 001 - R500 000	2	3.6	22.2	22.2
	R500 001 - R1 200 000	5	8.9	55.6	77.8
	More than R2 000 000	2	3.6	22.2	100.0
	Total	9	16.1	100.0	
Missing	System	47	83.9		
Total		56	100.0		

Company Gross Asset

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 - R100 000	1	1.8	14.3	14.3
	R100 001 - R1 000 000	2	3.6	28.6	42.9
	R1 000 001 - R2 000 000	4	7.1	57.1	100.0
	Total	7	12.5	100.0	
Missing	System	49	87.5		
Total		56	100.0		

Custom Tables

Question		Count	Column N %
Question 1 What are the reasons for e-commerce adoption in your company?	1.1 Provides a competitive advantage	34	60.71%
	Helps in the reduction of costs	26	46.43%
	Provides an opportunity to increase customer base	32	57.14%
	Helps to improve customer service	33	58.93%
	Convenient-assist in creating a paperless office	20	35.71%
	Provides an opportunity to trade at international level	31	55.36%
	Avails information that we could not access previously	14	25.00%
	Provides timely information	23	41.07%
Question 2 Some of the risks that can be associated with e-commerce adoption include	Lack of privacy	30	53.57%
	Vulnerability to information theft	20	35.71%
	Technical failures (example, software bugs)	31	55.36%
	Loss of finance as a result of theft, virus attacks, fraud and others	35	62.50%
	Challenges to comply with e-Commerce requirements	9	16.07%
Question 3 The company IT maintenance and website up-dating is done by….	In house IT department	13	23.21%
	A third party(Outsourced)	18	32.14%
	Hiring of IT specialists (could be on a temporary basis	18	32.14%
	Permanent employee in the company	16	28.57%
Question 4 Have you or your company suffered from any of the following?	Computer theft	20	35.71%
	Loss of data not backed up before	24	42.86%
	Virus infection	40	71.43%
	Any kind of hacking or electronic intrusion	7	12.50%
	Unauthorised disclosure of information by staff or outsiders	6	10.71%
Question 5 Data back up: Which of the following measures do you take regularly to protect and back up your data?	Staff/Employees conduct back-up on their computers	31	55.36%
	Back up of data is done on the server	17	30.36%
	Back up is done off-site in storage media	14	25.00%
	None of the above	8	14.29%
Question 6 If employees receive some attachments via their emails, they are encouraged to…..	Delete it without opening it	25	44.64%
	Open it to find out what it is	12	21.43%
	Email the sender back to tell him/her not to email again	0	0.00%
	None of the above	16	28.57%
Question 7 The challenges facing our company in the application of information security include:	Shortage of IT staff	33	58.93%
	Government legislation and industry regulations (e.g Cyber laws)	7	12.50%
	e-commerce requirements (always to be alert about security)	23	41.07%
	Lack of finance to adopt appropriate security measures	22	39.29%
	The constant growth and complexity of security attacks	22	39.29%
Question 8 How does the company ensure that the employees adhere to the security procedures?	Employees are provided with some training	15	26.79%
	New employees are provided with a thorough training	14	25.00%
	Whenever employees breach security they are reprimanded	5	8.93%
	Employees are encouraged to ask when they are not sure about security matters	28	50.00%
	Employees are encouraged to report any suspicious security incidents	25	44.64%

APPENDIX E: SMME DETAILS

The validity of the SMME respondents are revealed, where the aim was to determine whether businesses that participated in this research, were indeed SMMEs. The South African Government Gazette, Act 2003, specifies three features that are used to define SMMEs, namely:

- Financial turnover;
- Number of fixed assets that the company owns; and
- Number of employees.

Table 7.1: Respondent SMEs' validity

Number of employees	Response rate Percentage (%)	Annual turnover Rand(Optional)	Response Rate Percentage (%)	Value of assets owned by company (Optional)	Response Rate Percentage (%)
1-10 Employees	55	100 000 - 500 000	4		
11-20 Employees	27	500 001- 1000 000	9		
21-200 Employees	18	1000 001 and over	4		

Table 7.1 depicts the validity of responding SMME according to South African Gazette definition, Act 2003. A total of 55 per cent indicated that they have between 1 and 10 employees. A total of 27 percent of the respondents indicated that they have between 11 and 20 employees, while a total of 18 per cent indicated that they have between 21 and 200 employees. On the other hand, only 15 per cent of the respondents responded to the question about the annual turnover. Table 7.1 further depicts that a total of 4 per cent of the respondents indicated that their annual turnover ranges between R100 000 and R500 000. A total of 9 per cent indicated that their annual turnover is between R500 001 and R1000 000. A total of 4 percent indicated that their annual turnover is over R1000 000. None of the companies answered the optional question about the value of assets that the company owns.

Table 7.2 depicts information about the position in the company of the respondents as well as the age of the company.

Table 7.2: Respondents details

Position in the	Response Rate Percentage (%)	Age of the company	Response Rate Percentage
Owner	12	1-5 years	41
Owner and Manager	43	6-10 years	29
Manager	45	11 years and more	30

Table 4.2 depicts that a total of 12 percent were owners while 43 percent were owner-managers. A total of 45 percent were managers. As indicated in Chapter 3 only managers/owners were targeted thus relying on the fact that they should have a better understanding of their businesses. Table 4.2 further depicts that a total of 41 percent of respondents were from businesses that are 1- 5 years old. A total of 29 percent of respondents were from businesses that are 6-10 years old, while 30 percent of respondents were from mature businesses that ranged between 11 and 30 years old. These statistics are important as they show that the business represents a cross section in terms of both new and established businesses.

APPENDIX F: INTERVIEW 1

SMMEs 1 Manager Interview

Interviewer

Good morning Madam.

Good morning.

Thank you for accepting my invitation to take part in this study, I am sure it will help SMMEs in the long run. My name is David, currently studying towards my MTech at CPUT conducting my study on computer usage in hospitality SMMEs.

It is my pleasure.

Let's go straight into the questions

I will appreciate that because I don't have much time.

1.1 What percentage of e-commerce applications does your organization use?

Our company is 100 per cent e-commerce dedicated. In other words we have quite a number of e-commerce applications offered by the company. For example, booking is done online including the payments. As you know hospitality companies rely on the Internet to succeed and we are not an exception. Most of our clients are based outside the country and therefore to conduct business with them, we needed to be an e-commerce dedicated company. Emails are a good example of e-commerce application within our company.

1.2 What physical access controls are in place to keep desktop computers and other computing devices secure?

When it comes to physical access controls in place to keep computers secure, only one person has been given the mandate to lock and unlock the building. The person usually leaves after everyone has left and must come early to open doors for other staff members. Besides the company is located in a secure place where everyone who enters the place must first sign at the main gate where there are security guards day and night. The building is under security surveillance 24 hours 7 days a week. So I can say we don't have a problem of theft.

*1.3 W*hat *percentage of your overall budget do you assign to information security (Computer security)?*

It is difficult to specify but the company put a good sum of money to take care of all information technology related issues. Security being one of the worrying

factors is highly emphasized and the company makes sure that it acquires the latest technologies to address security issues. The company deals with personal information and as such, it must keep it secure. I can just say our security is target marketed with security in place,

1.4 What kind of security breaches has your company experienced in the past?

The common security problem that is facing the company is attempted credit card fraud. In most cases, the culprits try to make use of fictitious credit card information. Fortunately the company has never experienced a serious credit card scam. We have been fortunate because the company has been able to detect the scams before they happen. There was only one minor incident where client wanted to accuse the company of double charging him when he was paying for the flight. This problem was sorted out quickly.

1.5 How do guard against, detect and report malicious software in your company? For example, how does the company make sure that the computer system and information resources are kept secure?

The company relies on the Internet Service Provider firewalls to guard against malicious software. I then look after the network as the administrator. My roles as the network administrator in this company is to make sure that we use the best technology and making sure that confidential information in the network is only available to the right people. To sum it up, staff members are authenticated into the system through the usage of username and the personal password. The user's password expires after three months and staff members will then have to change the password. The good thing is once the password has expired, it cannot be used again.

1.6 How is data backed up, in other words what is the data backup plan?

Since we deal with confidential information, we take all the necessary steps to make sure that we do not lose critical information. We back information in external hard-drives onsite and off-site. Confidential data is also backed up as a cloud service. Through cloud service we are able to get the information that we need at that moment. The service provider manages everything connected to that information. One of the advantages that we get from applying cloud as a backup system is that we can access data from anywhere.

1.7 Do you have procedures in place for recovery of lost data?

We have a gentleman that comes in that does our back-up and double checks and recovers any data that we might have lost. The other option is to request data from the Johannesburg branch because in most cases that is where the backed up data is stored. As I indicated earlier, data is transferred into external hard drives every two hours at the Johannesburg offices. As the Cape Town branch, we have never lost important data that we couldn't recover. We also have three devices that backs-up the data as the satellite branches. We plug one device and copy all the files before we plug another one. And we also have the main Office in Johannesburg that has got all the data controlled there as well. The name of the one in Johannesburg is called More Hotels. (Laughs) We have got property in Cape Town, Kruger National Park, Madikwe and Johannesburg. Everything happens at the main office in Johannesburg. We have got the central reservation office.

1.7.1 Do you perhaps pay insurance for confidential information?

We only pay insurance for the hardware like computers and external hard-drives. If lets says the computer can be stolen, then we will consult the insurance company that will then replace the computer. If it happens that we lose information alone then it will mean the company has lost. May be the reason why the company decided to not pay insurance for information is because it is sometimes difficult to quantify information.

1.8 How are users authenticated into the system?

As I indicated previously, users can only access the system through the usage usernames and password. The username is usually the person's surname while the password is personal.

1.*9 What is the company doing to make sure that the employees do not download malicious software from the Internet?*

Firewalls are used to minimize downloading of malicious software from the Internet. Our firewall does not allow downloading of files from the Internet except attachments sent via mail. People in the management are provided with modems that allow them to download important files. If an ordinary employee needs to download a file urgently, then they can request from the manager. Each and everyone who joins the company is warned against abusing the Internet..

1.10 There are some security standards used to help companies with security like SABS and ISO 27001. Is the company making use of any of these standards?

The company does not make use of those guidelines as we believe that we have rules that are tailored to suit the company. As much as I believe that those security standards are useful, we also believe that we have a team of experts capable of formulating security rules that will drive the company forward.

2. SECURITY TRAINING AND AWARENESS

2.1 How often does the company provide security training to staff members?

The company deals with confidential information and besides, technology keeps on changing and therefore employees must be up to date to address all these challenges. In order to cater for that, employees are usually sent to training every three months. Before anyone is sent for training, there must be a general meeting where people are going to be selected for training. The participants will then be sent away for training. Normally training ranges from three to six months.

2.2 What is being done to make sure that new staff members do not compromise the company's information resources?

All the employees signed a confidentiality contract. As soon as a new employee is hired he or she will be given the new contract to sign with all the conditions of employment. Employees are therefore aware of what is expected from them immediately.

2.3 In the event of a security breach (incident) what are staff members expected to do?

Staff members are expected to let me know as the network administrator in the event of a security breach. I will then deal with the problem. I am capable of addressing most of the security breaches. The other thing is that, I do random checking of the network to check if there are no security breaches or tempering of the network. In most cases I will be the first one to pick the breach up.

2.4 Are staff members informed about acceptable and unacceptable usage of the company's information systems (e.g. email and Internet conduct)?

Yes, staff members are well informed about acceptable behaviour. As I mentioned earlier they sign contracts and if they violate them they are given warnings. An employee is given a warning if the abuse was not serious. If it is a serious security breach then they will be fired. It is stated in their contracts.

INFORMATION SECURITY POLICIES

3.1 *What is your company doing to make sure that staff members comply with security policies?*

In order to make sure that staff members do not violate the company's policies, each employee's Internet protocol is monitored. Just like in the previous question, employees who violate the policies will be given warnings. If the employee keeps on violating the policies, then he or she will be fired. Employees are expected to abide by the rules and regulations of the company. As it is norm, in other companies, when a new employee is hired, he or she is provided with induction where he or she is provided with training, told about all the company's rules and regulations.

3.1.1 Have you ever experienced such a problem?

Yes, one employee was fired because he somehow managed to bypass the firewall and downloaded a lot of files from the Internet. He was caught downloading music and the company just decided to fire him because it was discovered that he had been doing it for a long time. That incident made the company to be stricter to employees.

3.2 How are security policies formulated in the company and how often are they updated?

Our security policies were formulated through the assistance of the Internet Service Provider. They came up with the policies and we selected those that can drive the company forward. We believed that this was the best decision since these people are experts and provide service to a whole lot of companies. Our policies are updated once in a while.

3.3 *Does the company have any other documentation to guide staff members in connection with information security? If yes, what is it?*

Yes, Employees sign contracts. This is done as soon as the employee is recruited into the company.

3.4 If the company makes use of anti-virus software, how often is it updated?

The company makes use of the anti-virus that is updated on a daily basis. As you might be aware, it is risky to connect your computer to the Internet. In order to avoid losing important information we have made sure that our anti-virus is updated on a daily basis. Each and every day, a new virus is released.

3.5 If online booking is conducted in your company, what measures have been put in place to make sure that the customer's details are kept secure?

We do not have any means except making employees sign contacts. We believe that is the best way of protecting the customer's secure information. Customers are very important to our company so we cannot afford to expose their information as this will put our company at risk. They are the reason why we exist.

3.6 How frequently must passwords be changes and what complexity requirements do you use?

Passwords are changed after every 60 days. Our system does not allow staff members to use the password for more than 60 days. It has been programmed in such a way that after 2 months a new password must be used.

3.7 In your own opinion, do you think the company's information security policies are in line with its objectives.

The company's security policies are in line with our goals. The company strives to be one of the service companies. Our policies support this and we make sure that even the people that we hire are aware of this. As I mentioned earlier on, employees are sent to training regularly to make sure that we achieve we achieve our goal

Thank you

It's my pleasure. Good luck with your studies

APPENDIX G: INTERVIEW 2
SMME 2 General Managers/Owner Interview

Good afternoon madam
Good afternoon

Thank you for accepting to be interviewed so that we can discuss this burning issue.
It is my pleasure, you may shoot.

Question 1 – General Security Requirements

1.1 What percentage of e-commerce applications does your organization use?

The company uses e-commerce as the core of the business. Most of our business transactions are done online. Basically I can say the company is 90 percent e-commerce connected. Clients can still book telephonically and then they can pay online or via bank transfers. Most of the overseas customers book and pay online. On the other hand, we still have some customers who prefer paying via bank transfers especially African customers.

1.1.2 *Are reservations allowed?*

We welcome reservations but a client must pay a certain amount to reserve the room. If he or she does not pay, then he or she can easily lose the room. We work on first come first serve principle.

1.2 What physical access controls are in place to keep desktop computers and other computing devices secure?

We just have the common security controls that are common in most companies whereby offices are locked at night. But our company opens until late because there are situations where we have guests arriving very late. Our workers work on shifts to cater for those guests who might arrive late at night. Besides we have a security guard in the building at night to safeguard against any criminal activities.

1.3 What percentage of your overall budget do you assign to information security (computer security)?

Now you want to know our budget? (Pause a bit)...We are a small company and therefore do not assign much finance towards security. We have hired an IT company that deals with the company's information security issues. They are the ones who handle our security issues and therefore we pay them on a monthly basis and that is almost all the amount that we spend on security. I must admit though that we bought computers from our own budget and the IT

company just maintains them. For example, if one of the computers is not working, we just call them and they will come and repair the computer.

1.4 What kind of security breach has your company experienced in the past?

We have never experienced any security breach before. The only minor problem that we normally experience is viruses especially from the computers that are used by the clients because they sometimes use their flash drives that might be infected with viruses. Other than that we have never experienced a serious breach.

1.5 How do you guard against, detect and report malicious software in your company? For example, how does the company make sure that the computer system and information resources are kept secure?

Well, as I indicated we have hired an IT company that handles most of our IT issues. If for example, one of the staff members notices that someone is trying to hack into the company's network, he will inform me and I will then decide whether to call the company or not. The other thing is that important folders are backed up by the IT Company on a daily basis. After seven days the backed up data will be overwritten over the one that was backed up. The downfall is that should we need information that was backed up may be eight days ago, we won't be able to get it because the system would have written over it. We have never experienced such a problem though. When it comes to credit card information, ordinary staff members do not have access to it. Only people in the management like me can access that information.

1.6 How is data backed up, in other words what is the data backup plan?

As I indicated above, the IT company does the back up for us. Data is backed up on daily basis and after seven days the data is deleted and new data is written over that one. The staff members must decide which data is important and it will be backed up in the network. Data that is not important will not be backed up.

1.7 Do you have procedures in place for recovery of lost data?

Well, we do have a plan in place to recover lost data. The IT company that we hired is a well established company that easily deals with that. For example, sometimes clients lose their data as a result of viruses, if they had important folders, then we normally call the company to help recover the lost data. The

client will then have to pay the company. The company charges the client based on the size of the recovered data. If the data was in a 2 gigabyte flash drive, it will be cheaper than if they recovered data from three hundred and fifty gigabyte external hard drive. When it comes to the company data, we have never lost any data but should it happen, then the company can help us recover it. We don't have to pay for data recovery because it is part of the IT company's duties to make sure that all IT issues are take care of.

1.7.1 Do you pay the company on a monthly basis?

Yes we pay them on a monthly basis. We have signed a contract with the company and pay them according to the agreement on the contract. Basically the amount is the same

1.8 How are users authenticated into the system?

Users are commonly authenticated through the usage of passwords. When it comes to staff members, they have their personal passwords that they use to access the system. Staff members must have two passwords, one for personal usage and the other for accommodation booking. The password for accommodation booking does not change, is stays the same forever. As for personal passwords, it is up to an individual to decide whether to change it or not.

*1.8.1 The company's system does not remind users to change their password*s?

No, it is up to an individual to make that he or she changes the password. Even the management does not enforce regular password changes because we expect users to keep their passwords secure and therefore do not see the need to enforce regular password usage

1.*9 What is the company doing to make sure that the employees do not download malicious software from the Internet?*

Our system has been set in such a way that there are no downloads that can be done. Staff members can only browse the Internet. They are allowed to use social networks such as Facebook during office hours as long as they know when to do it. For example, it is wrong for a staff member to use social media when a client is waiting for service. I know some people are addicted to Facebook. But I encourage them to join social networks because in a way it helps advertise the company.

1.10 There are some security standards used to help companies with security like SABS and ISO 27001, COBIT 5, is the company making use of any of these standards?

We do not make use of any of security standards. The management is well aware of security issues and how to go about avoiding breaches. We do not see a need to make use of these security standards. Remember we are a hospitality company and we do not need to know information security in deep. Besides we rely on an external company to fulfil our IT needs.

2. SECURITY TRAINING AND AWARENESS

2.1 How often does the company provide security training to staff members?

The company does not provide security training to staff members. Security training is expensive and the company cannot afford it. We normally look at the person's CV before hiring him or her. New staff members are only provided with a thorough induction to familiarise them to the working conditions in the company. I also try to maintain a healthy relationship with the employees to make sure that I am accessible. If employees have questions, they know they are welcome into my office.

2.1.1 So you recruit people who are familiar with computers?

Yeah, we hire people with the skills we are looking for. Once someone has been hired, he or she will be provided with an induction in order to familiarise him/her to the new environment.

2.2 What is being done to make sure that new staff members do not compromise the company's information resources?

Nothing much, we just have to trust that they will be honest. I mean they also signed a contract with the company and it is clear in the contract that anyone caught abusing the company's resources will be dealt with. Should the employee deliberately disclose sensitive information, he or she will be fired from the company. So we make new employees aware of all these issues.

2.3 In the event of a security breach (incident) what are staff members expected to do?

If a security breach was to happen, staff members are expected to report the incident to management as soon as possible to make sure that it is addressed immediately before it escalates. Management will then decide whether to call

the IT company or not. If it is something that I can deal with then I will address the breach to make sure that it does not happen again. But as I said, we have never had this problem before.

2.4 Are staff members informed about acceptable and unacceptable usage of the company's information systems (e.g. email and Internet conduct)?

We have regular staff meetings to discuss burning issues. Besides staff members are well aware of when to use the Internet and emails. They cannot use the Internet when a client is waiting for a service. Previously we were paying Internet according to how much we have used. That time I was very strict with Internet usage. These days we are using uncapped Internet and we do not monitor staff members on their internet usage. They are allowed to browse the Internet as much as they want as long as they don't forget their duties. If they are on social media, then that is good because it can be beneficial to the company.

INFORMATION SECURITY POLICIES

3.1 *What is your company doing to make sure that staff members comply with security policies?*

We do not have written policies as we cannot afford to keep on updating them but what we do is, we have incorporated everything that we expect from our employees in the contract. Employees are expected to read their contracts before they sign them. If an employee breaches his or her contract then he or she will be called for a hearing. Depending on the severity of the offence or the breach, the employee can either be given a verbal or written warning. If it is a serious breach then he or she will be fired from the company.

3.1.1 Have you ever experienced such a problem?

No we have never had a situation whereby an employee breached his or her contract. The only problem we experienced before was staff members abusing Internet when we were still paying for Internet according to usage. That was the common problem.

3.2 How are security policies formulated in the company and how often are they updated?

We are very informal and relaxed and we do not have formal security policies but just like any other companies we have rules. The rules pertaining to

information security were formulated by management. As you might be aware, this company has number of branches around Cape Town, so we sometimes sit as managers to decide the way forward. If we feel that there is something that needs an urgent address, then we call a meeting to discuss the issue.

3.3 *Does the company have any other documentation to guide staff members in connection with information security? If yes, what is it?*

The company does not have any other security documentation. We rely on rules and regulations and most of them are general. Most of the time our security decisions are based on trust. That is why we didn't see the need for written security policies.

3.4 If the company makes use of anti-virus software, how often is it updated?

We do make use of the anti-virus and it is updated regularly. To be precise it is updated after every three months. It updates itself and we just buy the licence at the beginning of the year throughout the year we don't bother about the anti-virus because it updates itself. At the moment I do not have any problems with it because it is working well.

3.5 If online booking is conducted in your company, what measures have been put in place to make sure that the customer's details are kept secure?

Yes we do have online booking system in place. We have made sure that credit card information is not accessible to ordinary staff members. Only managers can access credit card information. In other words, we have made sure that the number of people who can access sensitive information is limited.

3.6 How frequently must passwords be changed and what complexity requirements do you use?

We use two forms of passwords in our company. The first password is just to authenticate the user into the system. That password is personal and the user (staff member) can change it whenever he or she feels like. We don't monitor personal passwords. The other password is to allow the staff members to conduct the booking for customers. This password is changed after every three months. There is no formal way of formulating passwords in our company. Passwords for booking are changed by me and I just come up with the characters and let the staff members know them. That is all, nothing special.

3.7 In your own opinion, do you think the company's information security policies are in line with its objectives.

Again, we do not have policies. In a way I can say the rules we have are in line with the company's objectives. I have made sure that we have rules that are success driven. We want the company to grow and our rules support that. Our company is well known and we always receive guests from different countries, some from overseas.

APPENDIX H: INTERVIEW 3

SMME 3 Manager- Interview

Good afternoon Madam, thank you for accepting my invitation to take part in this interview
Good afternoon, I hope I will be able to answer the question as this is not really my speciality.

Questions are not that difficult, as long as you are part of the management team, you should in a position to answer them
Ok, if that is the case then I will give them a try.

1.1 What percentage of e-commerce applications does your organization use?

Where do I start, well we just use the basics of e-commerce. Guests can book online, send us an email requesting prices, or even book via email. After booking they must transfer money into our accounts. After transferring money, they must email or fax us the receipt then we can make the booking official and confirm it. So I can say we use 75 per cent of e-commerce.

1.2 What physical access controls are in place to keep desktop computers and other computing devices secure?

We don't have much control except that our building is secure. As you have noticed, you must use the intercom to gain access into the building. Yes, criminal activities can take place even in the most secure places, but we have never had a problem of theft. We also make use of security alarms. In cases of hostages, we can press a panic button and the armed security guards will show up. When it comes to guests, they are always monitored when using our computers. We do not lock the computers. The computer room is by the reception and there is always someone there.

1.2.1 *What about credit card fraud?*

We have never had such a problem. I know it is a common problem for companies that conduct online business but we have been lucky. I must also applaud the people who are taking care of our IT services. They are doing a good job.

1.3 What percentage of your overall budget do you assign to information security (Computer security)?

That is a difficult question. Let me put it this way, we do not assign much finance to computer security. We do hire IT technicians sometimes just to check our network systems. The company's primary role is to provide

accommodation to the guests and security is not our biggest concern and as a result don't see a point of assigning too much finance towards it. Our security expenditure varies from one month to another. If nothing goes wrong with our networks and computers, then we do not spend much that month.

1.4 What kind of security breaches has your company experienced in the past?

Most of the security breaches that we experience are virus attacks. Even though we have an anti-virus in our systems, viruses somehow still manage to attack our computers. Last year a virus attacked our computers and one of the computers ended up crashing. Fortunately we did not have valuable information stored in the computer. As a result of this, we do not allow clients to use their memory sticks in our computers. If a client is desperate to use the memory stick then we scan it and that's when he or she can use it. But as you know, people have ways of cheating around rules. They still make use of the flash drives without scanning them. That is a challenge that we need to address.

1.5 How do you guard against, detect and report malicious software in your company? For example, how does the company make sure that the computer system and information resources are kept secure?

We do not do much except the antivirus that we have in place. As I mentioned earlier, we sometimes hire an IT technician to come and check our network system especially if we are experiencing problems. For example, sometimes our Internet tends to be slow. To address the problem, we normally call the IT consultant to address the problem. We do not have a dedicated IT specialist except relying on outsiders.

1.5.1 How do you make sure that these outsiders do not abuse your sensitive information?

We do not do anything special except to make sure that they do not access the rooms that we keep important documents. Credit card information is always kept secure and we do not even want to compromise on that one. As for the information sent via the network, we have never had problems. The thing is we had to consider the costs of hiring an IT expert on a permanent basis versus on a temporary basis. The costs of hiring an expert on a permanent basis were too high. In a nutshell, IT experts that we hire do not have access to sensitive data.

1.6 How is data backed up, in other words what is the data backup plan?

We back up important data in external hard-drives. Each staff member has an external hard drive that he or she uses to store sensitive information. We work on shifts and sometimes you might find that one staff member is not here when you want to store some information. That is why we decided to buy each staff member an external hard drive. Each staff member is expected to take his or her external hard drive with him when he or she knocks off. That is how we back up information.

1.7 Do you have procedures in place for recovery of lost data?

Not really, like I said we hire IT consultants on temporary basis if we encounter problems.

1.8 How are users authenticated into the system?

Our systems are not locked. No passwords required to access the system. The company does not have a big workforce and we don't see the need for passwords. We trust each other and have never experienced any problems.

1.8.1 How many staff members does the company have?

All in all we have 14 employees, 3 cleaners, 3 managers and 8 employees who conduct the bookings and other administrative work within the company.

1*.9 What is the company doing to make sure that the employees do not download malicious software from the Internet?*

Clients can only access basic internet and downloading of documents is not allowed. Basically the computers that they use allow them to browse the Internet only without downloading any files from the Internet. Even if they use their laptops to access the net, they won't be able to download anything from the Internet. We have wireless Internet and clients can buy some Internet bundles if they want to use the Internet. Actually even if they want to use the company's computers, they are required to buy Internet bundles to access the net. On the other hand, staff members can download files from the Internet. We have made it clear that they are can only download work related files from the Internet. If a person is caught downloading personal stuff from the Internet, he or she will be taken for disciplinary hearing.

1.9.1 Is there any device that you use to stop clients from downloading files from the Internet?

We do not make use of any device to control downloading of files but we make it clear to the guests that downloading is not allowed. We monitor the websites that they visit to make sure that they do not sabotage the company by downloading corrupt files from the Internet.

1.10 There are some security standards used to help companies with security like SABS and ISO 27001. Is the company making use of any of these standards?

We do not follow any security standards in our company. As I indicated earlier, we do not have a big workforce that needs formal security procedures. We believe that the way we do our business it is the right way especially that we believe can drive the company forward.

2. SECURITY TRAINING AND AWARENESS

2.1 How often does the company provide security training to staff members?

Staff members are not provided with training. The company cannot afford to send employees to training. I personally believe that it is useless for small companies to send employees to training and end up losing them to big companies. Big companies are always waiting to pounce and we can't compete with them in terms of salaries.

2.2 What is being done to make sure that new staff members do not compromise the company's information resources?

Nothing much is done except to make employees sign contracts when they join the company. We make it clear to the employees that if they violate the terms of the contracts they will be fired. We know that people tend to sign contracts without reading them. As a company, we encourage employees to read their contracts thoroughly. We once had an incident where an employee allowed a client to use staff computer. The employee was given a warning. There is a reason why we don't allow employees to use staff computers. These computers store sensitive information.

2.3 In the event of a security breach (incident) what are staff members expected to do?

If it is a serious breach then the staff employee can phone an IT expert. If you look at the notice board next to my computer, we have the different numbers of the IT companies that we normally hire to sort out our systems. If the

breach is a minor one, then he or she can report it to the manager who is on duty.

2.4 Are staff members we informed about acceptable and unacceptable usage of the company's information systems (e.g. email and Internet conduct)?

Staff members are well informed about acceptable usage of the company's computers systems. We cannot afford to compromise the sensitive information that we deal with. Clients' information is very sensitive and needs to be protected at all costs.

INFORMATION SECURITY POLICIES

3.1 *What is your company doing to make sure that staff members comply with security policies/rules?*

As I said, they sign contracts when they join the company. We constantly remind them to keep clients' information secure because that is the most sensitive information that we are dealing with.

3.2 How are security policies/rules formulated in the company and how often are they updated?

The managers formed the rules after consulting with the owner. Let me make it clear, our rules are mostly by word of mouth. They are not written. Therefore we do not update them. If there is a need for us to communicate a message to the employees then we do that but mostly we arrange meetings if it is a serious matter.

3.3 *Does the company have any other documentation to guide staff members in connection with information security? If yes, what is it?*

We do not have any other documentation for guiding staff members on the do's and don'ts.

3.4 If the company makes use of anti-virus software, how often is it updated?

Our anti-virus is updated after a year. We have never had a problem with it. May be we should start updating it regularly especially that these days technology changes at an alarming speed.

3.5 If online booking is conducted in your company, what measures have been put in place to make sure that the customer's details are kept secure?

As it is the case with most tourism businesses, we have online booking. First of all, our website states clearly that under no circumstances that we are going to reveal their information to third parties. Staff members are expected to keep the client information secure. As I indicated earlier, staff members sign contracts when they join the company. These contracts state clearly what is expected from them. That is one way of making sure that we do not expose the clients' personal details.

3.6 How frequently must passwords be changed and what complexity requirements do you use?

As I indicated, we do not have passwords. As a company with a few members of staff, we do not see it necessary to introduce the usage of passwords. The company is still growing and as soon as we see it necessary to make use of passwords, then we will introduce them.

3.7 In your opinion, do you think the company's information security policies are in line with its objectives?

I believe our rules are in line with our company's objectives. Businesswise the company has been doing well and I believe that it is partly because of the rules that are in place. Even though we do not have written rules, the company's information resources have been well guarded.

Thank you once again

It is my pleasure

APPENDIX I: INTERVIEW 4

SMME 4 Manager Interview

Good morning sir
Good morning and how are you?

I am very well. Thank you for accepting the invitation to take part in the interview.
It is my pleasure. Hopefully I will be able to answer the questions.

Questions are not too technical.
I don't have a problem with technical questions as I come from the IT background but my worry is that I might not be able to answer some. But you can go ahead

1.1 What percentage of e-commerce applications does your organization use?

Wow! That is a tricky question. What I can say is that we are using most of the applications that are used by hotels. As you know, e-commerce plays an important role in the tourism industry. Most of our clients are from outside the country and in order for them to book accommodation; they must make use of e-commerce. It is difficult for me to put it in percentage.

1.2 What physical access controls are in place to keep desktop computers and other computing devices secure?

We have a number of controls. First of all, we have engaged a security guard company to make sure that our building is secure. Secondly, we have made sure that we desktops are kept in a secure place by the reception area, where there is always someone. As for the laptops, they are personal and we expect staff members to keep them secure. You can't leave a laptop unattended and staff members are aware of this. Most of the thugs are not interested in stealing desktops. They want laptops.

1.2.1 What about credit card fraud?

Credit card fraud is common amongst the hospitality industry, but we have never experienced it. Remember I told you that we have branches in other areas such as Johannesburg and Kruger National Park. But as the Cape Town branch we have never experienced credit card fraud. Our staff members and the IT technicians are doing a great job by making sure that they are very attentive.

1.3 What percentage of your overall budget do you assign to information security (computer security)?

Remember we have branches in other areas as I told you earlier. So it is difficult for me to tell you the exact percentage of the overall budget that we allocate to security. The headquarters in Johannesburg allocates funds to each branch for different purposes. Even though IT is not our core business; the company spends handsomely to make sure that we keep up with the latest developments. Let me put it this way, the headquarters provides enough funds to cater for all out IT needs.

1.4 What kind of security breaches has your company experienced in the past?

As a company that has set high standards, we do not even want to condone virus attacks. We have put some measures in place to make sure that the company does not experience any breaches. We do not want to hurt our reputation by letting security breaches steal the show. Coming to your question, we have never had any security breaches except minor virus attacks. Our laptops are the ones that mostly experience these minor hiccups. Apart from viruses, no breach has taken place in our company.

1.5 How do guard against, detect and report malicious software in your company? For example, how does the company make sure that the computer system and information resources are kept secure?

1.5.1 How do you make sure that these outsiders do not abuse your sensitive information?

We have got a system back up, that backs-up every two hours and it picks up viruses as well. As the people in the management like me as the operations manager, we have a program running in our laptops that we get alerted if there are any viruses in any of the laptops so that we can sort it out as soon as possible.

1.5.1 Lets say a client wants to use a computer and a memory stick.

There is no memory stick used in the computers that are used by clients. They can only use the computers to browse the net; they can't use it for Word. They don't have any applications except to browse the Net and that's it. They can print documents from the Internet though.

1.6 How is data backed up, in other words what is the data backup plan?

Data backup is run on a program and all our data gets backed up every two hours in all the computers and then it is transferred into the external hard drive

at the main offices. Basically our data is backed up at the main offices in Johannesburg. As the Cape Town branch we do not have access to backed-up information. The company wanted to minimize the number of people who have access to backed-up data.

1.7 Do you have procedures in place for recovery of lost data?

We have a gentleman that comes in that does our back-up and double checks and recovers any data that we can recover. We have never had such a problem. We also have three devices that backs-up the data that we have. We plug one device and copy all the files before we plug another one. And we also have the main office in Johannesburg that has got all the data controlled there as well. The name of the one in Johannesburg is called More Hotels. (Laughs) We have got property in Cape Town, Kruger National Park, Madikwe and Johannesburg. Everything happens at the main office in Johannesburg. We have got the central reservation office.

1.8 How are users authenticated into the system?

All the users over here, there are only 8 users that have access to the computers and they have personal passwords and we can track everything that is done during their shifts. So all the Internet usage, everything that they did on the Internet can be traced.

1.*9 What is the company doing to make sure that the employees do not download malicious software from the Internet?*

Our firewall does not allow downloading of files. So users cannot download anything from the Internet Remember we are not a research organisation where users spend most of their time looking for information on the Internet and downloading and saving that information for use at a later stage. Even anti-virus that we use; it is not downloaded from the Internet. Our anti-virus was not purchased on the shelves. We consulted the vendors to make sure that our anti-virus meets our expectations.

1.10 There are some security standards used to help companies with security like SABS and ISO 27001, is the company making use of any of these standards?

We have to. In terms of SABS approved laptops and what we have to have when we do follow it. I mean, everything that we do here must meet certain standards and is monitored and approved. Obviously these standards can help us improve our security goals and avoid losing important information.

1.10.1 Seeing that you have branches in other places, do you have a permanent IT staff member?

We have one consultant that does all our cameras, laptops and our computers. Because we are a hotel, we have got a property management system that runs in all these computers and we have another person that handles that as well. All of them are consultants. So the company that handles our property management system has a single guy that checks on our computers. Because we have only four computers in the whole building, I assume one person is enough.

1.10.2 Can these consultants access the company or the client's information?

No. No. None of them can access sensitive information. Only staff members have access to sensitive information especially people in the management. Actually there are only six of us who can access sensitive information especially credit card information. We try to keep it as limited as possible.

2. SECURITY TRAINING AND AWARENESS

2.1 How often does the company provide security training to staff members?

Training? We do not provide training to our staff members. In terms of computer usage, they are equipped enough to know about the do's and the don'ts. Basically before we hire someone we look at the person background to see what they worked on. We also expect our staff members to be sensible enough to know a few security issues that might pop up within this industry.

2.2 What is being done to make sure that new staff members do not compromise the company's information resources?

I mean we have made it clear that they cannot take anything for granted. We are dealing with sensitive information and they know that. We also have properties in other cities and they can't take anything for granted because our booking system is centralised. That is what they are informed when they come for interviews. It is also stipulated in their contracts.

2.3 In the event of a security breach (incident) what are staff members expected to do?

In each and every shift there is someone from the management or should I say senior staff member. So if it happens that any of the junior staff member, notices that there is breach taking place, they can notify the senior staff

working then he will know what to do. All the people in the management are trained enough to know what to do in a case of a breach.

2.4 Are staff members informed about acceptable and unacceptable usage of the company's information systems (e.g. email and Internet conduct)?

Yes, as I indicated earlier workers are informed during the interviews of the acceptable behaviour. They also sign contracts that also inform them of the acceptable behaviour.

INFORMATION SECURITY POLICIES

3.1 *What is your company doing to make sure that staff members comply with security policies/rules?*

Nothing much is done except to warn them during interviews. We do not have policies but rather have rules. Even though most of our rules are not written down, staff members are well aware of them. A few of them are written down but the contracts that the employees signed when they joined the company are important because employees know what is expected of them.

3.2 How are security policies/rules formulated in the company and how often are they updated?

Management came up with our security rules. They consulted the IT consultants and the employees were made aware. Most of the rules were formed by the headquarters. In most cases they consult with other branches before coming up with new rules. Our rules are standard throughout all the branches.

3.3 *Does the company have any other documentation to guide staff members in connection with information security? If yes, what is it?*

We do not have any documentation to be signed by the employees except the contracts that are signed when they sign after the interviews. We believe that contracts are enough to persuade employees to not abuse the company's information systems. Once in a while, we speak to the employees reminding them about importance of keeping information secure.

3.4 If the company makes use of anti-virus software, how often is it updated?

Our antivirus is updated on a monthly basis. As I indicated earlier, we have an IT guy who takes care of our property management system. He visits us on a weekly basis to check if our systems are running well. He will then check the

antivirus and scan all the computers for viruses. So far we have never had any problems. Let me put it this way, ever since I joined the hotel, we have never experienced a serious breach as a result of viruses.

3.5 If online booking is conducted in your company, what measures have been put in place to make sure that the customer's details are kept secure?

As you know to effectively compete in the hospitality industry, you must make use of modern technology. We are not exempted from this and most of our guests make use of online booking system. We have made sure that our systems are secure. Staff members are advised to be vigilant whenever they are helping a client with online booking. We have also minimized the number of staff members who can access credit card information. The other thing that the company is doing is encouraging staff members to report any suspicious transactions to make sure that they attended to early.

3.6 How frequently must passwords be changed and what complexity requirements do you use?

As for the password, we do not have any password policy. Staff members can use the password for as long as they want. We have made it clear to them to them that a password is personal and should be treated as such. They know that they must keep the passwords secure.

Thank you for availing yourself for this interview.
It is my pleasure, I wish you