UNIVERSITY OF ZIMBABWE

GRADUATE SCHOOL OF MANAGEMENT

AN ASSESSMENT OF THE EFFECTIVENESS OF E-BANKING SECURITY STRATEGIES IN ZIMBABWE: THE CASE STUDY OF STANBIC BANK ZIMBABWE.

MINMORE CHIGARO

R113076M

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF BUSINESS ADMINSTRATION

SUPERVISED BY: DR D. MARAVANYIKA

AUGUST 2014

Dedication

This dissertation is dedicated to my workmates and my family members for their love support and time sacrificed during the research period. To Stanbic Bank Zimbabwe I hope this study will contribute to the prudent adoption of e-banking security strategies.

Declaration

I .....do hereby declare that this dissertation is a result of my own work investigation and research, except to the extent indicated in the acknowledgements, references and comments included in the body of the report, and that it has not been submitted in part or in full for any other degree to any other university.

.....	.....
Student Signature	Date
.....	.....
Supervisor Signature	Date

Acknowledgements

I would like to first acknowledge my supervisor, Dr Maravanyika for the continued support and guidance during my research. His boldness in getting what needs to be done was extremely amazing. I would also like to thank my work colleagues for the favour and understanding during the weekends sometimes when I was supposed to be at work and school.

I would like to thank my family, especially my son Mukundi and my husband Vitalis Kereke for they endured my prolonged absence from their lives because of my pursuit of the MBA degree.

Moreover I wish to thank University of Zimbabwe Graduate School of management for the useful information and knowledge that I acquired during the MBA programme. Lastly I would like to thank all management and staff of Stanbic Bank Zimbabwe who were respondents in the face to face interviews that I conducted as part of my data collection.

Abstract

The general direction of literature is that effective e-banking security strategies result in improved organisational performance by increasing market share through building customer's trust and confidence in the privacy and confidentiality of the services provided. It is quite important to note that this research aims at assessing the effectiveness of e-banking security strategies in use in a Zimbabwean organisation, thus after the literature review on e-banking had been confined to other parts of the world.The study is hoped to fulfill academic gaps in terms of literature on the subject in Zimbabwe and to research information to benefit the corporate world. This research was based on a single case study design of the Stanbic Bank.

In carrying out the study, the researcher used personal interviews and the audience group included Chief Executive, Finance Director, Head IT, five unit managers and two unit officers. Furthermore the research was elaborated using the qualitative philosophy whilst data displays in form of content analytic summary tables were used to analyse primary data gathered. Moreover gathering depth information from the respondents was done through the use of unstructured questions.

The study concludes that Stanbic bank is using effective e-banking security strategies and is constantly researching on more effective security strategies with the aim of eradicating fraud. The organization faced challenges on implementation emanating from the lack of finance and skills. The other obstacles were the legal issues surrounding regulation of adopting the strategies before implementation and misinterpretations of security messages due to lack of communication. In view of these findings this study recommends that Stanbic bank should send its employees for education and training on e-banking security so that they acquire necessary skills and expertise. It is also recommended that the organization should invest in continuous research and development on up to date e-banking security and ensure that relevant infrastructure is a prerequisite for the successful implementation of security strategies.

Table of contents

Chapter 5 : Conclusions and Recommendations

List of tables

Table description

List of figures

Description

List of Abbreviations

Description

1. ATMs : Automated Teller Machines
2. IT : Information Technology
3. E-banking : Electronic Banking
4. GEFs : Group Enabling Functions
5. SSL : Security Socket Layer

Chapter 1: Introduction and Background

1.0 Introduction

Electronic banking is transforming the financial services industry through numerous impossible innovations of modern technology. E-banking uses particularly information technology to generate, collect and process information about bank operation and bank customers efficiently and effectively. Results and findings on European countries shows that ownership of diverse financial products and services, attitudes towards finances and trust in the electronic banking influence the usage of the application as posed by Guerrero et al. (2007). Electronic banking offers many benefits to banks and their customers. Enhancement of bank's reputation, better customer service, cost savings and efficiency are the main benefits to banks as Brogdon (1999) and Jayewardene et al 2000 highlighted. Thus the more transactions can be converted online, the more money will be saved. Robinson (2000) echoed that costs were less if done on line than the traditional banking through branch banking. It has been argued that electronic banking customers are more valuable to banks than other customers with similar demographics. Burns (2000) indicates that flexibility and opportunity for better service will replace other delivery channels.

The greatest challenge to the electronic banking security as literature reviewed in numerous studies will be winning the trust of consumer in issues of security and confidentiality as posed by Range et al (1997) Funnel et al (1999) and Be Stavros (2000). The growth in the usage of electronic delivery channels such as mobile banking and the internet indicates that Zimbabwe has also been part of the worldwide trend into the use of advanced technology. However less work has been done in Zimbabwe with regard to electronic banking security issues. The present study aims to assess the effectiveness of e-banking security strategies in Zimbabwe through a case study of the Stanbic Bank in Zimbabwe for period 2010 to 2013.

1.1.1 Industry analysis

Reserve Bank of Zimbabwe Act (Chapter 22:15) regulates and monitor the banking sector in Zimbabwe .The Central Bank regulates the sector through enforcing various pieces of legislation such as Banking Act (Chapter 24:20) and Bank Use Promotion. The Minister of Finance also regulates the sector by issuing guidelines from time to time which contains macro and micro policy statements that banks need to follow to stay within the expected conditions. The Banking sector is made up of the eighteen commercial banks, two merchant banks, four building societies and one savings bank as at 31 January 2014.

In recent years electronic banking security is a topic that has taken centre stage in banks and other financial institutions. It continues to provoke debate among academics because of its continued relevance to the present prevailing situations the in the world over. The issue of stability through systemic impulses in the Zimbabwean Banking Industry has shown that it is highly exposed to risks and uncertainties as IMF (2013) commented. The Zimbabwean banking industry has been characterized by serious challenges in the form of unanticipated policy shifts high staff costs, a poor deposit base, and an unfavourable country risk profile that makes it extremely difficult to source international credit lines since year 2003 due to high inflationary figures. All these challenges affected every individual bank's profitability threatening its existence hence some banks lost their licenses through industry clean-up efforts by the Reserve Bank of Zimbabwe while some were technically competed out of business for instance Royal bank.

The introduction of multi-currency system in February 2009 came with a new wave to the industry's competitive landscape as banks tried to strike a balance between cost of offering services, profitability and change of models to suit the new system. Stanbic Bank Zimbabwe is never spared in this challenge and all strategies now need to focus around improving profitability of all banking business. Among several strategies to achieve sustainable profitability there is need to invest in technology and acquire expertise in information technology security thus a critical approach towards achievement of organization's objectives.

Kannabiran et al, (2005) adds on that information technology helps banks to improve business efficiency, service quality and attract new customers. In Zimbabwe the first visible form of electronic innovation was through introduction of Automated teller

machines (ATMs) by Standard Chartered bank and Central Africa Building Society in the early 1990s. Furthermore other forms of electronic innovations that have found their way into Zimbabwean banks are Electronic Funds Transfer Systems, Mobile banking, Personal Computer banking and recently internet banking. Chang, (2003), Sullivan and Wang, (2005) notes that these electronic innovations have released banks from the constraints of time and geographical location and has allowed banks to cut costs on transactions, improve their service delivery, and respond better to the demands of the market

However financial challenges in the Zimbabwean banking sector have slowed the adoption of these electronic banking strategies despite the convenience it brings to the customers and the banks. While literature is abounding with studies conducted mostly all over the world, in the Zimbabwean context this area is underrepresented as no studies to the best knowledge of the authors have been conducted in this area. It is against this background that this study undertakes to assess the effectiveness of e-banking security strategies in Zimbabwe through a case study of Stanbic Bank.

1.1.2 Background to the case study organization

Stanbic Bank Zimbabwe is a wholly owned subsidiary of Standard Bank Africa and is listed on Johannesburg Securities Exchange. In November 1992, Standard Bank South Africa's banking group acquired the operations of ANZ Grindlays Zimbabwe which was then renamed to Stanbic Bank Zimbabwe Ltd in 1993.The Standard Bank Group is one of the leading banking and financial services group in Africa proving a broad range of Corporate and Investment banking, personal and business banking products and services. In Zimbabwe Stanbic bank has eighteen branches and its head office is located in Harare.

The Bank's Vision

All its activities in the market are heavily guided over a long foreseeable future by its vision. According to Stanbic Bank Zimbabwe annual report (2013), the bank's vision statement states that it aspires to be a leading emerging markets financial services organization.

Mission Statement

Pearce & Robison (2006) emphasise that mission statement ensures unanimity of purpose and is the organization's tie post. He went on to mention that a mission statement provides a basis for organizational resource allocation and helps specify organizational purposes and their translation into goals and objectives. Stanbic bank Zimbabwe is also guided by a strong mission statement which states that the bank is committed to making a real difference to financial services in Zimbabwe by providing banking technologies and products to enhance customer service delivery.

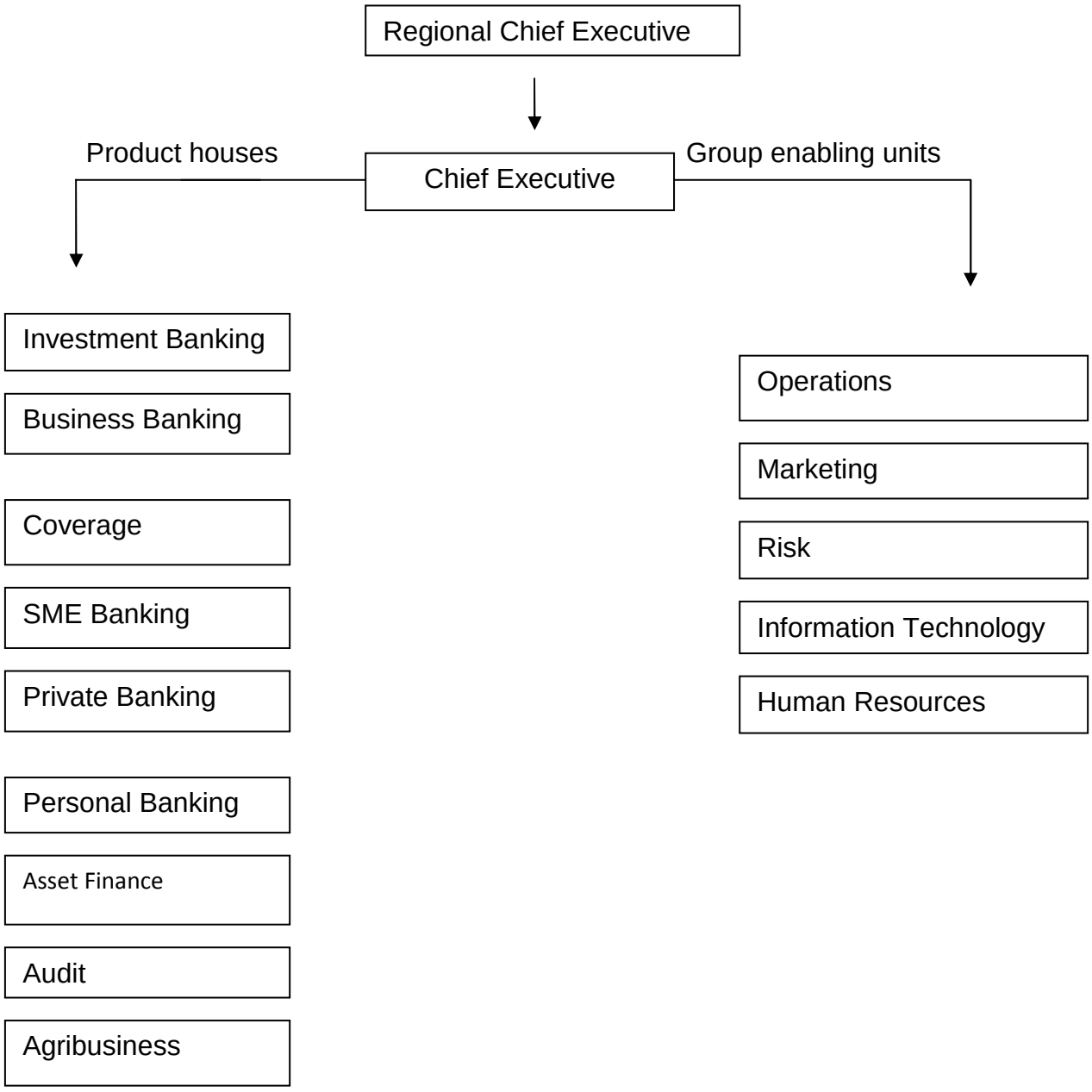
Values

- Delivering to shareholders
- Developing and growing people
- Serving customers
- Upholding highest levels of integrity

Organisational Structure

Stanbic Bank Zimbabwe departments are divided into two main categories by functions, namely Group Enabling Functions (GEFs) and Business Units. Group Enabling Functions are departments that are not core to the banking business and are not directly connected to business activities and the market. Their purpose is to assist core departments to execute their business activities on a daily basis. Core Business Units are departments of the bank that are directly linked to the main functions of the bank that generates and contribute to total revenue for the bank. They are also called product houses because they are responsible for management and offering special products to the market for a profit and these profits are expected to outweigh costs associated with Group Enabling Functions for the whole bank to attain a net profit position. All departments report in to the office of the Chief Executive.

Figure 1 Stanbic Bank Zimbabwe Departments by Function



Source: Stanbic Bank Zimbabwe Human Resources Report, 2011

In the first half of 2013 alone, Stanbic Bank has witnessed an alarming increase in the number of theft and fraud cases. A random sample of the reported cases indicates that the crime has been perpetrated through various means such as;

a) Armed robberies

b) Internal frauds (staff)

c) External frauds

Undoubtedly, the bank has made great strides in terms of investing substantial amounts of their profits into, internal policies and procedures in an effort to minimize occurrences of financial crime as well as to ensure that there is a clear segregation of duties and that the maker checker concept is well defined. Vast resources have been poured into acquisition of CCTV cameras which has enhanced surveillance to all bank corridors, vaults, customer areas and other vulnerable areas. The same measures have also been introduced to all high risk areas in the banks in an effort to combat financial crime.

Despite all these interventions, Stanbic bank sector has witnessed an alarming increase in the number of theft and fraud taking place. The Reserve Bank of Zimbabwe attributes these revenue leakages through theft and fraud to lack of sound risk based conceptual frameworks within the sector hence the strong insistence to Basel 3 implementation.

According to the Interbank Security Liaison Committee meeting minutes of January 2013, between the period extending from April 2011 and October 2011, a total of thirty five accused persons applied to open accounts with the Bank at various branches countrywide and fraudulently applied for loans for varying amounts totalling US$ 247 900.00. The fraudsters took advantage of the Bank which had a facility to its customers to access unsecured personal loans that were based on customers' salaries. The fabricated loans were credited to the accounts that the customers had with the Bank. The accused persons succeeded in obtaining the said loans, through use of fake payslips and utility bills. The cases were reported to CID Serious Frauds and this is a classic example of a fraud perpetrated with the knowledge of staff members who knows that there are security loopholes in the systems. In this regard, this study has found it necessary to conduct a research on the effectiveness of e-banking security strategies in Stanbic bank Zimbabwe. In essence, the researcher

seeks to understand whether security strategies deployed are serving any real purpose or is actually abating financial crime.

1.2 Problem statement

Enos (2000) postulated that banks must make sure that the systems are well integrated and more convenient to the customer. Factors such as are improving customer trust and integrating the current services offered to the customer in the new system should be considered in building up a secure transaction system.

The introduction of E-Banking has come with its challenges and this range from technology adoption, financial limitations, and lack of expertise. Moreover Masocha, (2010) added on that other implementation challenges experienced globally are the increase in security fears, cultural barriers, limited internet access and legal issues. Auta (2010) found that security, user friendly, queue management, accessibility, time factor and fund transfer are major factors in the adoption of e-banking and that security is rated as the most important issue of online banking services.

Security is constantly highlighted as a critical success factor for the success of e-banking. Shah et al, 2012 notes that the inadequacy of security potentially leads to financial losses, punitive measures by regulators and negative media publicity therefore its importance cannot be over emphasised. In e-banking, fraud is a major contributory factor to the term security and needs to me managed closely. Roberds (1998) pointed e-banking fraud for instance as situations when transactions are made anonymously or at point of sale, when claims cannot be effectively verified at the point of sale and when issuers of payment claims bear the costs of fraudulent transactions.

In 2013, most of the fraud cases were perpetuated via electronic banking systems therefore reflecting weaknesses in the internal control systems. Security in the form of keeping customer safe from an invasion of their privacy, affects trust and satisfaction. Customers prioritise privacy and confidentiality hence influenced by the imagination-capturing stories of hackers, they may fear that an unauthorized party will gain access to their online account and serious financial implications will follow. Moreover insecurity has posed a sit back in e-banking as people fear their bank

accounts and transactions being are tampered with. These unfavourable familiarities have deterred some people from adopting internet banking.

The common e-banking security strategies that are currently in place include, use of passwords and encryption of sensitive data which has brought up several vulnerabilities to both the banks and their clients. The research problem is therefore to assess the effectiveness of e-banking security strategies at Stanbic bank and make recommendations that will result in Stanbic bank gaining competitive edge over its rivalries and building customer trust in line with literature.

1.3 Research objectives

The main objective of this study is to find out the effectiveness of the e-banking security strategies through a case study of Stanbic Bank Zimbabwe. This study seeks to achieve the following objectives:

1. To find out the e-banking security strategies used by Stanbic Bank Zimbabwe.
2. To determine the benefits of effective e-banking security strategies.
3. To evaluate the attributes that is used to measure the effectiveness of e-banking security strategies.
4. To investigate the challenges faced by Stanbic Bank Zimbabwe in implementing e-banking security strategies.
5. To give recommendations on the way forward to improve the evaluated e-banking security strategies.

1.4 Research questions

1. Is Stanbic Bank using effective e-banking security strategies?
2. What e-banking security strategies are used by Stanbic Bank Zimbabwe?
3. What attributes are used to measure the effectiveness of e-banking security strategies?
4. What challenges are faced by Stanbic Bank Zimbabwe in implementing e-banking security strategies?
5. What recommendations can be drawn from the study?

1.5 Research proposition

The limited effectiveness of electronic banking security strategies in Zimbabwe is due to inadequate investment in technology and the relatively low levels of skills.

1.6 Justification of research

This study is important in many ways. The study is aimed at providing the best security strategies for Stanbic Bank Zimbabwe that are timely compatible with technological trends so as to minimize computer threats. The study will also provide a basis for understanding and anticipating responses by employees to e-banking security risks facing the Stanbic bank Zimbabwe. It is also hoped that this study will cultivate increased usage of e-banking services by clients and equip the researcher with the knowledge on importance of electronic banking security strategies. This study will contribute to the fulfilment of academic gaps in terms of literature on the subject in Zimbabwe. In addition, the study will assist regulatory bodies such as the Reserve Bank of Zimbabwe to lower e-banking charges as a way of improving usage by clients. The study should also assist commercial banks in Zimbabwe in managing risk and boosting confidence of the customers hence increased capabilities of the banks.

1.7 Scope of the research

This research is confined to Stanbic Bank Zimbabwe and may not be generalised for other financial institutions.

1.8 Limitations of the research

Banks by their very nature are sensitive institutions and information pertaining to their operations does not freely flow. Section 76 of the Banking Act (Chapter 24:20) provides that it shall be an offence for anyone to disclose information acquired in the performance of functions under Act. The common law further provides that under the banker to customer relationship concept, no one party can disclose information without the consent of the other. Suffice to say, bank information is confidential and can only be released under strict exceptions allowed at law. Information gathered is limited to those accesses and made available by the respondents. However, to ensure that the results of this research are valid the limitations will be reduced.

1.9 Structure of the Research

Chapter 1

This chapter covers: the background to the study, the problem statement, research objectives, research questions, research proposition, and justification of research, delimitation of research and limitations of the study.

Chapter 2

The chapter details a critical review of the relevant literature on e-banking security

Chapter 3

The chapter outlines the research methods that the researcher used to collect, classify, and present data in the study. These includes research design, study population, sampling techniques, data collection tools and methods, data analysis, validity and reliability of the research.

Chapter 4

The chapter looks at the research findings that feed into conclusions. These discussions are closely linked to literature discussed in the previous chapter (chapter two). Research findings are also presented and critically analysed to allow for inductive conclusions

Chapter 5

This is made up of conclusions and recommendations made to the benefit of Stanbic Bank Zimbabwe management and the academic world.

1.10 Chapter conclusion

This chapter has set the tone for the study. It has pointed out that electronic banking security is constantly highlighted as a critical success factor for the success of E-Banking. The Stanbic bank Zimbabwe is not an exception since it is has most of the fraud cases that are perpetuated via electronic banking systems such as the ATMs. In order to develop effective security strategies, Stanbic bank needs to evaluate the attributes that are used to measure the effectiveness of e-banking security strategies.The study will look at the e-banking security strategies used by Stanbic Bank Zimbabwe; determine the impact of e-banking security strategies on different integrated core banking systems and the challenges faced by Stanbic Bank Zimbabwe in implementing e-banking security strategies.

Chapter 2: Literature Review

2.0 Introduction

In this chapter, the researcher looks at the definitions of e-banking, presents the main security concerns and threats that are driving the need for sound security. This chapter provides detailed analysis of the many e-banking security strategies, as well as a set of guidelines for selecting and implementing enhanced authentication, based on the learning and knowledge of industry experts and the consumer.

2.1 Definition of e-banking

Vilattes (1997) defines e-banking as a distance banking that not only handles the flow of information between customers and the physical facilities of the bank, but also deals with solicitation, sales, distribution and access to services, all without requiring the customer and the financial institution representative to be in the same physical place at the same time.

According to Sarel and Mamorstein (2003) e-banking is beneficial to both banks and their customers. E-banking has helped banks to reduce costs through the reduction of manual opertions and use of self-service automated teller machines; resulting in increasing sales performance (Grabner-Kraeuter and Faullant, 2008).Vatanasombut et al, (2008), observe advised that the development of trust can help reduce the effect of key inhibitors to online service among non-e-banking customers.

2.2 E -banking security and threats

Ganesan and Vivekanandan, (2009) postulated that internet has continued to provide services to customers in a convenient manner through a multipurpose platform for business. They went on to say that internet based solutions have transformed the revolutionary approach of how business is done electronically. Furthermore they found out that electronic banking has endowed banks to improve profitability through information communication technology adoption. In contrary however, they noted that this good success has also come with challenges.

Furthermore, other scholars who include Egwali et al echoed that several threats come from spoofing, identity theft, phishing scams and larcency. They added that to disclose confidential information techniques such as an amalgamation of social

engineering and Web site spoofing can be used to hoax a user into revealing the. Landwehr et al (2002) echoed that all commercial operating systems have weaknesses in their computer systems. He added on explaining that information stored on commercial operating systems can create opportunities for possible threats such as theft on the bank's transactions. Loch et al (2003) noted that security threats as fraudsters' risker as compared with external threats such as hackers and cyber criminals, Mccrohan (2003).Moreover DÁrchy et al (2009) reported that between fifty and seventy percent of all security related incidents from within the organisation and outside incidents poses fewer issues.

Leach(2003) emphasised that threats comprises both non deliberate and deliberate acts by the users .He postulated that security awareness and training is usually used by managers to address deliberate and non-deliberate acts by users. In addition to that he suggested that employees have a tendency of not following security policies and procedures in place. Kajava, (1998) suggested that people respond both positively and negatively to set policies and procedures with some cooperating and others resisting. Leach, (20003) argued that security incidents suffered by a company can be significantly attributed to poor behaviours by its users. Thus, the findings are that security audits should regularly be performed to ensure employees are following proper policies and procedures. Opplger (2003) stressed that while effective external threats are as common as internal threats they do pose a significantly different challenge. Moreover security measures must be accounted for even though natural disasters might seem insignificant. He raised the issue that the organisation need to have disaster site where in the event that natural disaster was to occur it would recover any lost data. It further argued that a company's image can be damaged by negative media coverage resulting from accidental leaks of information. Moreover he suggested that identifying the likely threats the first step towards safeguarding organisations information. Thus once a threat investigation has been completed the organisation can then set its goal to develop counter measures against the threats. He pointed out that ways to combat threats exist and these are functions that eliminate weaknesses in the system. The next section discusses these counter measures and gives more information about security

strategies that are deployed to ensure confidentiality, intergrity and availability of information.

2.3 E-banking security strategies

Hawkins et al (2000) stated that, securing security mechanisms such as Socket Layers (SSL), encryption of data, digital certificates and passwords are used by most financial institutions and banks. Banks are constantly introducing new security measures with the aim of eradicating e-banking fraud. Subsequently, there is still need for research to narrow down on specific areas for enhancement. The common use of the same passwords for authentication increases the exposure whenever such information is stolen. Thus, an additional security measure is required to confirm the identity (Robert Moskovitch et al, 2009). Given that conventional methods of authentication via usernames and passwords are no longer sufficient (Vandommele, 2010), points out that to improve security biometric technology can be used.

Ally and Toleman ,(2005) indicated similar comments that each security mechanism implemented strives to clear security goals such as confidentiality and integrity, security socket layer (ssl) is another noble mechanism used in e-banking security

In addition to that Clessens et al (2002) pointed out that in order to improve the overall security of the electronic banking systems, mechanisms, such as passwords must be implemented to ensure safety. Researcher like Aburrous et al (2000) stressed that security socket layer is one security mechanism that is used in the electronic banking security. Moreover Ganesan and Vivekanandan (2009) proposed a secured hybrid architecture model for the electronic banking using Hyper elliptic curve cryptosystem and MD5 apart from foregoing security strategies. Several security strategies that include virtual keyboards, device registering and transaction monitoring were discussed in a study in Brazil carried out by Peotta et al (2011).

2.4 E- Banking security measures

Sensitive corporate information, which includes customer data, financials and corporate strategy, can be protected through precautionary measures Barlas et al (2007). Oppliger (2003) discussed security policy, host security, network security, organizational security and legal security as aspects that should be considered in security. He argues that security aspects must be managed collectively rather than individually.

2.4.1 Network security

It refers to the integration of security such as security policies, host security, organizational security and legal security Oppliger, (2007). He added that a security policy goes the simple idea .It is very complex and is meant to govern data access, web- browsing habits, encryption and more. Hiring hackers, changing passwords oftenly, keeping the network free from viruses and deploying patches have been provided by Newhouse (2007) as some of the resolutions to build a secured network. Green, et al, (2007) recommended the hiring of hackers as very useful as they use creative techniques to infiltrate the system, since no system is completely hack proof. He further advocated found the use of strong passwords, deploying patches and updates as other actions that could be considered in increasing security on network as these are pro-active (ensures that weaknesses are encountered for as they are discovered).

2.4.2 Organizational security

Winkler and Dealy, (1995)suggested that it is of much rationale for the organisations to train users and make them aware of policies, procedures to combat possible threats on e-banking pointed out users as the biggest threats to e-banking. Given that security awareness is the weakest link in information security, factors such as organizational, socio political, institutional education and computer ethical have been identified by Siponen (2001) as dimensions of security.

The socio political dimension is the security awareness training that is required by the law. The general public dimension entails us all users outside of the information technology department. The organisational dimension consists of various groups of people within the organisation that security awareness training should target,

2.4.3 Legal security

It is important to ensure that those who breach the e-banking security [for example, hackers] are prosecuted so that threats are minimised. (www.arraydev.com/commerce)(Accessed 12/06/14). It is further argued that an organisation can reduce potential threats by having penalties in place. Moreover this legal security should be derived from the security policy that is implemented within organization, addressing all the aspects of security thus all stakeholders associated with the organization should be made aware of security policies and consequences.

2.4 E-banking security implementation issues

The Economist (1999) recounts that e-banking potentially expose hitherto isolated systems to open and risky environments. In addition security breaches have serious financial, legal and reputational implications and they fundamentally fall into three categories that are breaches with serious criminal intent, breaches by hackers and flaws in systems design.

Furthermore, other challenges in implementation spans from technology selection, adoption, and lack of knowledge. In addition Earl, (2002) furthermore identified that while managers naturally often lack employees with the experience and skills necessary to adopt software technologies and educate customers although they have a high-level understanding of their business and operational processes.

Infrastructure - Taddesse & Kidan, 2005 postulated that infrastructure is necessary for the successful implementation of security strategies. It is a prerequisite to have components such as the internet, hardware specifications that are up to date and operations.

- **Regulatory and legal issues -** National, regional or international set of laws, rules and other regulations are important requirements for the successful implementation of e-banking security schemes.
- **Socio-Cultural challenges** - According to Taddesse & Kidan (2005), difference in the degree of the required security and efficiency among people of different cultures and level of development aggravates the problem. Consumer's confidence and trust in the traditional payments system has made customers less likely to adopt new technologies.

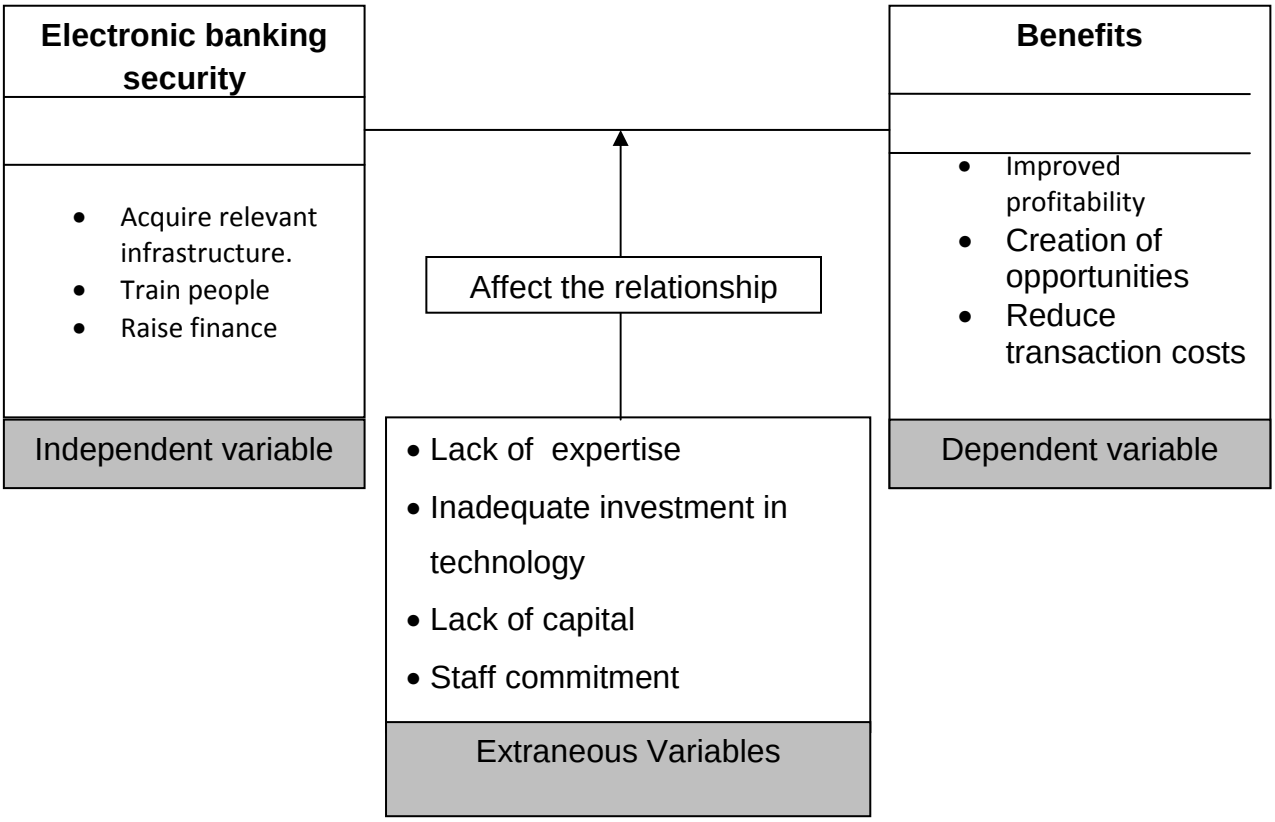
- **Lack of knowledge and skills** – companies often face challenges of implementing up to date security strategies due to employees that do not have necessary skills and knowledge hence prompting the institutions to hire where necessary.

2.5 Conceptual framework

The researcher proposed a slightly different analytical framework for the e-banking security strategies. The relationship is explained as follows: variables such as inadequate investment in technology, lack of expertise and lack of capital affects the e-banking security strategies that a bank adopts.

Conceptual framework

Figure 2



Source: Adapted from Kumar (2011)

2.6 Chapter conclusion

This chapter has discussed the electronic banking security strategies that banks are using, the challenges faced in implementing these strategies , the benefits of employing sound secured systems and measures that can be taken to combat fraud and threats. Finally the chapter concluded with an analytical framework, which inadequate investment in technology and lack of skills at the centre of the e-banking security strategies.

CHAPTER 3: Research methodology

3.1 Introduction

This chapter is divided into the following sections: research design, philosophy, strategy, data collection and data analysis. The first section defines the research design concept. This is followed by selection and justification of the research philosophy employed for the study. The third section section will explain why it was found appropriate to employ the case study research approach. The section on data collection describes the study population, sampling strategy and research instruments that were used. Finally the chapter ends with a brief account on how data was analysed.

3.2 Research design

According to Brink (1997), a research design is a framework or a detailed blueprint that can be used to guide a research project towards its objectives. One of the most significant decisions in a research project is the choice of the research design because this determines how the information for the project will be obtained. The researcher used a single case study design of Stanbic Bank. Yin (2003) argues that one of the five rationales for a single case is when a case is representative or typical. The Stanbic Bank is a representative of commercial banks in the Zimbabwean banking industry in terms of branch network and number of employees. The results of the research are applicable to other commercial banks which operate under similar government regulations, financial institutions and may also extend to other organisations operating in the banking industry in Zimbabwe.

3.3 Research philosophy

According to Saunders, et al (2009) there are different views about the way in which knowledge is developed. The two major philosophical schools of thought that have dominated literature on the research process are positivism and phenomenology.

Positivism (quantitative approach)

Positivism as a philosophy adheres to the view that only “factual” knowledge gained through observation (the senses), including measurement, is trustworthy. In positivism studies the role of the researcher is limited to data collection and

interpretation through objective approach and the research findings are usually observable and quantifiable. According to the principles of positivism, it depends on quantifiable observations that lead themselves to statistical analysis.it has been noted that “as a philosophy, positivism is in accordance with the empiricist view that knowledge stems from human experience”. It has an atomistic, ontological view of the world as compromising discrete, observable elements and events that interact in an observable, determined and regular manner”,(Collins,2010).

Phenomenological (qualitative approach)

Creswell, (2009) defined qualitative research as a means of exploring and understanding the meaning of individuals or groups ascribe to a social or human problem and this means that the process involves emerging questions and procedures, data typically collected in the participants setting, data inductively building from particulars to general themes and the researcher making interpretations of the meaning of data. Hussey (1997) alluded that qualitative research (phenomenological approach) is subjective in its approach of examining and reflecting on perceptions of understanding social and human activities. In addition to that, Bryan (2004) echoed that the qualitative research approach embodies a view of social reality as a constantly shifting emergent property of individuals’ creation. In carrying out the research the researcher shared similar views with the above mentioned authors, as the intention was to critically investigate and analyse specific research questions through the use of a qualitative approach.

3.4 Research strategy

According to Saunders et al, (2007), there are seven different strategies that can be used for research and these include:

- Case study
- Ethnography
- Archival research
- Grounded theory
- Action research

- Surveys
- Experiment

He further echoed that each of these strategies has peculiar pros and cons depending on the three conditions namely the type of research, the extent of control that the investigator has over actual behavioural events and the focus on contemporary as opposed to historical phenomena.

In light of the nature of this study as described in chapter 1, the case study approach was found to be the most appropriate strategy. According to Yin (2003) the case study approach is used when the investigation is aimed at answering 'how' or 'why' questions about contemporary events over which the researcher has little or no control. The present study was conducted to establish how or why Stanbic bank implemented its e-banking security strategies.

3.5.1 Advantages of case study

Apparently there are a number of merits and demerits of using the case study approach. Data is examined within the natural setting of the investigation (Yin, 2003). Yin (1984) also noted that researchers should not confuse case studies with qualitative research, he emphasised that case studies can be based entirely on quantitative evidence. Block and Hosenfeld (1986) argued that variations in terms of intrinsic, instrumental and collective approaches to case studies allows for both quantitative and qualitative analysis of data

Punch (1998) has noted, case studies play a major role in training in the fields of business, law and medicine. He states that this is possible because cases are not totally unique. There is therefore transferability of knowledge from case to case.

3.5.2 Disadvantages of case study

Critics of the case study believe that, case studies fail to establish reliability or generality of findings. Some writers also say that the case approach can result in biased findings. Robert et al (2000) dismissed the view that case study research is only useful as an exploratory tool. Yet some researchers continue to use case study research method with successions carefully planned and crafted studies of real life

situations, issues, and problems. Yin (2003) has also pointed out that for case studies what is important is analytic and not statistical generalisation. Further, Punch (2000) states that if cases were not generalizable they would not be used successfully in such the fields as law and medicine. It was against this background that this study employed the case study approach.

3.6 Data collection

3.6.1 Population

Polit and Hungler (1999) refer to the population as an aggregate or totality of all the objects, subjects or members that conform to a set of specifications. In this research the population constituted the Stanbic bank management and staff.

3.6.2 Sampling Strategy

A basic choice in formulating the approach to data sampling exists between probability sampling and non-probability sampling. In light the qualitative philosophy cited above and the problem statement in Chapter 1, non-probability data sampling strategy appropriate for the present study.

3.6.2.1 Non probability sampling methods

- Judgement or purposive sampling

This study employed purposive sampling as recommended by Saunders et al (2009). These writers state that purposive sampling allows the researcher to select only those respondents that are best able to answer the study questions. In line with this recommendation the researcher interviewed relevant Stanbic senior management and key personnel in the IT department. The former respondent category set strategy and the latter implements.

3.7 Data collection methods

Yin (2009) stated that properly conducted case study benefits from having multiple sources of evidence, which ensure that the study is as robust as possible. Prasad, (2005) mentioned that the concept of methods refers in general to the appropriate use of techniques of data collection and analysis

The researcher used both primary data and secondary data in carryout this research, with primary data being obtained through the use of personal interviews while secondary data being obtained through financial annual reports at Stanbic bank.

3.7.0 Research instruments

3.7.1. Semi structured questionnaires

Collins and Hussey (2003), defines a questionnaire as a collection of decisively structured questions, chosen after considerable testing, with an aim of gathering reliable responses from a selected sample. Saunders et al. (2000) proposed that questionnaires are an efficient way of collecting responses from a large sample because each person answers the same set of questions.

Saunders, et al (2009) echoed that prior to using the questionnaire to gather data it should be 'pilot tested' .The same was done with Stanbic staff and management so as to enable the researcher to obtain feedback on the questions asked. The questions asked can be structured, semi-structured or unstructured. According to Aslant and Dill man, (1994), the use of semi-structured questionnaires has the following advantages and disadvantages:

3.7.1.1 Advantages of semi-structured questionnaires

Oppenheim, (1992) stated that advantages for semi-structured questioning include freedom and spontaneity of answers, opportunity to probe and usefulness for testing awareness. For example, after a respondent has given an answer to a question, a follow up question can be asked to get clarification.

3.7.1.2 Disadvantages of semi-structured questionnaires

Payne (1951) posed that, questionnaires do not provide an opportunity for the researcher to clarify questions, verify that answers are understood, seek clarification or elaboration of answers or ensure that the respondent answers all questions on the form. However, despite these disadvantages, there is more merit in using semi-structured questionnaires in this type of study.

3.7.2. Personal interviews

Collis and Hussey, (2003) noted that interviews which can be used for both positivist and phenomenological methodologies are a data collection method in which selected participants are asked questions about what they do, feel and think about the subject matter. The strengths of interviews are the process of open discovery. The use of interviews in this research was significant to obtain in-depth information about e-banking security strategies. An interview guide with semi-structured and open-ended questions was employed. The interview guide was pre-tested before use in order to establish usability. In all cases, the face-to-face interviews were conducted.

3.7.2.1 Advantages of personal interviews

Within, et al (1995) postulated the following as advantages of personal interviews. One of the main reasons why researchers achieve good response rates through this method is the face-to-face nature of the personal interviews. Unlike administering questionnaires, people are more likely to readily answer live questions about the subject simply because they can concentrate as they are part of the sample.

If you wish to probe the answers of the respondents, open-ended questions are more tolerated through interviews due to the fact that the respondents would be more convenient at expressing their long answers orally than in writing. In addition the researcher can benefit a greater opportunity to observe the attitude and behaviour of the respondents as interviewing progresses.

3.7.2.2 Disadvantages of personal interviews

Personal interview is a costly method of data collection as the interviewer is required to be paid travelling and daily allowances. In addition, limited numbers of interviews are possible within one day by an interviewer.

The information supplied by the respondents may not necessarily be accurate as they have to supply information on the spot. The answers given by the respondents may not be fully supported by facts. The respondent may give inadequate information due to personal reasons. This is likely to affect the final outcome of the survey. The interview time may be of 15 to 30 minutes but the interviewer has to

spend time for example on travelling thus takes a longer duration hence time consuming.

Source - http://ppa.aces.uiuc.edu/pdf_files/Conducting1.PDF (accessed on 03/07/2014)

3.8 Data analysis

According to Neuman (2006), unlike quantitative research there is no standard format for analysing qualitative studies. In view of this, in the present study data was analysed in line with the recommendation of Miles and Hurberman (1994). This entailed the use of Data Displays and detailed write-ups

3.9 Chapter conclusion

This study employed: the single case design, a phenomenological philosophy, judgemental sampling, and semi-structured interviews to collect data and data displays for data analysis. The next chapter presents analyses and discuss the results

Chapter 4: Results and Discussion

4.1 Introduction

The previous chapter outlined the methodology that was followed in conducting the present study. The objectives of this chapter are to present, analyse and discuss results. The results are summarised in data displays tables. This is followed by an analysis of the findings, in the form of detailed write-ups. The findings are then compared with literature to establish whether they are in line with, or contrary to prior literature. Finally, findings are summarised at the end of the chapter.

4.2 Key respondents

The research population as stated in Chapter 3, was the Stanbic Bank Zimbabwe management and staff, and for the purposes of this study, face-to-face interviews were conducted with ten key respondents. The respondents chosen were Chief Executive, Finance Director, Finance Manager, Head IT, Senior IT manager, IT Security Manager and Risk Manager, Risk Officer, Audit Manager and Audit officer.

4.3 Key respondent description

The researcher selected the sample from Stanbic IT department because they are directly involved with the banking systems deployed and the security strategies adopted within the organisation. For example, in this study the IT security manager would be surveyed because he implements e-banking security strategies hence the need to assess the effectiveness.

Additionally the researcher chose Internal Audit because it is an independent, objective assurance and consulting department designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes thus it would help on the assessment of effectiveness of e-banking security strategies employed at Stanbic bank.

Moreover the researcher chose compliance team because its main purpose is to ensure that an organization has systems of internal control that adequately

measure and manage the risks that it faces. This helped when the researcher was checking on the attributes that are used to measure the effectiveness of e-banking security strategies.

The Chief Executive, Finance director and Head IT were chosen on the basis that they were at strategic level hence aids on determining overall objectives action and preparing for future changes.

The study covered the following key areas:

A. Respondent Background
B. E-banking security strategies
C. E-banking implementation challenges
D. E- banking security measures
E. E-banking security threats

Part A: Chief Executive, Finance Director, Head IT and Senior IT manager

4.3.1 Section A: Demographic information

Table 4.1 Demographic information of the respondents

Respondent	**Age of respondents**	**Professional or Academic background**	**Number of years employed by Stanbic Bank**	**Number of years in current position**
Chief Executive	Above 56	Economics	22	15
Finance Director	Above 56	Accounting	19	11
Head IT	46-55	Information technology	21	10
Senior IT manager	46-55	Information technology	18	7

The respondents were all mature and had been employed with the organisation for more than five years. The information indicated that the respondents had a strong

understanding of Stanbic bank IT operations by virtue of their positions and years within the organisation. The above findings showed that all respondents in the above table were at the strategic level of the organisation during the period covered by the case study (2010-2013).The diversity of their positions within IT enabled the researcher to obtain rich information from the perspectives of individuals who handle each a different portfolios and backgrounds.

4.3.2 Section B: E-banking security strategies

Table 4.2 E-banking security strategies

Respondent	Response
Chief Executive	We have invested heavily in information technology and efficient security strategies to enhance business processes with the aim of gaining competitive advantage.
Head IT	One Time Passwords, Multi-Layer Passwords and Smart Card Authentication are some of the fraud prevention security strategies that we have adopted to improve the bank's security of protecting information facilities.
Senior IT manager	Each security mechanism implemented strives to achieve a clear security goal such as confidentiality and integrity. We are implementing passwords, firewalls, encryption, virtual keyboards, pins, access codes and Secure Socket Layers.
Finance Director	The main idea behind the development and use of e-banking security is to improve the quality of our financial services while minimizing production costs hence we have been trying to provide funds to invest in technology.

The responses indicate that the organization is continuously seeking ways to improve the organization's security. According to the IT Security manager who is hands on and technical the most commonly used security strategies by the organization are passwords, firewalls, encryption, virtual keyboards and Secure Socket Layers .E-banking security is a product of IT thus the IT personnel knew more about the names of the strategies. As for the Finance Director he advised that

his responsibility was to ensure funds are there to invest in technology required being guided accordingly by the IT department. The Chief Executive pointed out that in order for the bank to fight competition it invested heavily in information technology security strategies with the aim of keeping the organization as a going concern. These findings are in line with literature, which states that overall security can be improved via such mechanisms as passwords (Claessens et al, 2002).

Table 4.3 Benefits of effective e-banking security strategies

Respondent	Response
Head IT	There has been an increase in sales and market share caused by the security of e-banking channels, which became a key enabler for minimizing consumers' fears on transacting through bank's services
Senior IT manager	By adopting effective security strategies the bank managed to increase their data collection, and management, efficient financial engineering which has resulted in ability of assessing potential creditors and measuring the creditworthiness of potential borrowers.
Chief Executive	Effective e-banking security strategies have created unprecedented opportunities for the organization and businesses globally
Finance Director	The experience of the bank following e-banking security measures and controls as part of security management procedures a positive effect on the profitability and growth of the organization.

The IT security manager proposed that survival and profitability of the organization is highly dependent on quality of service and efficiency hence the need to build customer trust by employing effective security strategies. Additionally the IT security manager commented how the organization gained competitive edge thus through increase of sales and reduction of costs as a result of secure systems that build customer confidence and trust in the bank's operations. The Finance Manager advised that there had been a positive profitability and growth after successful

implementation of e-banking security strategies. According to Speece et al (2003) effective e-banking security strategies enables banks to attract mobile customers and this offers tremendous profit potential by providing mobile financial services. This tied up with Chief executive's response that through adoption of effective strategies opportunities have risen for the organization locally and globally. The Head IT pointed out that there has been an increase in sales and market share caused by the security of e-banking channels, which became a key enabler for minimizing consumers' fears on transacting through bank's services The banking sector is one of the competitive industries with continuous upgrading of skills, products and technology all in the interest of retaining and wining customers. As indicated by Wind (2001) many banks are motivated to implement security strategies relating to the maximization of their earnings through increased market scope and improved customer relationship due to product delivery convenience and service customization.

4.3.3 Section C: E-banking implementation challenges

Table 4.4 E-banking implementation challenges

Respondent	Response
Head IT	Acquiring the relevant infrastructure has been the challenge since it is a prerequisite to have components such as the internet, hardware specifications that are up to date for the successful implementation of security strategies.
Senior IT manager	We face difficulties in ability to adopt global technology to local requirements thus technology selection as the organization would be considering the generation gap in adoption and aiming at securing customers trust of the providers online brand's security.
Chief executive	The organization often faces challenges of implementing up to date security strategies due to employees that do not have necessary skills and knowledge hence prompting the institutions to hire where necessary thus incurring additional costs.
Finance Director	We have faced financial challenges in implementing the e-banking security strategies with the aim to keep upbreast of the changing trends in technology which requires heavy investment in technology.

According to the Finance Director, the introduction of multi-currency system in February 2009 came with a new wave to the banking industry's competitive landscape as there is need to strike a balance between cost of offering services and profitability. He however cited that the bank has faced financial challenges to implement security strategies that are up to date. Earl, (2002) identified that while managers typically have a high-level understanding of their business and operational processes, they often lack employees with the experience and skills necessary to adopt software technologies and educate customers. In addition the Senior IT manager pointed out compatibility and gap issues between the old and new software as an adverse to adoption of security strategies.

In their responses the respondents indicated that challenges in implementation spans from lack of funds, technology selection, adoption, and lack of knowledge and skills. The Chief Executive was of the same view that the organization had challenges of lack of expertise and skills in implementing e-banking security strategies. Earl, (2002) identified that while managers typically have a high-level understanding of their business and operational processes, they often lack employees with the experience and skills necessary to adopt software technologies and educate customers

4.3.4 Section D: E-banking security and threats

Table 4.5 Reviews on security mechanisms

Respondent	Response
Head IT	We conduct reviews quarterly to check if there any new mechanisms that we need to employ to ensure safety of customer's bank accounts.
Senior IT manager	Successful audit trails assist us in conducting reviews on the security strategies and we conduct such quarterly.
Chief Executive	I do special meetings with the executive members semi-annually.
Finance Director	I am not called in such meetings.

The Chief Executive advised that he conducted such reviews semi-annually in a special meeting on half yearly financial results to check if there improvements that needs to be done on the bank's security systems. The Head IT and Senior IT manager concurred that they conducted reviews quarterly to ensure safety of customers' accounts. However the Finance director advised that he is not called to attend such meetings. Security concerns are of greatest importance for the adoption of e-banking services hence the need for improved continuous improvement in security to prevent fraud and mitigate the risk of customers' losing confidence in e-banking services (Giles, 2010).

Table 4.6 Ways of combating security threats

Respondent	Response
Head IT	• Protect authentication cookies with Secure Sockets Layer • Use resource and bandwidth throttling techniques. • Validate and filter input.
Senior IT manager	• Use digital signatures. • Use tamper-resistant protocols across communication links. • Secure communication links with protocols that provide message integrity
Chief executive	• Use strong authorization. • Use encrypted communication channels.
Finance director	• Create secure audit trails. • Use strong authentication.

The Chief Executive and Finance director did not have much to say on the threats since threats lies in IT area mostly. Moreover the Chief executive pointed out that there was need to use strong authorization and encryption of e-banking channels. In addition Finance Director suggested use of strong authentication and creation of secured audit trails as ways of combating threats. The Head IT indicated that use of bandwidth throttling and encryption were counter measures that could be used by the organization against security .His response concurred with the Senior IT Manager who echoed that encryption in communication channels and use of digital signatures could be used as ways of combating threats.

4.3.5 Section E: E- banking security measures

Table 4.7 Attributes of effective security strategies

Respondent	Response
Head IT	Customers want new level of convenience and flexibility thus good service delivery tends to measure the effectiveness of e-banking security strategies adopted.
Senior IT manager	In my opinion flexibility and compatibility are attributes that can measure effectiveness of security strategies.
Chief Executive	The bank's prime objective is to make profit through winning market share against the competitors. Therefore, consumer's needs to access the banking systems based on how easy they are used and how effective they are in helping them accomplish their task.
Finance director	The degree to which an innovation is perceived as being consistent with the existing values, past experiences and need of the receivers presents a relative advantage for the organization.

The Head IT echoed that convenience and flexibility of security strategies assists consumers' access of the banking platforms. The Senior IT manager emphasized on compatibility of security strategies thus maintaining consistency in relation to the technology advancements and changes. The Chief Executive emphasized that customers are mainly concerned with the ease of how to perform tasks that they need to achieve. A common obstacle to e-banking adoption has been the lack of security and privacy over the internet. Characteristics such as consistency can measure the effectiveness of e-banking security strategies thus the Finance director postulated that this will present relative advantage for the organization. As far as online banking adoption is concerned, security, trust and privacy concerns have been outlined as extremely important ones from the consumer's standpoint (Benamati and Serva 2007). The security attributes that banks must offer to

encourage consumers to switch to online banking are perceived usefulness, flexibility, reliability, confidentiality and continuous improvement (Liao and Cheung, 2008).

Table 4.8 Comments by respondents

Respondent	**Response**
Head IT	Personally, I believe that improved authentication systems are the way forward and can play a significant role in e-banking fraud prevention
Senior IT manager	The organization should keep an eye over risk on adopting security strategies because online customers typically expect their personal information and records to be kept accurately and securely.
Chief Executive	Technology is the way to go, the organization should keep researching on security strategies towards achievement of set goals.
Finance Director	No comments.

Due to high reports of e-banking fraud it seems existing measures have not been able to eradicate fraud. The Head IT commented that there is still need for research to narrow down on specific areas for improvement for instance improved authentication. The Chief Executive mentioned that adoption of improved strategies was important towards achievement of set

The Senior IT manager was of the view that the organization should consider risk as it tends to be an important characteristic from a consumer's perspective in the adoption of e-banking. According to Salisbury et al, (2001) risk is defined in relation to internet banking as the security and reliability of transactions over the internet.

4.4 Part B: Management and non-managers

4.4.1 Section A: Demographic information

Table 4.9 Demographic information of the respondents that were interviewed.

Respondent	**Age of respondents**	**Professional or Academic background**	**Number of years employed by Stanbic Bank**	**Number of years in current position**
IT Security manager	36-45	Information technology	15	6
Risk Manager	36-45	Risk management	11	6
Risk Officer	46-55	Risk management	9	5
Audit Manager	Above 56	Business management	25	12
Audit officer	46-55	Economics	7	7
Finance manager	36-45	Business finance	14	6

The respondents are all above the age of thirty six years. The respondents were in the employ of the Stanbic Bank and held their current positions during the period under study. The professions of the respondents include auditors, risk team and IT personnel and an accountant. This shows a diversity of skills in the organisation.

Table 4.10 Respondent position in the e-banking security management

Respondent	**Response**
Senior IT manager	Leading e-banking projects
IT Security manager	Active action in all IT projects
Risk Manager	Risk evaluation
Risk Officer	Risk analyst
Audit Manager	Part of the organization's general activities
Audit officer	Part of the organization's general activities
Finance manager	Participation to project activities

The Table 4.10 depicts the employees' units were part of main levels of hierarchy that is the execution level, in which units were responsible for daily routine activities such as part of the organization's general activities and the managerial level, in which units were responsible for surveillance, control and decision-making activities. Therefore, each unit depending on what level of the hierarchy it belonged to, and on its functionality, had access to specific responsibilities to pursue in the bank.

4.4.2 Section B: E-banking security strategies

Table 4.11 Benefits of effective e-banking security strategies

Respondent	Response
IT Security manager	I am pleased to advise that employing effective e-banking security strategies has benefited the organization in many ways through convenience and transparency to do transactions.
Risk Manager	IT risks have reduced big time due to implementation of effective e-banking security strategies.
Risk Officer	We have noted high levels of confidentiality, availability and integrity of the bank's system as a result of adoption of effective e-banking security strategies.
Audit Manager	There has been improved efficiency on the bank's internal control processes and loophole findings have reduced a lot.
Audit officer	There has been reduction in disruptions to banking business and potentially losses have reduced as a result of strong measures.
Finance manager	We have realised an increase in sales and reduced costs as the customers tend to favour the banks' core system.

All the respondents indicated that the organization benefited a lot from effective e-banking security strategies. The Risk Manager pointed out that IT risks have reduced and the Risk Officer echoed that they had noted high levels of availability and integrity of the bank's system. The Finance Manager postulated that the bank's prime objective was to make profit and implementation of effective e-banking security strategies helped the organisation with increase in sales as customer's trust and confidence has risen. According to Speece et al (2003) effective e-banking offers numerous benefits to both banks, transfer money, pay bills, collect receivables and ultimately reduce transaction costs and establish greater control over bank accounts. Similarly the Audit Manager said that there was improved efficiency in the

internal control processes and additionally the Audit Officer was of the view that there was reduction in disruptions to banking business thus less offline services and application errors.

Table 4.12 Reasons for e-banking security strategies adoption

Respondent	**Response**
IT Security manager	We are implementing e-banking security strategies for the reasons of ensuring confidentiality, integrity, availability, authentication authorization, non-repudiation and privacy.
Risk Manager	To prevent fraud and mitigate the risk of customers losing confidence in e-banking services.
Risk Officer	Inadequacy of security potentially leads to financial losses through losing market share hence the need for improved continuous improvement in security.
Audit Manager	We have realized that security concerns are of greatest importance for the adoption of e-banking services hence the need to ensure that the customer's funds are protected.
Audit officer	To ensure that there is no manual intervention on editing of files that process customer's payments.
Finance manager	The organization needs to keep abreast with technology for it to gain competitive edge in the industry.

In addition the Audit Manager postulated that the reason was to ensure that customer's funds and accounts are protected from fraudsters. The Audit Officer said that they did not want manual intervention for example on editing of files that processed customer's payments, deposits or transfers for fear of fraud by employees who would take advantage of the open systems. The Finance Manager indicated that there was high competition in the banking industry hence the bank need to keep up to date with current trends in technology because customers will run away for example to competitors like Ecocash. The Risk Manager echoed that the main reason was to prevent fraud and mitigate the risk of customers losing confidence in

e-banking services. The Risk Officer postulated that inadequacy of security potentially leads to financial losses through losing market share hence the need for improved continuous improvement in security to ensure customers confidence in e-banking services. Similarly the IT Security Manager pointed out that the bank was implementing e-banking security strategies for the reasons of ensuring confidentiality, integrity, availability, authentication authorization, non-repudiation and privacy.

4.4.3 Section C: E-banking implementation challenges

Table 4.13 E-banking implementation challenges

Respondent	Response
IT Security manager	There are times where funding is not directed to the right direction since other units insist to ignore technology needs but I suppose that is because they find it difficult to adopt to changes.
Risk Manager	Regulatory and legal issues are important requirements for the successful implementation of e-banking security schemes. However the process is cumbersome as the route is long with many authorizers.
Risk Officer	Sometimes e-banking security will be misinterpreted due to lack of communication on planning and development in terms of how risk messages are formulated and circulated.
Audit Manager	Resistance to change has been noted where some employees feel they will lose jobs and do not have the necessary expertise if the organization adopts some new technologies.
Audit officer	Lack of support from top management to ensure projects are completed on time.
Finance manager	We face financial challenges in acquiring the software and hardware specifications that are meets the e-banking security strategies.

The IT Security Manager pointed out that different political agendas of other banking units, which required a larger amount and this led to communication breakdown

among those units for instance there are times where funding is not directed to the right direction since other units insist to ignore technology. The Risk Officer advised that there was lack of good communication between the bank's units hence misinterpretation loomed in terms of how risk messages were formulated and circulated. The Finance Manager postulated that financial resources were a main problem as adoption of new technology development required large amounts of investments. The Audit Manager said that lack of expertise and skills was a challenge in implementation of e-banking security strategies and there was resistance to change as some feared losing jobs due to new changes. Support and understanding either ethical or financial from top management is a basic requirement for successful completion of e-banking projects (Turban et al, 2000). This concurred with the Audit Officer's response who echoed that there was lack of support from top management on implementing e-banking security which resulted in projects not getting completed on time. According to The Economist (1999), national, regional or international set of laws, rules and other regulations are important requirements for the successful implementation of e-banking security schemes. Similarly the Risk Manager concurred to this literature and echoed that regulatory and legal issues are important requirements for the successful implementation of e-banking security schemes, however the process was cumbersome.

4.4.4 Section D: E-banking security and threats

Table 4.14 E-banking security threats

Respondents	Response
IT Security manager	A threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. Threats can be external or internal. Internal threats can stem from three areas: the application development department, the infrastructure, and the data centre.
Risk Manager	I would say a security threat can be an event that modify, waste, deny or disclose information or reduce efficiency of the data and network resources. Examples include identity theft.
Risk Officer	A threat can be anything that destroy or harm the bank's system for example viruses.
Audit Manager	These threats include both negligence and deliberate acts by the users.
Audit officer	Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses.
Finance manager	Refers to anything that has the potential to cause serious harm to a computer.

The Risk Manager pointed out that a threat can be an event that reduces efficiency of the data and network resources. The IT Security manager pointed out that threats can be internal and external and they affect data centres and application development. The Head IT echoed the same on definition of threat and highlighted that examples included spoofing, phishing scams and identity theft. The Audit Manager postulated that threats could appear at the client or the server side and these could originate due to human, system or communication errors as a result of deliberate acts by the users. The Risk Officer and Finance Manager concurred that a

computer threat refers to anything that has a potential to cause harm to the computer. The finding confirms what Egwali (2008) found; threats come in many different forms. Similarly the Risk Officer echoed that example of security threat include viruses.

Table 4.15 Comments by respondents

Respondent	**Response**
IT Security manager	Personally, I believe that continuous improvement in adopting up-to-date technologies build a brand for the bank.
Finance manager	There is need to prioritize Information Technology when drafting the budget as the trends keep changing.
Audit Manager	I suggest that Stanbic staff should get some form of training on e-banking security to get an understanding of such issues as computer threats where for instance an email can be cloned and some people will respond to hackers.
Audit officer	Take note of all the systems were manual intervention from employees is taking place and strive to replace such with high security of automation.
Risk Officer	Introduce whistleblowing with incentives to the assist the existing security measures.
Risk Manager	It is important to communicate with the bank's network to ensure they understand the security needs in providing financial products and services.

The IT Security manager pointed out there was need to continuously seek for up to date technologies in order to safeguard customer's accounts and this would help in building brand for the organization. The Risk Manager postulated that it was important to make other units understand the security needs so that it would ease complications in implementation of security strategies. The Audit manager suggested that it was high time when the bank should replace manual interventions with high security automation to reduce fraud. The risk officer added that the bank can introduce whistleblowing with incentives to encourage employees to shout when they

see fraud taking in the organization. The Finance manager echoed that it was keen for the organization to prioritize Information Technology when doing budget allocations because the trends kept changing and it was idle to keep up to date.

4.5 Summary of findings

4.5.1 E-banking security strategies

The important finding on this issue is that organization is constantly researching on security strategies with the aim of eradicating e-banking fraud. One Time Passwords, Multi-Layer Passwords and Smart Card Authentication are some of the fraud prevention security strategies that Stanbic bank has adopted to improve the bank's security of protecting information facilities.

4.5.2 Attributes to measure the effectiveness of e-banking security strategies

According to the research outcomes, consumer's needs to access the banking systems based on how easy they are used and how effective they are in helping them accomplish their task. The findings indicated that attributes such as compatibility, flexibility and convenience measured the effectiveness of e-banking security strategies.

4.5.3 E-banking implementation challenges

The study established that implementation was inhibited by lack of funds, technology selection, adoption, and lack of knowledge and skills. While the organization had management with a high-level understanding of their business and operational processes, they often lacked employees with the experience and skills necessary to adopt new software technologies. In addition the bank faced financial challenges in implementing the security strategies as the banking industry's competitive landscape is sore.

4.5.4 Benefits of effective e-banking security strategies.

The study found that the mains benefits of e-banking security were transparency thus improved efficiency on the bank's internal control processes. In addition the Research findings also indicated that effective security created unprecedented opportunities for the organization and businesses globally by way of growth in market share thus gaining competitive edge in the industry.

4.6 Chapter conclusion

This chapter presented, analysed and discussed results in line with literature. The findings which are summarised in the sections above formed the basis of conclusions drawn in the next chapter.

CHAPTER 5: Conclusions and Recommendations

5.0 Conclusions

5.1 Introduction

The previous chapter covered research results and discussions. This chapter is aimed: drawing conclusions in line with research objectives, evaluating the research proposition in view of conclusions, and making recommendations [based on conclusions and findings].

5.2 Conclusions

5.2.1 E-banking security strategies

The research concludes that Stanbic bank is using effective e-banking security strategies and is constantly researching on more effective security strategies with the aim of eradicating fraud.

5.2.2 E-banking implementation challenges

5.2.2.1 Lack of finance and skills

It is also concluded that e-banking implementation challenges emanate primarily from lack of skills and finance. The Stanbic bank got this problem in implementing, with regard to human resources, where people lacked necessary skills and with regard to financial resources, where large amounts of investments were required on new security technologies.

5.2.2.2 Lack of communication

Another study conclusion is that lack of communication caused implementation challenges where there are misinterpretations on planning and development in terms of how risk messages are formulated and circulated e-banking implementation challenges. People reacted differently to poorly constructed security messages hence communication will break down and may confuse task knowledge and security awareness among the employees. The e-banking security management therefore faced challenges to implement change.

5.2.2.3 Legal issues

The activities of the organization are controlled by the government hence any changes to strategy thus need to be approved before implementation of e-banking security schemes. The study concludes that the process of regulation was cumbersome as it involved so many stakeholders and would then be time consuming to ensure all relevant authorities have been engaged. The Banking sector is a statutory body under the legislation Banking Act (Chapter 24:20) and Bank Use Promotion.

5.2.4 Benefits of effective e-banking security strategies.

It is further concluded that there have been tremendous benefits from effective e-banking security strategies that became a key enabler for minimizing consumers' fears on transacting through bank's services thus creating opportunities for the organization globally and locally. In addition increase in sales and market share have also been realized as part of benefits to the organization.

5.2.5 Evaluation of Research Proposition

The following proposition was set for this study:

The limited effectiveness of electronic banking security strategies in Stanbic Bank Zimbabwe is due to inadequate investment in technology and the relatively low levels of skills.

The research has shown that although the organization had effective e-banking security strategies it faced financial challenges and lack of skills in implementing them. Therefore the study confirms this proposition.

5.3 Recommendations

In light of the study findings and conclusions this study makes the following recommendations for Stanbic Bank:

5.3.1 Methods of communicating e-banking security

Stanbic bank should primarily exploit the good communication channels, thus the main implication for e-banking security management is to focus on changing attitudes and human behaviour, which are parts of the organizational norms and

values of an organization's culture in order to enhance awareness among the employees about e-banking security emerging trends.

5.3.2 E-banking security planning

The study recommends that acquiring the relevant infrastructure is a prerequisite to have components such as the Internet, hardware specifications that are up to date for the successful implementation of security strategies.

5.3.3 Research and development

The second recommendation is that the organization should invest in continous research and development on e-banking security that have current implemented strategies. This will enhance security for electronic transactions.

5.3.5 Training and education

Finally, Stanbic bank should send IT employees to get education and training on e-banking security so that they acquire the necessary skills .The training can be both inclusive and exclusive to develop a uniform understanding by employees of e-banking security it faces. This is important because it will help the organization in acquiring skills which would help in identification of possible threats it faces.

5.4 Study limitations and areas of further research

In real academic and professional worlds, it is not practical to carry an exhaustive single research due to time and coverage constrains. It was also difficult to gather information, given the confidentiality involved.

There are opportunities to undertake further intensive research to identify more social and organizational factors that affect communication standards and procedures in e-banking security. Although communication seems to positively influence e-banking security, we cannot be sure as to how communication can always do that.

APPENDIX 1

INTERVIEW GUIDED QUESTIONS

My name is Minmore Chigaro and I'm studying for a Master's Degree in Business Administration at the University of Zimbabwe. I am conducting a study on the effectiveness of e-banking security strategies in Zimbabwe and would be grateful if you could take your time to answer the questions I have on the stated subject matter. I specifically chose you because of your experience and knowledge of the subject matter. Your input would be of use to the University of Zimbabwe, policy makers in Government and stakeholders in the legal industry. All information and data obtained from you will be treated as strictly confidentiality.

SECTION A: BACKGROUND OF RESPONDENT

1. What is your position in the organization?

.....

2. Please state your age

□25-35years □ 36-45years □ 46-55 □ above 56

3. Please state your professional/academic background.

.....

4. How many years have you been employed by the organization?

.....

5. How long have you been in your current position?

.....

SECTION B: E-BANKING SECURITY STRATEGIES

1. What e-banking security strategies are you implementing to protect information processing facilities?

.....
.....
.....

2. Explain how the organization benefits from adopting security strategies that you mentioned previously?

.....
.....
.....
.....
.....
.....

3. Why are you implementing e-banking security strategies in your organization?

……
……

SECTION C: E-BANKING IMPLEMENTATION CHALLENGES

1. What barriers and challenges do you face in implementing e-banking security strategies?

.....
.....
.....
.....
.....

2. How often do you conduct reviews on your security mechanisms?

……
……
……
……
.....

SECTION D: E- BANKING SECURITY AND THREATS

1. What do you understand by security threats and give examples?

.....
.....
.....
.....
.....

2. What is your role in the e-banking security management?

……
……

3. From your own point of view how well do you think the organization can combat security threats?

.....
.....
.....
.....
.....

SECTION E: E-BANKING SECURITY MEASURES

1. What attributes are used to measure the effectiveness of e-banking security strategies?

.....
.....
.....
.....

2. Do you have any further comments that may assist in this study?

……
……
……
……
……
.....

End of Questionnaire

Thank You for Your Valuable Time and Support.

References

1. Bargh, M., Janssen, W., & Smit, A. (2002). Trust and Security in E-business Transactions. Retrieved 08 August, 2012, from
2. Business Wire (1995). Stanford federal credit union pioneers online financial services. *Business Wire*, June 21.
3. Chau, P., and Lai, V. (2003). An empirical investigation of the determinants of user acceptance of internet banking. Journal of Organizational Computing and Electronic Commerce, 13 (2), 123-145.
4. Claessens, J., Dem, V., Cock, D. D., Preneel, B. & Vandewalle J. (2002). On the security of today's online electronic banking systems. Computers & Security, 21 (3), 257-269.
5. 5.Cooper, R.G. (1997). Examining some myths about new product winners, in Katz, R., ed., The human side of managing technological innovation, Oxford, 550-560.
6. *Daniel, E., (1999). Provision of Electronic* Banking in the UK and the Republic of Ireland. The International Journal of Bank Marketing, 17(2), 72-82.
7. Egwali, A. O. (2008). Customer Perception of Security Indicators in Online Banking Sites in Nigeria. Journal of Internet Banking and Commerce,13(3).
8. Fatima A., (2011). E-banking security issues – Is there a solution in biometrics? Journal of Internet Banking and Commerce, 16 (2).
9. Gerrard, P., and Cunningham, J. B. (2003). The diffusion of internet banking among Singapore consumers. International Journal of Bank Marketing, 21(1), 16 – 28.
10. Gerrard, P., and Cunningham, J. B. (2003). The diffusion of internet banking among Singapore consumers*. International Journal of Bank Marketing*, *21*(1), 16 – 28.
11. Grabner-Krauter, S., and Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment, *International Journal of Human-Computer Studies*, 58, 783-812.

12. Grandison, T., and Sloman, M. (2000). A survey of trust in Internet Applications. IEEE. Retrieved 08 ugusthttp://www.comsoc.org/pubs/surveys/.
13. Hutchinson, D. and Warren, M. (2003). Security for internet banking: a framework. *Logistics Information Management*, 16 (1), 64-731.Hutchinson, D. and Warren, M. (2003). Security for internet banking: a framework. Logistics Information Management, 16 (1), 64-73.
14. Kesh, S., Ramanujan, S., and Nerur, S. (2002). A framework for analyzing e-commerce security. *Information Management and Computer Security*, *10*(4),149-158.
15. Khan, M. S., Mahapatra S. S., and Sreekrumah (2009). Service quality evaluation in internet banking: An empirical study in India. *International Journal of Indian Culture and Business Management*, *2*(1), 30 – 46.
16. Knorr, K., & Röhrig, S. (2000). Security of electronic business applications: structure and quantification. Paper presented at the proceedings of the First International Conference on Electronic Commerce and Web Technologies.
17. McClave,T., Benson,P and Sincich,T. (2007). "*A First Course in Statistics"*: Prentice Hall
18. Maijala, V. (2004). Outlook of the information security in e-business. Retrieved 8th August, 2012, from www.tml.tkk.fi/Publications/Thesis/maijala.pdf#
19. Oppliger, R., and House, A. (1996) Authentication systems for Secure networks. Retrieved 8th August, 2012, from www.artech-house.com
20. Peotta, L., Holtz, M.D., David, B.M., Deus, F.G., de Sousa, R.T. (2011). A Formal Classification of Internet Banking Attacks and Vulnerabilities. *International Journal of Computer Science & Information Technology, 3* (1).
21. Sathye, M.(1999). Adoption of Internet Banking by Australian Consumers: An Empirical Investigation. *International Journal of Bank Marketing, 17*(7), 324-334.
22. Schneier, B. (2005). Two-factor authentication.Too little, too late, *Communications of the ACM*,*48*(4),136.
23. Singhal, D., and Padhmanabhan V. (2008). A study on customer perception towards internet banking: Identifying major contributing factors. *The Journal of Nepalese Business Studies*, *V* (1), 101 – 111.

24. Suh, B., and Han, I.(2002). Effects of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications*, 1, 247-263.
25. Thorton, C. (1996). Thorton consulting online banking: a success. Australian Banking and Finance, 5(13), 2.
26. US-CERT (2006). Banking Securely Online. Retrieved from: http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf
27. Kesh, S., Ramanujan, S., and Nerur, S. (2002). A framework for analyzing e-commerce security. Information Management and Computer Security, 10(4),149-158.
28. Sathye, M.(1999). Adoption of Internet Banking by Australian Consumers: An Empirical Investigation. International Journal of Bank Marketing, 17(7), 324-334.
29. Neuman, W.L., (2006) *"Social Research Methods, Qualitative and Quantitative Approaches":* Boston
30. Rotchanakitumnuai, S. and M. Speece (2003). Barriers to Internet Banking Adoption: a qualitative study among corporate customers in Thailand. International Journal of Bank Marketing, vol. 21, no.6/7, pp. 321-23.
31. Economist (1999): "The Net Imperative – Business and the Internet Survey, The Economist, London.
32. Earl, M. (2000): "Evolving the E-Business", Business Strategy Review, Vol.11, No. 2, pp 33-38.
33. Salant, P and D.A Dillman (1994) "*How to Conduct Your Own Survey"* John Willy & Sons Inc
34. Stanbic Bank Industry Review, 2012
35. Stanbic Bank Zimbabwe 2012 Financials, published.
36. Saunders, M., Lewis, P. & Thornhill, A. (2009) Research methods for business students, 5th ed., Harlow, Pearson Education.

37. White. B, (2000), *"Dissertation Skills for Business and Management Students, Continuum"*

38. Yin, R.K. (1994). *"Case Study Research Design and Methods",* 2nd Edition: Sage.

39. Yin, R.K. (2003). "*Case Study Research Design and Methods",* 3rd Edition: Sage.