USERS' PERSPECTIVES OF ELECTRONIC BANKING RISK ISSUES AND CONTROL MEASURES TO MANAGE THE IDENTIFIED RISK: A CASE STUDY OF GCB BANK LTD

DICKSON SEREBOUR TAYLOR

(ID: 10700450)

A LONG ESSAY SUBMITTED TO THE UNIVERSITY OF GHANA BUSINESS SCHOOL LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF A DEGREE IN MASTER OF SCIENCE ACCOUNTING & FINANCE

AUGUST 2019

DECLARATION

I hereby declare that this submission is my own work towards the degree of MSc Accounting & Finance and that, to the best of my knowledge and believe, it contains no material previously published by another person nor material which has been accepted for the award of any other degree of the university, except where due acknowledgement has been made in the text.

DICKSON SEREBOUR TAYLOR ....

. Student's Name Signature Date

(10700450)

Dr. PATRICK ASUMING ....

Supervisor's Name Signature Date

ACKNOWLEDGEMENTS

Special thanks to God Almighty for seeing me through this long essay. I would like to take this opportunity to thank my supervisor Dr. Patrick Asuming, for his help and guidance in the completion of this long essay. All friends of MSc Accounting & Finance 2018/2019 Professional Class for their massive support and encouragement. Georgina and Miracle Taylor – thank you for your patience. I would also like to thank my family for all the help provided throughout my education.

Finally, I would like to thank all the respondents who took part in this study, for their insightful contribution to this work is greatly appreciated.

DEDICATION

I dedicate this work to my late mother Madam Selina Boafoa and father Mr. Charles Taylor for their great investment in my education. My second dedication also goes to my wife, Mrs. Georgina Taylor and daughter Miracle Taylor for their love and encouragement.

ABSTRACT

The speed of technological advancement has improved financial innovation in the banking sector by the introduction of new products and services, with electronic banking capabilities to enhance the convenience of banking. However, this financial innovation poses risk issues, which need to be addressed**.**

This research study was carried out to obtain users' perspectives on e-banking risk issues and the control measures to manage the identified risk, using GCB Bank Ltd as a case study. It examines the personal safeguard measures put in place and the e-banking risk management strategies employed. Finally, the role of the bank in ensuring the safety of the e-bankers is discussed. A qualitative approach was employed as the method of this study, where fifty (50) respondents answered structured interview questions.

The research findings indicate that systems vulnerabilities and identity theft can lead to fraudulent/unauthorized withdrawals, but risk consciousness and awareness can help prevent these e-banking risks. Banks with strong security controls and financial system defenses will go a long way to provide safety to the e-bankers.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Background

Continuous financial innovation is expanding the electronic banking space rapidly with the introduction of new products and services by the banks, to gain competitive advantage and to be more efficient to meet the high expectations of customers.

Electronic banking involves the use of Payment Cards (Credit Cards and Debit Cards) on ATMS, Point of Sales (POS) Devices, e-commerce platforms and the use of other channels such as Internet Banking, SMS &Mobile Banking etc., for delivering banking services. Khan (2017) described two forms of e-banking services as; transactional activities comprising, transfer of funds, payment of bills, loan applications etc. and non-transactional activities like request for issuing of cheque books, stop or make payments, online statements, updating the contact information of a customer etc.

E-banking as alternative channel for delivering banking services carries risk as well as new business opportunities for banks and service benefits (banking services at the comfort of your home) for customers, Georgescus (2005). He indicated legal and reputational risk can be addressed by the banks through adequate disclosure of information on their web site and also taking the right measures to protect customer privacy. Khan (2017) is also of the view that banks are supposed to review their risk management policies and processes to be able to mitigate the risk associated with e banking. The Basel Committee on e-banking (2003) cautions on e-banking risk to both retail and wholesale customers of the bank. The Committee further advised that banks should assess and manage such risk in a prudent manner.

This research solicited views and opinions of electronic banking from users forming their perspectives as to the challenges (risk and issues) associated with e-banking services. Therefore, qualitative research method, which allows participants to express opinions /views unrestrictedly, on open-ended interview questions, is appropriate for this study (Cassell et al 1994). According to them, qualitative research attempts to be meaningful and give different interpretations to phenomena. The research studied the phenomena in its real world context through a case study. GCB Bank has been selected for the study due to its large size and customer base, huge portfolio of electronic products & services and the high length of time in the electronic banking business. Furthermore, GCB Bank has relatively higher electronic banking users than other banks due to their large customer base. GCB Bank started banking business since 1953, now operates a universal banking and has invested a lot in information technology and its associated e-products; comprising: Payment Cards, Internet, SMS &Mobile Banking, POS &ATM Acquiring etc., The bank was adjudged the best Retail Bank in Ghana in 2016 by the Banker Africa, during the fourth annual West Africa Awards, attracting more than 11,800 votes. GCB Bank Ltd received a certificate and crystal trophy in recognition of outstanding, best practice & excellence performance, and its contribution to the retail banking in Ghana.

To collect data for this study, in all, a purposive sampling of 50 participants from GCB Bank were interviewed, comprising; 15 retail customers, 15 business customers and 20 GCB e-banking staff. According to qualitative researchers the ideal sample size is the one that additional participants do not provide any new insight (point of saturation), Latham (2014). Guest, Bunce, and Johnson (2006) propose 12 as saturation for homogeneous group. To test for saturation, one must go beyond the saturation number for homogeneous group to ensure that no new concept emerges, therefore sample size of 15 for each group works very well, Latham (2014).

The empirical data collected through the interviews were analysed using the SQC Model (set up, quote and comment). Themes generated from the interview transcripts were categorised and coded. The perspectives gathered from the interviews were linked to the literature review to ascertain its relationship.

1.2 Problem statement

The use of electronic means in undertaking banking services has several security implications. Cyber-crime is on the ascendency, where hackers hack into the accounts and transaction of account holders to make unauthorized withdrawals. The threat of customer information privacy, the risk exposure and other associated challenges like ATM skimming, where a device is fixed on the ATM terminals by fraudsters to gain access to card and pin information of cardholders. The above-mentioned schemes of fraudsters among others, poses a great threat to electronic banking. Most electronic banking users may not be aware of the security implications of e banking. This study seeks to explore. Utakrit (2012) discovered from his studies on e-banking users' awareness on phishing attacks security, that users have insufficient knowledge to protect themselves. For e-banking issues, Khan (2017) argued that security implication was the biggest challenge in e- banking. A number of researchers have done studies on the impact of electronic banking on efficient service delivery, however only a few researched on the issues and risk associated with e-banking. Khan (2017) identified eight benefits of e-banking as: customer convenience of doing banking transaction from the comfort of their home; customer enjoying better bank rates as a result of cost savings derived from e-banking; ability to perform banking transactions whiles on the move (mobility); increased comfort and timesaving; quick and continuous access to information; better cash management; speed and funds management. According to Singh (2013), most of the studies were conducted on factors accounting for the adoption of e-banking services, application of extended

Technology Acceptance Model (TAM) to e-banking sector, behaviour of non-users of e-banking services, development of scale to measure e-service quality and many more. He concluded that most of the studies were on the perceived risk and privacy issues but not on how to address them. His study was to discover the experience of using online banking security by users to protect them from possible phishing attacks. Birkeland (2015) researched on e-banking security and organizational changes. The study looked at the common misconception of security situations in e-banking between customers and internal staff, the separation of technical security from human security as there are new security sources like social engineering resulting in huge losses and fraud in digital banking. His finding was that though re-organizational planning does not increase customer security instantly, it has long term benefits. According to Bilal (2011) on the study of Trust & Security issues in Mobile banking and its effect on Customers; several literatures reviewed, indicated that customers did not trust mobile banking payment transactions, and the authors identified that customer mainly distrusts the authentication and level at which data transactions are made securely. He concluded by his research findings that fingerprint mechanism as a bio metric method among others can improve mobile banking security. Kiljan (2017) studied on usable security on online banking and identified that, every transaction security measure is a trade- off between ease of use and ultimate security, therefore research is needed to solve the many challenges involved. Digital transformation has created new vulnerabilities that criminals are quick to exploit and monetize, though technology is employed with the trust that, it will be secured and safe. The world of digitization is now under the threat of cybercrime, Hanson (2018). He further stated that cyber security has now become critical management issue, which sits right on top of boardroom agenda.

There have been several concerns for banks to have a robust system in place to timely identify and deal with the threat of cyber-attacks. The Bank of Ghana (BOG) has recently unveiled the

Cyber & Information Security Directives for the Financial Industry and established security Operations Centre (www.myjoyonline.com). Dr Maxwell Opoku-Afari, the First Deputy Governor of BOG, speaking at the launch of the directives, pointed out that, the study by the bank has disclosed that, there were more than 400,000 malware incidents, 44 million spam incidents, and 280,000 bot incidents within Ghana's financial industry. There is a cause for further studies on this phenomenon. The institution of Cyber Security Awareness month in October, starting from October 2018, by the Ministry of Communications-Ghana, is a good initiative in educating e-banking users. According to the CEO of the Standard Chartered Bank Ghana, Mrs. Mansa Nettey, speaking at the Cyber Security Awareness Forum; "Cyber Security remains top priority for financial institutions" and called for organizations to invest willingly in resources to combat cybercrime She further advised on putting in place appropriate corporate governance and compliance procedures to reduce cyber risk (Business & Financial Times, 2018). The gap in research regarding the identification of security implications, challenges involved in electronic banking, the concern for awareness of cybercrime and how to address them will be covered by this research.

1.3 The Research Questions

This study solicited responses to the following questions

1. What are the issues and the inherent risk, the users (bank customers) exposed to?
2. Are there, adequate control measures to address the identified issues and the inherent risk?

This paper seeks to assess the users' perspectives of electronic banking, a case study of GCB Bank Ltd.

1.4 Aims/Objectives

The purpose of this study is to investigate into the following:

- Issues and risk associated with electronic banking
- Control and personal safety measures to address the identified risk of electronic banking.

1.5 Significance/contribution

This study will improve our understanding of the security implications of electronic banking and customer awareness of an up to date e-banking risk mitigation measures to address them.

Majority of the users of e-banking services do not have an in-depth knowledge about the risk associated with undertaking banking services through the various channels such as ATMS, Point of Sales (POS) Devices, e-commerce platforms, Internet Banking, SMS &Mobile Banking etc.

This research will also add to the body of knowledge of the various risk issues and the application of the appropriate control measures to manage them.

1.6 Scope of Work

The study was conducted at the five (5) branches of GCB Bank in Accra. The branches are Liberty House, High Street, Ministries, Legon and Adabraka branches. These branches were chosen because they are the branches selected by GCB Bank to promote e-banking products and services, according to internal source from the bank. The respondents were fifty (50) in all, comprising 15 retail customers, 15 business customers and 20 e-banking staff of GCB Bank Ltd. The study laid emphasis on users' perspectives on e-banking risk issues and the control measures to manage the identified risk.

1.7 Outline of the Study

The research paper was organised into five chapters: chapter one focusing on the background of the study, problem statement, objectives and significance of the study. Chapter two reviewed a range of literatures for information relevant to e-banking risk issues and control measures to manage the identified risk. Chapter three covers the methodology used to achieve the results; including the study design, sampling, sampling technique and data analysis. Chapter four presented the results and chapter five the main findings, conclusions and recommendations of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter will review the available theoretical and empirical literature on this research study of users' perspectives on e- banking. It will examine the risk issues in e -banking and the control measures to manage the identified risk. In addition, it will examine personal safeguard measures to be implemented by e-banking users. Finally, it will explore the role of the bank in protecting the e-banking users.

2.2 Electronic Banking Risk Issues

The role of information technology (IT) in the development of new banking products and services and the expansion of the alternative delivery channels of banks cannot be over emphasized. Electronic banking users can now engage in various banking transactions at the comfort of their homes through the various alternative channels such as internet/online banking, mobile &SMS banking, ATM services, POS Devices, e-commerce platform etc. for convenience. However, it is important to recognize that e-banking has an inherent risk issues, if not properly controlled and managed, will result in greater financial losses for both customers and the financial institutions.

Theoretical Review:

Perceived Risk Theory

Perceived risk explains the customer's perception about the uncertainty and the potential adverse consequences of buying a product or services. The purchase decision of the customer is highly influenced by the level of risk they are willing to take, Nasri (2011).

Every new technology may carry both benefits and risks to the user, the decision to adopt the technology or otherwise is dependent on how the benefits outweighs the risk. The risk perceived in e- banking services may minimize the benefits of the technology (Horst, Kuttschreuter, and Gutteling, 2007).

Empirical Review:

E-banking carries risk as well as benefits for banks and customers, Mircea ((2005).

The Basel Committee on e-banking, (2003) cautions on the risk in the delivery of banking services. The Committee emphasised on managing the risk prudently.

Khan (2017) argued that security implication was the biggest challenge in e banking.

Digitization is now under the threat of cybercrime, Hanson (2018).

There have been several concerns for banks to have a robust system in place to timely identify and deal with the threat of cyber-attacks. The Bank of Ghana (BOG) recently unveiled the Cyber & Information Security Directives for the Financial Industry and established security Operations Centre, (www.myjoyonline.com/business). The First Deputy Governor of BOG, disclosed that, there were more than 400,000 malware incidents, 44 million spam incidents, and 280,000 bot incidents within Ghana's financial industry.

Utakrit (2012) studies on e-banking users' awareness on phishing attacks security, reveals users' insufficient knowledge to protect themselves. His study was to discover the experience of using online banking security by users to protect them from possible phishing attacks.

Birkeland (2015) looked at the common misconception of security situations in e-banking between customers and internal staff, the separation of technical security from human security as there are new security sources like social engineering resulting in huge losses and fraud in digital banking. His finding was that though re-organizational planning does not increase

customer security instantly, it has long term benefits. Bilal (2011) on the study of Trust & Security issues in Mobile banking and its effect on Customers; indicated that customers did not trust mobile banking payment transactions, and identified that customer mainly distrusts the authentication and level at which data transactions are made securely. He concluded by his research findings that fingerprint mechanism as a bio metric method among others can improve mobile banking security.

Kiljan (2017) studied on usable security on online banking and identified that, every transaction security measure is a trade- off between ease of use and ultimate security, therefore research is needed to solve the many challenges involved.

E-Banking risk comes in various forms such as systems vulnerabilities, identity thefts and unauthorised or fraudulent withdrawals.

2.3 Systems Vulnerabilities

Criminals are exploiting and monetizing the vulnerabilities in digital transformation, Hanson (2018). In today's world, cyber criminals are able to bypass the security controls to exploit breaches or vulnerabilities within the cyber and information security defences of the financial systems, BOG Cyber and Information Security Directives -Document (2018).

Researchers at the Birmingham University discovered several flows in banking applications that allowed attackers to conduct man-in -the -middle attack and steal the credentials of millions of users. It was observed that nine (9) banking apps, had flows, even those of Bank of America, Meezan Bank, HSBC, Smile Bank and VPN Provider Tunnel Bear were affected, Jay (2018). Though, banking applications are now more secured than in 2015, two- thirds of online banking systems still contain at least one critical vulnerability, according to the new Financial Application Vulnerabilities Report from Positive Technologies (2017). Another discovery by Positive Technologies was that 48 percent of mobile banking apps contained at

least one critical vulnerability, which allows the attackers to "decrypt, intercept, or brute force accounts to access the mobile app or bypass authentication entirely" (Positive Technologies Report (2017), Jay (2018).

2.4 Identity Theft

Fraudsters use identity theft to take over your identity and pretend to be you. Fraudsters can steal your personal data when doing internet banking or when making online payment. Personal data can be stolen via phishing, malware or another type of social engineering. By phishing, technique perpetrators of fraud get hold of your personal data and/or your payment card by sending e-mails, sms messages and/or calling you on the telephone. Those data (and your payment card) will allow them to withdraw money from your account and also to perpetrate identity fraud. Malware is a collective name for all sorts of malicious and harmful software. Internet banking fraud occurs in these ways; firstly, customer security data stolen, secondly, the offender moves funds from the victim's account to the perpetrator's account using the stolen data. According to (Kaleem & Ahmed, 2008), fraudsters undertake their operations through the following schemes: "over the shoulder looking" where the offender observes the victim's financial transactions and records the personal information used in the transaction; "phishing" where a mail /sms is received purported to be from the consumer's bank as a way to obtain the consumer's personal information. Scammers capitalize on the vulnerabilities of users in order to trick them into divulging their data,(https://medium.com/@CloudMosa/the-vulnerabilities-of-digital-banking).

2.5 Fraudulent Withdrawals

Systems vulnerabilities and identity theft eventually result in unauthorized/fraudulent withdrawals from users' bank accounts.

According to Sravanthi (2016), 65% of total fraud cases reported by banks were technology related frauds, covering internet banking committed frauds, ATMs and others like payment cards (credit/debit/prepaid cards). He further argued that, the e-banking crimes are committed by persons with exceptional knowledge and expertise in password hacking (talented net users –techies) through the following means: Key Logger Software is able to detect a particular computer or laptop, records keystroke of user e-banking transactions in encrypted log files and able to send the details at specified email id. Other Password cracking Software's are Cain and Abel, John the Ripper, hash cat, Hydra and Elcom Soft. The software packages combine cracking strategies, and advanced attacks like dictionary attacks, brute force attacks that can also harm your passwords Personal Computers (PCs) or desktops. Hacking supported Websites –Hacking supported tools and software are provided by the various websites. Personal mails, online e-banking ids and passwords can be traced on various websites. OTP by pass -One-time password received by customer 's authenticated phone via message and mail is found unsecured, as hackers are able to bypass the OTP and transfer funds without the two-factor authentication. Hackers are able to clone payment cards and make unauthorised withdrawals.

2.6 Control Measures to Manage E-Banking Risk Issues

To control and manage the e-banking risk issues, several measures have been suggested to curb the negative impacts of this worrying phenomena. Keeping cards, documents and passwords safe, and regular monitoring of bank accounts to avoid bank fraud committed through identity theft. Find out how to you can prevent identity theft (BSP, 2006). Keeping systems up-to- date, install anti-virus on PC. Avoiding practices that can lead to security hazards, checking fingerprints of certificates (Claessens et al., 2002; BSP, 2006).

Don Duncan, director at Nu Data Security caution banks to implement security tools that do not rely on the data provided by the customer. He argued that multi-layered solutions including

passive biometrics will provide enhanced account protection and reiterated that will be hard for attackers to impersonate users while carrying out online attacks. Even if the static data has been stolen, decrypted, and ready to be used, bad actors cannot take over the account, Jay (2018).

To deal with identity theft, users are being advised to browse online using a virtual private network (VPN). Since this tool ensures that your information is kept secure and hidden from hackers by filtering all your web traffic through unique, encrypted connections provided via cloud servers. This tool essentially establishes a hacker roadblock which prevent access to you or your data because you are not directly online. Hackers will never know when you are logging into your bank(https://medium.com/@CloudMosa/the-vulnerabilities-of-digital-banking-7073b36334b)

Sravanthi (2016) suggested the need for the following steps to be taken: education, training and the use of advanced technologies to reduce operational errors; tight security measures by the bank to protect customer confidential information; changing of password and pin regularly by users and the use of virtual key boards to avoid being trapped by loggers.

2.7 Personal Safeguard Measures to Manage E-Banking Risk

Banks regularly send security tips for users of e-banking services, which eventually becomes personal safety measures to manage e-banking risk issues.

FDIC Consumer News, Winter, 2016 outlines the following as personal safeguard measures and basic security tips:install good anti-virus software that periodically runs to search for and remove malware; don't visit untrusted websites and don't believe everything you read; be suspicious if someone contacts you unexpectedly online and asks for your personal information; remember that no financial institution will email you and ask you to put sensitive information such as account numbers and PINs in your response ;verify the validity of a

suspicious-looking email or a pop-up box before providing personal information; take precautions when communicating with your bank (FDIC Consumer News, Winter, 2016)

2.8 Bank's Responsibilities for E-Banking Risk Management Framework

According to Munir (2017) e-banking technology, has facilitated the rise in operational risks He argued that legal risks failure to provide adequate privacy protection may also subject a bank to regulatory sanctions in some countries.

The Basel committee on e-banking mandates the Board of Directors and the management of banks to ensure that both logical and physical access security control processes are in place for e-banking to provide comfort to the e-bankers and ensuring the existence of clear audit trails for all e-banking transactions, Basel committee on E-Banking (2003)

The cyber and information security directives introduced by Bank of Ghana (BOG) in October 2018, outlines the following obligations among others for all regulated banks: placing special emphasis on cyber and information security, protection and management of systems and data effectively; enhancing the cyber and information security capabilities; PCI-DSS certification for banks with e-banking capabilities (BOG Cyber and Information Security Directives - Document, 2018.

2.9 Sample Safety Messages from GCB Bank to its Internet Banking Users

User -ID and Password

The user is required to mandatorily change the User-Id and password assigned by the bank on accessing Internet Banking Services for the first time. To secure the password, the user is expected to change the password possibly, once in 90 days. The user is expected to keep the User-id and password confidential, create a password of at least 8 characters long; a mix of alphabets, numbers and special characters, with no relationship with personal data such as the

name, address, date of birth, telephone number, vehicle number, driver license etc. Not to provide confidential information over email/SMS/phone call even if it is purportedly from the bank (GCB Bank Internet Banking Portal, 2019)

2.10 GCB Bank Ltd Electronic Products Offerings

GCB Bank as one of the largest bank in Ghana offers a variety of electronic banking products and services through a variety of channels, including over 300 ATM networks, mobile banking, POS, internet banking and payment cards.

GCB ATM network enables cardholders to undertake the following services: access your account, check your balance and withdraw money safely and securely, 24/7.

GCB Mobile Banking Services allow customers to undertake the following transaction and non-transaction activities: SMS alert on transactions, check your Account Balance, Mini Statement, Top Up your phone credit, Intra Account transfer, Mobile Money transactions, Bill & School Fees Payment

GCB Internet Banking allows users to perform the following: check your Account Balance,

view your statement of account, transfer funds within GCB accounts, initiate Standing Order instructions, obtain foreign exchange rates, find out more about GCB products and services (www.gcbbank,com,gh)

2.11 Conclusion

The aim of this chapter was to review the available literature relating to e-banking risk issues and the control measures to manage the identified risk. It discussed personal safeguard measures users of e-banking can observe and e-banking risk prevention strategies. It also

looked at the role of banks to protect the e-banking users. The next chapter looks at the methodology employed to collect data for presentation and analysis.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter covers the research approach, processes and technique used in carrying out the study. Source of data collection, sample and the criteria used to select the sample from the population and a description of the research participants /interviewees. It also provides an outline of research design and the instruments for data collection. The method for the research instruments, data analysis and measures for validating the instruments used.

3.2 Research Approach

There are several methods of conducting a research; which includes qualitative, quantitative and mixed research methods. This study takes a qualitative research approach which attempts to make different interpretations to a phenomenon meaningful. The qualitative approach is appropriate for this study as it allows participants to express opinions/views unrestrictedly on open-ended interview questions forming their perspectives on electronic banking. Qualitative approach studies the phenomena in its real world context (Cassell et al, 1994).

3.3 Study Area

The following GCB Bank branches in addition to the E-banking Centre were selected for the study: Liberty House branch; High Street branch; Ministries branch; Adabraka branch and Legon branch. These branches were chosen because various E-Banking facilities or products including ATM services, Internet Banking, Mobile/SMS Banking, Point of Sale (POS), Smart Pay etc. are available. Also the above mentioned branches are strategically located and mandated to champion the promotion of all GCB e-products. These selected branches

continuously record high utilization rate of electronic banking products; according to internal source from the Bank ‘s E-banking Centre. All these branches have, retail customers as well as business ccustomers. Other factors accounting for the study area selection is proximity and ease of access to information to the researcher.

3.4 Study Design

The research design provides the procedural outline or blue print for the collection and analysis of data for the research. To gather an in depth information to address the objectives of the study, a case study approach was adopted. In all, fifty (50) interview questionnaires, were administered to interviewees from the five GCB Bank branches and the E-banking Centre to ascertain their perspectives on e-banking. The fifty (50) consist of three homogenous group comprising; business customers (15), retail customers (15) and e-banking staff (20). According to qualitative researchers the ideal sample size is the one that additional participants don’t provide any new insight (point of saturation), Latham (2014). Guest, Bunce, and Johnson (2006) propose 12 as saturation for homogeneous group. To test for saturation, one must go beyond the saturation number for homogeneous group to ensure that no new concept emerges, therefore sample size of 15 for each group works very well, Latham (2014).

3.5 Sources of Data

The study used both primary and secondary sources of data. The primary source of data is the fifty (50) interview questionnaires administered to GCB Bank customers in the five selected branches and the e-banking staff. The interview questionnaire was developed in consultation with the supervisor bearing in mind the research questions. All the fifty (50) respondents completed and returned the interview questionnaires. A copy of the interview questionnaire is attached as Appendix 1. The secondary source of data includes data gathered from World Wide Web (www.gcbbank.com.gh(data on GCB Bank), www.bog.gov.gh (BOG Directives on

Cyber& Information Security), myjoyonline.com (BOG Directives on Cyber& Information Security), graphic.com.gh, thebftonline.com (data on cyber-crime awareness), literature on e-banking, and journals to assist in analysing the empirical data collected.

3.6 Target Population

Population refers to the entire aggregation of items from which samples are drawn. The population for this study is the entire business and retail customers of the selected five GCB Bank branch customers as well as the E-banking Centre staff.

3.7 Sampling and Sample Technique

Six (6) respondents were interviewed in each of the five selected branches, comprising: business customers (3) and retail customers (3). Also twenty (20) E-banking Centre staff were interviewed. These categories of respondents were interviewed in each of the five selected branches, making a total of 30 respondents plus twenty (20) E-banking Centre staff respondents to make up in all, 50 sample size. Thus each of the three homogeneous groups represent a sample size beyond twelve (12) respondents, to support the assertion by qualitative researchers that after interviewing twelve (12) participants, additional respondents will not provide any new concept when interviewed, thus reaching a saturation. A saturation number of twelve (12) provides adequate and quality data to support a qualitative study. Guest, Bunce, and Johnson (2006) propose twelve (12) as saturation for each homogeneous group. To test for saturation, one must go beyond the saturation number for homogeneous group to ensure that no new concept emerges, therefore sample size of 15 for each group works very well, Latham (2013). The questionnaires were self-administered to the respondents. Purpose sampling was used for the E-banking Centre staff, whiles simple random sampling technique was employed for other respondents.

3.8 Data Collection Instruments

Primary data source of self-administered interview questionnaires was used by the researcher. For convenience of respondents, the self-administered interview questionnaires were given to respondent to answer open ended interview questions and returned them. (See Appendix 1). The questionnaires were developed based on the research questions and the literature.

The interview questionnaire began with an introductory statement, which indicated the purpose of the research as purely academic. Respondents were entreated to be objective with their responses since they were assured with confidentiality.

3.9 Data Collection Procedure

To encourage active participation, consent of all respondents were sought before they were included in this study. Convenient sampling was used to select respondents for the study.

Respondents were asked to express their views/opinions unrestrictedly on an open ended interview questions forming their perspectives. The intentions of the study were made clear to all respondents. It took approximately three weeks to administer all the interview questionnaires.

3.10 Data Analysis

The empirical data collected through the interviews was analysed using the SQC Model (set up, quote and comment). Themes were generated from the interview transcripts then categories and or coded. The perspectives gathered from the interviews were linked to the research questions and the literature review to ascertain their relationships.

3.11 Limitations

Though all respondents returned their interview questionnaires, some of them were reluctant initially to provide answers to the interview questions until were persuaded to do so.

Indifference on the part of interviewees limited the objective of the study.

CHAPTER FOUR

PRESENTATION OF RESULTS AND ANALYSIS

4.1 Introduction

This chapter presents the findings and analysis of user's perspectives on risk issues in e-banking and the control measures to manage the identified risks-a case study of GCB Bank Ltd, Accra. In all fifty (50) interview questionnaires were administered to both customers and employees of GCB Bank Ltd, Accra.

4.2 Demographics of Respondents

The study was carried out in Five (5) GCB Bank branches in Accra, namely: High Street; Liberty House; Legon; Ministries and Adabraka. A total number of fifty (50) respondents were interviewed, of which 62% were males, whiles 38 % were females. Forty percentage (40%) forming majority of the respondents were within the age bracket 31-40 years, followed by 32% of the respondents within the age bracket 21-30 years. Both age brackets are relatively young and more inclined to technology, therefore highly patronize e-banking services. All the respondents had some level of education which was exhibited in the quality of their responses Significant number (30%) of the respondents have been customers of GCB Bank for over decades, between 11-15 years. reflecting their loyalty and therefore, candid responses.

Table 1 Demographic Characteristics of respondents.

Age of Respondent	**Frequency**	**Percentage**
Under 20	0	0
21-30	16	32
31-40	20	40
41-50	7	14
50-59	7	14
60+	0	0
Total	**50**	**100**
Gender of Respondents	**Frequency**	**Percentage**
Male	31	62
Female	19	38
Total	**50**	**100**
Qualification	**Frequency**	**Percentage**
1.WASSCE/O'Level	0	0
2.Diploma/HND	2	4
3.First Degree	22	44
4.Postgraduate	18	36
5.Professional	8	16
Total	**50**	**100**
No of Years With GCB	**Frequency**	**Percentage**
0-2	11	22

3-5	3	6
6-10	10	20
11-15	15	30
16-20	6	12
Above 20	5	10
Total	**50**	**100**

4.3 Findings

The key themes that emerged out of the interview of fifty (50) respondents on users 'perspectives on e-banking risk issues and control measures to manage the identified risk, are presented below.

Systems Vulnerabilities, Identity Theft and Fraudulent Withdrawal. For control measures to manage the identified risk issues, the following were suggested by the respondents: Security Consciousness, Risk Awareness and Risk Prevention. All of the themes are interconnected and from the data analysis, it emerged that systems vulnerabilities may lead to identity theft, which may result in possible fraudulent withdrawals. Security consciousness will increase risk awareness of e- banking and help prevent the identified risk.

4.4 Systems Vulnerabilities Risk

Vulnerabilities in e-banking systems have been identified by some respondents, from the interview responses, as one of the key inherent risk in e banking. Respondent 1, a staff of GCB Bank, E-banking Centre, made it clear that, fraudsters knowing the systems vulnerabilities, want to advantage of it. According to him: *"Fraudsters exploiting vulnerabilities in the system to their own advantage (ATMS, internet banking and SMS banking)"* He was quick to add that there is a threat of cyber-attacks on users.

"*Threats of cyber-attacks in the form of malware, phishing, man-in -the -middle attack that may negatively affect the user and cause reputational damage*". (Respondent 1)

A Business Customer of GCB Bank- High Street Branch, respondent 11, also pointed out:

"Cyber-crime" (Respondent 11)

A Retail Customer of GCB Bank- Adabraka Branch, respondent 42, was the last to mention cyber-attack: "*Cyber robbery*" (Respondent 42)

Five of the respondents said it is possible to transfer monies to a wrong account.

A Business Customer of GCB Bank- Ministries Branch, stated: *"Transferring fund to wrong account"* (Respondent 22)

A Retail Customer of GCB Bank- Ministries Branch, said: "*Wrong accounts can be credited using Mobile Banking"* (Respondent 24)

A Business Customer of GCB Bank- High Street Branch, indicated: *"There is that risk of transferring money to unknown person"* (Respondent 12)

A Retail Customer of GCB Bank- High Street Branch, mentioned: "*Sending money to a wrong account"* (Respondent 13)

A staff of GCB Bank, E-banking Centre, emphasized: *"Funds can be wrongly transferred"* (Respondent 49)

Respondent 20, a staff of GCB Bank, E-Banking Centre, identified operational risk as one of the e-banking risk issues. According to him: *"Operational Risk, arises from fraud, processing errors and system disruptions"* He further stated security risk as another e-risk

"Security Risk-This arises on account of unauthorized access to my account or critical information" (Respondent 20)

A Retail Customer of GCB Bank- High Street Branch, respondent 25, highlighted that e-banking transactions can be duplicated: *"There are times transactions get duplicated when system is down/slow"* (Respondent 25)

Respondent 21, a staff of GCB Bank, E-Banking Centre, mentioned lack of privacy as one of the e-banking risk issues. "*The risk involve is by exposing your full card details in transacting on-line purchases or business"* (Respondent 21)

A Business Customer of GCB Bank- Liberty House Branch, respondent 27, also cautions of exposure of PIN when one is not very careful: *"A third party knowing your secret pin especially with the mobile banking and that of the card usage if not careful"* (Respondent 27)

A Retail Customer of GCB Bank- Legon Branch, respondent 17, was of the opinion that there is a security threat at the ATMS: *"You may be exposed to fraudsters during ATM Services especially when people are around ATM"* (Respondent 17)

The aforementioned interview responses, suggest that, e-banking systems are vulnerable, and can be exploited by fraudsters to commit cyber-crime. It is common to make funds transfer to unintended beneficiaries. Operational risk of processing and system errors can occur, unauthorized access and lack of privacy to essential security information may be high and finally, e-banking transactions can be duplicated causing a greater risk to users.

According to researchers, systems vulnerabilities remains the major e-banking risk, as two-thirds of online banking systems still contain at least one critical vulnerability that can be exploited by hackers, Positive Technologies Report (2017), Jay (2018).

4.5 Identity Theft Risk

It emerged from the interview responses that fraudsters are able to steal personal data or security information of e-banking users and use same to impersonate them to carry out fraudulent withdrawals. Some respondents mentioned the likelihood of account being compromised to gain unauthorized access to security information for unauthorized withdrawals. Respondent 2, a staff of GCB Bank, E-Banking Centre, stated:

"The risk of accounts (ATM cards &Internet banking being hacked) being compromised leading to unauthorized debits"

Respondent 41, a staff of GCB Bank, E-Banking Centre, mentioned:

"Basically the only likely risk is your account being compromised"

A Business Customer of GCB Bank- Legon Branch, respondent 45, was of the opinion that security information can be stolen: *"Pin or password falling into the hands of an unauthorized person"*.

A Retail Customer of GCB Bank- Liberty House Branch, respondent 9, stated:

"Someone knowing your pin" "Anyone who has access to your phone could have access to your bank details"

A Business Customer of GCB Bank- Legon Branch, respondent 15*:"If someone gets my pin"*

A Retail Customer of GCB Bank- Legon Branch, respondent 18*: "Theft of ATM pin & card"*

Some respondents mentioned hacking, ATM skimming and phishing as identity theft.

"Phone hacking" - A Business Customer of GCB Bank- High Street Branch, respondent 4

"Hacking through internet or phones"- Respondent 5, a staff of GCB Bank, E-Banking Centre

"Internet hacking" - A Retail Customer of GCB Bank- Liberty House Branch, respondent 7.

"Skimming, phishing "- Respondent 39, a staff of GCB Bank, E-Banking Centre

It is very clear from the above interview responses that, identity theft or the stealing of security information of users to undertake unauthorized withdrawals is a form of e-banking risk, which is committed through the following: account being compromised, stealing of security information or security information inadvertently getting into wrong hands, phone or internet banking hacking, phishing and ATM skimming. This revelation supports the assertions that fraudsters can take your identity and pretend to be you (Kaleem & Ahmed, 2008) This is a worrying phenomenon for users as well as banking institutions.

4.6 Fraudulent Withdrawals Risk

It was discovered from the interview responses that one major risk that can occur in e banking is fraudulent or authorized withdrawals. Some respondents indicated that ATM cards can be cloned (Fraudsters can make a counterfeit copy of the card) Here are the views:

"Cloning risk" - Respondent 35, a staff of GCB Bank, E-Banking Centre

"Criminals" can clone e-cards- Respondent 33, a staff of GCB Bank, E-Banking Centre

"Cloning of cards"- Respondent 3, a staff of GCB Bank, E-Banking Centre

"Clone of cards" - Respondent 32, a staff of GCB Bank, E-Banking Centre

Unauthorized access by fraudsters were some of the interview responses:

"Unauthorized access to internet banking" - Respondent 32, a staff of GCB Bank, E-Banking Centre mentioned.

"Unauthorized use of electronic card to undertake transactions by fraudsters, unauthorized transfer of funds from your account when fraudsters get access to your internet banking log-in credentials"- A Business Customer of GCB Bank- Adabraka Branch, respondent 10 indicated.

"Unauthorized withdrawals on the ATM, Card details being used online by unknown assailant"-A Business Customer of GCB Bank- Liberty House Branch, respondent 6 said.

"Loss of funds by fraudsters"-A Retail Customer of GCB Bank- Adabraka Branch, respondent 8 stated.

''Fraudulent Activities"-A Retail Customer of GCB Bank- Ministries Branch, respondent 36 pointed out.

"*Card Fraud & Internet Fraud*" -A Business Customer of GCB Bank- Liberty House Branch, respondent 46 mentioned.

"Robbery as in using the ATM" -A Business Customer of GCB Bank- Liberty House Branch, respondent 38 suggested.

"Card fraud" - Respondent 31, a staff of GCB Bank, E-Banking Centre indicated.

"Easy target for fraud" - Respondent 37, a staff of GCB Bank, E-Banking Centre

"Fraud, hacking "-A Retail Customer of GCB Bank- Ministries Branch, respondent 36.

The various interview responses so far affirm the believe that there is the risk of unauthorized or fraudulent withdrawals associated with e banking. It can take the form of unauthorized access to internet & mobile banking platforms, cloning of cards and other card and ATM frauds. Dependence on advancement in technology to make banking easier has paved way for technology-based crimes, Sravanthi (2016). According to Sravanthi, 65% of total fraud cases reported by banks were technology related frauds, covering internet banking committed frauds, ATMs and others like payment cards (credit/debit/prepaid cards).

4.7 Control Measures to Manage E-Banking Risk

As a control measure to manage the e-banking risk of system vulnerabilities, identity theft and fraudulent withdrawals, interview responses solicited for personal safety measures and strategies for managing the identified e-risk generated themes as security consciousness, risk awareness and risk prevention.

4.7a Personal Safety Measures Against E-Risk

The sub themes generated from the interview responses as personal safeguard measures includes **:** use of cards on only GCB ATMS **,** not disclosing PIN to anyone, not keeping card and PIN together, memorizing PIN, keeping Login and Transaction Password securely, not to ask for assistance when using the card, cover PIN with hands when using for transactions, Keeping ATM cards safely, not sharing ATM card with anybody, using only secured ecommerce site ,registering card on Secured Code before doing ecommerce transactions inspecting ATM Terminals for any skimming device before using it, use strong password and change regularly, full -Service Internet Security Suite for real time protection, protection against identity theft, guarding personal data and not giving personal information over the internet, logout your computer when not using it, robust systems to prevent data breach, periodic software updates of personal computers, being up to date on security issues monitoring or checking account balance regularly not to use ATMS at on unsecured area and securing systems with firewalls. Respondents views are as follows:

"Only visit secured site for on-line shopping. Do not open mails from unknown source. Check the card slot area to ensure green light is blinking before slotting in my card". Respondent 35, a staff of GCB Bank, E-Banking Centre

"I do not keep my card and pin together, password(logon) and transaction password for internet banking are kept secure" -Respondent 33, a staff of GCB Bank, E-Banking Centre

"To ensure that pins are well protected"-Respondent 3, a staff of GCB Bank, E-Banking Centre

"No sharing of Pins/Password, keep cards safely"-Respondent 32, a staff of GCB Bank, E-Banking Centre

"Look out for skimming devices when using the ATM, do not share my log-in credential with anyone" -A Business Customer of GCB Bank- Adabraka Branch, respondent 10.

"I make sure I only do transactions on secure websites, I do not give my card out to anybody" -A Business Customer of GCB Bank- Liberty House Branch, respondent 6.

"Employ qualified risk personnel, employ firewalls on cyber network, educate customers/staff on cyber security, comply with cyber security regulations."

A Business Customer of GCB Bank- Adabraka Branch, respondent 8.

"Frequent change of pin"-A Retail Customer of GCB Bank- Ministries Branch, respondent 36.

"Not exposing my pin to a third party "-A Retail Customer of GCB Bank- Liberty House Branch, respondent 38.

"Use of passwords"-Respondent 29, a staff of GCB Bank, E-Banking Centre

"Strong password creation, avoid clicking strange e-mails, logout when not using the computer" -Respondent 30, a staff of GCB Bank, E-Banking Centre

"Secure code registration on card" -Respondent 31, a staff of GCB Bank, E-Banking Centre

"I use my card on GCB Terminal unless GCB is not available, my PIN is known to only me, I do not request for assistance when using the card, I cover my PIN pad with my hand"

Respondent 34, a staff of GCB Bank, E-Banking Centre

"Frequent change of password"- Respondent 37, a staff of GCB Bank, E-Banking Centre

"Frequent change of password, constant monitoring of accounts"- A Business Customer of GCB Bank- Ministries Branch, respondent 40.

"Protection of password, usage of verifiable internet sites" -A Retail Customer of GCB Bank- Adabraka Branch, respondent 44

"Periodic change of password and use of strong passwords, periodic change"-Respondent 2, a staff of GCB Bank, E-Banking Centre

"I never write my password down or save in the webpage" -A Business Customer of GCB Bank- Legon Branch, respondent 45

"Memorizing my PIN" -A Business Customer of GCB Bank- High Street Branch, respondent 4

"Use strong passwords, use secure sites, don't use card at off-site /obscure ATMS, cover the keyboard with your hand when typing your pin at ATM terminals"- Respondent 5, a staff of GCB Bank, E-Banking Centre

"Cover my PIN when transacting at the ATM, do not open emails from unknown sources"

Respondent 39, a staff of GCB Bank, E-Banking Centre

"To use strong password and change them regularly, to use a full -service internet security suite to provide real time protection, take measures to help protect me against identity theft by guarding my password data and not giving personal information over the internet"

Respondent 1, a staff of GCB Bank, E-Banking Centre

"Frequent check of balance" - A Business Customer of GCB Bank- Ministries Branch, respondent 22

"Keeping my password or pin safe or not sharing it with the second person"- A Business Customer of GCB Bank- High Street Branch, respondent 12

"By keeping my password/pin safely"- A Retail Customer of GCB Bank- High Street Branch, respondent 13

"Monitor your accounts regularly, change password regularly, access your account from a secure location, protect your computer "-Respondent 49, a staff of GCB Bank, E-Banking Centre

"I ensure to logout of the system after transacting my business" -Respondent 20, a staff of GCB Bank, E-Banking Centre

"Checking of account balance and statement regularly. Changing password frequently"- A Retail Customer of GCB Bank- High Street Branch, respondent 25

"I must protect my password. Must keep confidential information. Must use safe or secure online for business. Must check all activities at the ATM before inserting my card for any transaction"-Respondent 21, a staff of GCB Bank, E-Banking Centre

"Skip public Wi-Fi. Set up reminder to change your password. Ask your bank how is keeping your records safe /secure" -A Retail Customer of GCB Bank- Legon Branch, respondent 17

"I cover my pin when using the ATM. I prevent people from shoulder surfing when using ATM. I keep my ATM Cards very safe. I use stricter password for my internet banking".

Respondent 48, a staff of GCB Bank, E-Banking Centre

"Safeguarding password" -A Business Customer of GCB Bank- High Street Branch, respondent 11

4.7b Strategies to manage e-banking risk:

The interview responses by the respondents as strategies to manage e-banking risk issues were centered on the following themes and sub-themes: *"Safeguarding password"* -A Business Customer of GCB Bank- High Street Branch, respondent 11

4.7b Strategies to manage e-banking risk:

The interview responses by the respondents as strategies to manage e-banking risk issues were centered on the following themes and sub-themes:

Security Consciousness -not exposing card data, avoid downloads from unknown source, securing your password at all times. **Risk Awareness-** not storing sensitive information on phone and other devices to protect account information and password, risk awareness and education.

Risk Prevention-threat prevention plans in place to deal with e-risk, making terms and conditions clear to users, banks providing the risk management framework, banks to monitor, review and continuously improve the risk management framework, adhering to risk mitigation measures, constant upgrade of systems to prevent external breaches, keep all computer systems up to date, installation of ATM Anti-Skimming Device by the bank, not sharing ATM card with anybody, using only secured networks.

The highlights are as follows: *"Transacting activities only on secure sites"*- A Business Customer of GCB Bank- High Street Branch, respondent 11.

"Abreast yourself with E-risk. More secure network and powerful internet security. Educate customers or people on password security"- Respondent 48, a staff of GCB Bank, E-Banking Centre

"Customer sensitization campaign. Constant upgrade of systems to prevent data breaches" Respondent 26, a staff of GCB Bank, E-Banking Centre

"Stop sharing your password with anyone"- A Retail Customer of GCB Bank- Legon Branch, respondent 17

"Create awareness to all the customers on the safeguard at the ATM. The bank must purchase fraud monitoring tool to manage the risk"- Respondent 21, a staff of GCB Bank, E-Banking Centre

"Using a secure website" -A Retail Customer of GCB Bank- High Street Branch, respondent 25

"Authentication control is an essential security step in managing E-banking risk. The bank system must be technologically equipped to handle potential sources of risks"- Respondent 20, a staff of GCB Bank, E-Banking Centre

"Use only secured sites, do not open unsolicited mails, do a physical check of the ATM before using it. Ensure you keep pin and card securely"- Respondent 35, a staff of GCB Bank, E-Banking Centre

"Education and Risk Awareness Training"- Respondent 33, a staff of GCB Bank, E-Banking Centre

"Education of clients, identify the various risks and plan and execute their mitigation, updated patches of software when due, ensure anti-virus is installed on all machines, all PCS should be password protected" -Respondent 3, a staff of GCB Bank, E-Banking Centre

"Educate customers about risk, ensure they are advised to keep password secured, no sharing of card" -Respondent 32, a staff of GCB Bank, E-Banking Centre

A Business Customer of GCB Bank

"Customer education -bank official should educate the customers about the dangers involved when they share or communicate credentials. Search by customers & bank officials when about to use the ATM. Thus searching for skimming devices & security cameras"

A Business Customer of GCB Bank- Adabraka Branch, respondent 10.

"Educate customer more on electronic products and its usage, clearly spell out terms and conditions to customers who use electronic products" -A Business Customer of GCB Bank- Liberty House Branch, respondent 6.

"*Train staff on E-banking risk, ensure risk factors are avoidable, ensure strict adherence to risk mitigation"*-A Business Customer of GCB Bank- Adabraka Branch, respondent 8

"Education of customers via text messages"-A Retail Customer of GCB Bank-Ministries Branch, respondent 36.

"Protect my Password and Pin" -A Business Customer of GCB Bank- Legon Branch, respondent 46

"Education, use of risk monitoring tool" -Respondent 29, a staff of GCB Bank, E-Banking Centre

"*Supervision, anti-crime measures like firewall, software strict monitoring"* -Respondent 30, a staff of GCB Bank, E-Banking Centre

"Ensure card data is not exposed, avoid downloading strange apps, use only secured networks" -Respondent 34, a staff of GCB Bank, E-Banking Centre

"Educating customers" -Respondent 37, a staff of GCB Bank, E-Banking Centre

"Ensure names appear when money transfers are done to confirm beneficiary, Self Service Care (where a customer can lodge a complaint and it would be resolved automatically"

A Business Customer of GCB Bank- Ministries Branch, respondent 40

"Prompt customer support" -A Retail Customer of GCB Bank- Adabraka Branch, respondent 44

"Keep all systems up to date, have internal audit, constant awareness creation of E-Banking risk, have prevention plans in place to deal with the threat of E-Banking risks"- Respondent 2, a staff of GCB Bank, E-Banking Centre

"Propagate the awareness and sensitization of security measures and practices" - Respondent 41, a staff of GCB Bank, E-Banking Centre

"Systems should be scanned frequently to detect or spot any attempts to hack the system, personnel who handle such services should be trained on confidentiality &background checks do effectively" A Business Customer of GCB Bank- Legon Branch, respondent 45

"Getting more knowledge about E-banking transactions"- A Business Customer of GCB Bank- High Street Branch, respondent 4

"Employee training, customer education, system upgrade"- Respondent 5, a staff of GCB Bank, E-Banking Centre

"Educate customers with simple tips"- Respondent 39, a staff of GCB Bank, E-Banking Centre

"Beware of email attachments and do not open such, keep your password safe and secured at all times and do not share with others. Avoid keeping sensitive information on your phone and other devices in order not to expose your account information/passwords" - Respondent 1, a staff of GCB Bank, E-Banking Centre

"Safe and secure websites"- A Business Customer of GCB Bank- Ministries Branch, respondent 22

The interview responses stated above with respect to personal safeguard measures and strategies to manage e-banking risk issues suggest that e-banking users know the risk issues associated with e-banking and have great insight on the strategies and even personal

safeguard measures to manage the identified risk. The best practice that can help users' is awareness and knowledge of these vulnerabilities and bad practices.

In addition to the personal safeguard measures, respondents stated that they receive the following coded safety messages from the GCB Bank Ltd

4.7 Safety Messages from the Bank

Notices on ATM Sites, SMS to change PIN, not keeping Card & PIN together

memorize PIN and destroy it, checking for Skimming Devices on ATMS before making transactions

one-time password for e-commerce / Secured Code & V by V, mandatory password change on Internet Banking Portal, fraud Alert messages, not to disclose your ATM Card, Mobile& Internet Banking PIN and password to a third party, not exposing password, mails on internet phishing,

perform internet banking on a secured computer, tips on using the ATM, not disclosing full card details.

This practice of Banks' sending e-banking safety messages to their customers is in line with regulatory requirements for banks with e-banking capabilities to put in place rigorous risk management framework to ensure the safety of their customers. According to the Basel Committee on e-banking banks should recognize, address and manage such risk in a prudent manner according to the fundamental characteristics and challenges of e-banking services. (Basel Committee on e-banking ,2003).

4.8 Conclusion

This chapter presents the responses obtained from the 50 respondents of GCB Bank Ltd on users' perspectives on E-Banking risk issues and control measures to manage the identified risk. The main themes of systems vulnerabilities, identity theft and fraudulent withdrawals were identified as risk issues in e-banking and to manage the identified risk, the emerged

themes suggested by the respondents are security consciousness, risk awareness and risk prevention.

The next chapter will discuss and analysis the findings of this study.

CHAPTER FIVE

SUMMARY CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter provides an interpretation to the research findings obtain from the interview responses from the 50 respondents comprising GCB Bank customers and staff of GCB E-Banking Centre. It will also illustrate how the findings answer the research questions and relate it to other research carried out.

The main objectives of this study were to investigate into users' perspectives on e-banking risk issues and the control measures to manage the identified risk.

The findings of this study are based on the interpretations and analysis of data obtained from the open ended interview questions administered.

5.2 Summary

The research questions were answered with the main themes of systems vulnerabilities, identity theft and fraudulent withdrawals as the major e-banking risk issues. To control the identified e-banking risk issues; security consciousness, risk awareness and risk prevention were the main themes suggested as strategies to manage the phenomena**.**

All the 50 respondents suggested at least one of the following as personal safeguards measures and strategies to manage the identified E-Banking risk among others: use card on only GCB ATMS, not disclosing PIN to anyone, not keeping Card and PIN together, memorizing PIN, keeping Login and Transaction Password securely, not to ask for assistance when using the card. The following themes also emerged as risk management strategies for e-banking risk issues; security consciousness, risk awareness and prevention.

According to the responses gathered from the interview questions, users of e-banking services receive the following safety messages among others from GCB Bank Ltd: not keeping Card & PIN together, memorize PIN and destroy it, checking for Skimming Devices on ATMS before making transactions, One Time Password for e-commerce / Secured Code & V by V, mandatory Password Change on Internet Banking Portal. These safety messages go a long way to assist users 'of GCB e-banking services to equip them themselves with tips necessary to manage the identified e-banking risk. Mircea (2005) indicated legal and reputational risk can be addressed by the banks through adequate disclosure of information on their web site and also taking the right measures to protect customer privacy. Khan (2017) suggested that banks are supposed to review their risk management policies and processes to be able to mitigate the risk associated with E-Banking.

According to Singh (2013) most of the studies were conducted on factors accounting for the adoption of e-banking services, application of extended Technology Acceptance Model (TAM) to e-banking sector, behaviour of non-users of e-banking services, development of scale to measure e-service quality and many more. He argued that most of the studies were on the perceived risk and privacy issues but not on how to address them. This study of users' perspectives on e-banking risk issues and control measures to manage the identified risk; solicited views on the risk issues in e-banking and went further to ascertain views on how the identified risk can be managed. It is important to find out if users of electronic banking have sufficient knowledge of risk preventive measures. This is an improvement over the study of the perceived risk and privacy issues, which did not address them as indicated by Singh (2013). This research indeed answers the questions; what are the risk issues in e-banking and how the identified risk can be managed.

5.3 Conclusion

This study was undertaken to investigate into e-banking risk issues and control measures to manage the identified risk. The foregoing chapters covers the perspectives gathered from the interview responses from the 50 respondents with themes of systems vulnerabilities, identity theft and fraudulent withdrawals as e-banking risk issues. To manage the identified risk, users' security conscious, risk awareness and risk prevention, were the themes that emerged.

The research questions were examined through a qualitative approach in a form of interview questions. The use of interview questions allowed for an in-depth insight into the users' perspectives of e-banking risk issues and control measures to manage the identified risk in an open and candid manner, making the analysis and the interpretations more meaningful.

A review of literature corresponding to the research topic was presented. Finally, an interpretation and analysis of the research findings obtained and its relevant to the research and other research carried out to date was presented.

The findings of this research is very relevant to every user of e-banking services as cyber-crime and related e-banking risk are on the ascendency. The discovery is that users perceive systems vulnerabilities, identity theft can lead to fraudulent withdrawals and these can be managed, when there is security consciousness and risk awareness to prevent such risk

5.4 Recommendations

This research sought to solicit users' perspectives on e-banking risk issues and the suggested measures to manage the identified risk. Though the findings indicated users' awareness of the risk issues and the measures to control the identified risk, there is a limitation of this research. There may be several e-banking risk issues and control measures, which were not revealed by this study. Further studies are recommended in the areas such as; "to what extent are risk issues

of e-banking impacting negatively on efficient and effective services delivery, or “do the benefits of e-banking far outweighs its risk and challenges”. A key recommendation to the banks is the need to put in place appropriate and adequate security controls in the e-banking services offered to their clients as revealed by the interview responses that the existing controls are inadequate.

REFERENCES

Bilal, M., & Sankar, G. (2011). Trust & Security issues in Mobile banking and its effect on Customers.

Retrieved from https://www.diva-portal.org/smash/get/diva2:830466/FULLTEXT01.pdf

Birkeland, S. N. (2015). *E-Banking security and organisational changes: an action research study* (Doctoral dissertation, University of Liverpool). Retrieved from https://livrepository.liverpool.ac.uk/3001088/1/2005422393_Aug2015.pdf

CloudMosa, Inc. (2018).The Vulnerability of Digital Banking . Available at:https://medium.com/@CloudMosa/the-vulnerabilities-of-digital-banking-7073b36334b

Cyber Security Awareness Forum (Business & Financial Times, Nov 2, 2018, ISSUE 2735, (ISSN) 0855-1812 Page 3)

(BOG Cyber and Information Security Directives -Document, October 2018.) Retrieved from www.bog.gov.gh

BOG Directives on Cyber and Information Security. Retrieved from (https://www.myjoyonline.com/business/2018/october-24th/bog-launches-cyber-security-directive-for-financial-institutions.php)

BSP, (2006). Electronic banking consumer awareness program for internet products and services. Circular No. 542

(FDIC Consumer News, Winter,2016) A Bank Customer's Guide to Cybersecurity. Retrieved from https://www.fdic.gov/consumers/consumer/news/cnwin16/May 23, 2017

GCB Bank Product Offering. Available at https://www.gcbbank.com.gh/index.php/personal/eproducts-cards/mobile-banking

Georgescu, M. (2006). Some issues about risk management for e-banking. *Available at* https://ssrn.com/abstract=903419

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 24. doi: 10.1177/1525822X05279903

Hanson, E.A. (2018). Cyber Security is Everyone's responsibility, The Ghanaian Banker, Journal of the Chartered Institute of Bankers (Ghana), Vol. 2, pp. 28

Horst, M., Kuttschreuter, M., and Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. Computers in Human Behavior, 23(4), 1838-1852

Jay J.(2018).Two-Thirds of Online Banking Systems Contain Critical Vulnerabilities, Available at https://www.teiss.co.uk/threats/online-banking-systems-vulnerabilities/

Khan, F.H. (2017). "E-Banking: Benefits and Related Issues", American Research Journal of Business and Management, Vol.3, (I1) pp. 1-7

Kiljan, S.Z. (2017). Exploring, Expanding and Evaluating Usable Security in Online Banking. Retrieved from https://cybersciencecenter.nl/media/1096/sven-kiljan-phd-thesis.pdf

Kaleem, A & Ahmad, S. (2008). Bankers" Perceptions of Electronic Banking in Pakistan. Journal of Internet Banking and Commerce, Vol. 13, No.1.

Latham, J. (2014). Qualitative sample size: How many participants is enough. *John R. Latham, Ph. D.* Available at https://www.drjohnlatham.com/many-participants-enough/

Munir, M. M. M. (2017). An Empirical Study on Risks and Benefits of E-banking in Context of Employee Satisfaction in Rajshahi Division, Bangladesh. Available at

https://pdfs.semanticscholar.org/2e56/8602a3854c3a17e1ba25fc4d9d734abcc48b.pdf.

Nasri, W. (2011). Factors Influencing the Adoption of Internet Banking in Tunisia, International Journal of Business and Management, 6(8), 143-160

Positive Technologies Report (2017). Retrieved from https://www.teiss.co.uk/threats/online-banking-systems-vulnerabilities

Singh, T. (2015). Security and Privacy Risks in E-Banking, An Empirical Study of Customers‟ Perception”**.** Retrieved from http://www.iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdfJun 4

Sravanthi, G. (2016). Management of Risk Issues in E-Banking–A Case Study. *International Journal of Recent Research Aspects*, *3*(3), 38-44. Available at https://www.ijrra.net/Vol3issue3/IJRRA-03-03-08.pdf

The Annual Banker Africa Awards (2016) Available at https://www.gcbbank.com.gh/news-from-gcb/301-gcb-is-the-best-retail-bank-the-banker.html

Utakrit, N. (2012). Security awareness by online banking users in Western Australian of phishing attacks. Available at https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=&httpsredir= 1&article= 1504&context=theses

APPENDIX 1

INTERVIEW QUESTIONS

Dear Respondent,

My name is Dickson Serebour Taylor, an MSC Accounting and Finance student with the University of Ghana Business School, who is researching on the topic "**Users' Perspectives of E-Banking Risk Issues and the Control Measures to Manage the Identified Risk"**. The purpose of this study is to investigate into the issues and risk associated with electronic banking and control measures to address the identified risk of electronic banking.

The information you provide will be kept with utmost confidentiality and anonymity as they are purely for academic purposes. Your participation is voluntary. If you agree to participate, please provide answers that reflect your candid opinion on the questions below. If you have any questions, do not hesitate to contact using the following phone numbers: **0244292792 /0201513756**

Section A:

Biographical data

I. Age (in completed years)

☐ Under 20 ☐ 21 - 30 ☐31 - 40 ☐41 - 50-☐ 50 – 59 ☐ 60+

II. Gender: ☐ Male ☐Female

III. Academic Qualification: ☐ WASSCE/O'Level ☐Diploma/HND

☐First Degree ☐Postgraduate ☐Professional

IV. How many years have you been a customer of GCB Bank?

☐ 0 – 2-☐ 3 – 5 ☐6 – 10 ☐11 – 15 ☐16 – 20 ☐above 20

V. Are you a user of any of the electronic banking products of GCB Bank? (YES or NO)

VI. If YES, which of them have you used before or currently using

……

Section B:

Knowledge about GCB Bank E-Banking products/services

1. Please list the E-Banking products/services of GCB Bank:
   a. …….
   b. …….
   c. ……..
   d. …….
   e. …….
   f. ……..
2. Kindly state the types of E-Banking transaction activities offered by GCB Bank:
   g. …….
   h. …….
   i. ……..
   j. …….
   k. ……
3. Please state the types of e-banking non-transaction activities offered by GCB Bank
   a. ……
   b. ……

c. …….

d. …….

e. …….

4. Please indicate which of GCB Bank E-Banking services you frequently use?

……. …….

5. Kindly state how frequently you use GCB electronic banking services?

…….

Section C:

Customer Satisfaction of the E-Banking services

6. Kindly mention some of the benefits you derive from GCB Bank E-Banking services:

a. …….

b. ……

c. ……

7. Kindly state GCB Bank E-Banking services you are not satisfied with.

……

……

Section D:

Security Implications and how to manage

8. Please mention any issues/challenges you face when using GCB Bank E-Banking services

……

……

8. (a) Kindly state any risk you are likely to be exposed to by using GCB Bank E-Banking service……

……

8. (b) Please what is cyber-crime and its management?

……

……..

8. (c) Please what personal safeguard measures do you put in place to prevent any identified risk of GCB E-Banking services.

……

……

9.Kindly suggest strategies to manage E-Banking risk

……

……

10. Please share with me any safety messages GCB Bank has sent to you to prevent unauthorized access to E-Banking services.

……

……

Thank you for your time...