

SECURITY ISSUES IN ELECTRONIC BANKING
A CASE OF EQUITY BANK KENYA KIKUYU BRANCH

BY

MUGANE NAFTALY KAMITHA BCS/16309/71/DF

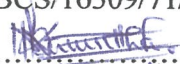
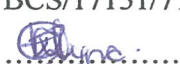
MWAI EVALYNE WAIRIMU BCS/17131/71/DF

**A PROJECT REPORT SUBMITTED TO THE SCHOOL OF COMPUTER
STUDIES IN PARTIAL FULFILMENT FOR THE AWARD OF
A BACHELORS DEGREE OF COMPUTER SCIENCE
OF KAMPALA INTERNATIONAL
UNIVERSITY**

JUNE, 2010

DECLARATION

We, Mugane Naftaly Kamitha and Mwai Evalyne Wairimu, declare that this research project is from our own findings and has never been produced by any body else for the same award in our institution.

Name of student:	Mugane Naftaly Kamitha	Mwai Evalyne Wairimu
Reg-No:	BCS/16309/71/DF.	BCS/17131/71/DF
Signature:		
Date:	23/06/2010	23/06/2010

APPROVAL

This is to approve that this Research Project entitled SECURITY ISSUES IN ELECTRONIC BANKING was written and conducted under my supervision.

Ms. ESTHER WABULE

Signature: Esther Wabule Date: 23/06/10

DEDICATION

To God Almighty and my family especially my dad Ephantus and my mum Hellen as it is through their guidance and support that it was a success, My brothers Anthony and Patrick and my sisters Grace and Jennifer and my best friend Evalyne.

- Naftaly

To God Almighty and my mum Nancy Mwai as it is through her guidance and support that it was a success. Special thanks go to my best friend Naftaly who supported and encouraged me to work hard and succeeded in my research dissertation

- Evalyne

ACKNOWLEDGEMENT

We would especially recognize the contribution of our parents who used all their possible means to meet all our expenses throughout our entire course in the university.

We also would like to thank our supervisor Ms Esther Wabule though on a busy schedule offered some of her time to supervise us thereby contributing greatly in the effective and efficient completion of this research dissertation.

We would also like to thank management of Equity bank Kikuyu branch (Kenya) and staff for making our project a success through the responses we got from the questionnaires we administered and the interviews we conducted.

We can't forget to thank our best friends Felix, Maurice, Jimwat, Hillah, Jael, Elly, Mbuchu, my sister Rosa Mwai and Dr. Roseann Mwaniki for their encouragement during our stay and writing of our research project.

Thanks and may God Almighty bless them.

ABSTRACT

The study was about addressing the security issues in e-banking a case study of Equity bank Kikuyu branch (Kenya). The specific objective of the study was to address the security risks experienced while using e-banking at Equity bank Kikuyu branch.

Chapter one established the background of the study, the statement of the problem, the purpose of the study which was to address the security issues in electronic banking at Equity bank Kikuyu branch (Kenya), the research objectives; to address the security risks in e-banking, to address the security responses in e-banking and to address the security risks management or measures in e-banking, the research objectives were used to formulate the research questions, the scope of the study was restricted to Equity bank Kikuyu branch (Kenya), and the significance of the study; which was necessary to address the security breaches like breaches with serious criminal intent, breaches by casual hackers of which these threats gave potentially serious financial, legal and reputational implications. It also helped address the security responses to be taken once any issue of security in electronic banking was experienced.

Chapter two was about the literature review of security-, the theoretical framework of the study and also discussed the research objectives in depth. Chapter three was about the research methodology employed, the research design used was both qualitative and quantitative, area of study Equity bank Kikuyu Branch (Kenya), and the study population was the employees of Equity bank Kikuyu Branch (Kenya) of the various departments. The sample design used was random sampling and the sample size was 60 respondents. Primary & secondary data sources were used for data collection through the use of interviews and questionnaires. Limitations of the study which were inadequate information, limited time & financial constraints.

ABBREVIATIONS

PC:-Personal Computer

PDA:-Personal digital assistant

ATM: -Automated Teller Machine

PIN: -Personal Identification Number

IDN: -Internationalized Domain Number

URL: -Unified Resource Locator

IP: -Internet Protocol

VOIP: -Voice Over Internet Protocol

MITM: -Man In the Middle Attack

ARP: -Address Resolution Protocol

ICMP: -Internet Control Message Protocol

IRC: -Internet Relay Chat

DDOS:-Distributed denial of service

LAN: - local area network

TABLE OF CONTENTS

COVER PAGE	
DECLARATION.....	i
APPROVAL.....	ii
DEDICATION.....	iii
ACKNOWLEDGEMENT.....	iv
ABSTRACT.....	v
ABBREVIATIONS.....	vi
TABLE OF CONTENTS.....	vii
LIST OF TABLES.....	x
LIST OF FIGURES.....	xi
CHAPTER ONE:.....	1
INTRODUCTION	1
1.0 Introduction	1
1.1 Background to the study.....	1
1.2 Statement of the problem.....	2
1.3 Objectives of the study	2
1.3.1. Main objectives.....	2
1.3.2 Specific objectives.....	3
1.4 Research questions	3
1.5 Significance of the study	3
1.6 Justification of the study.....	3
1.7 Scope of the study.....	4
CHAPTER TWO.....	5
LITERATURE REVIEW	5
2.0 Introduction	5
2.1 Definition of concepts	5
2.2 SECURITY RISKS:	5
2.2.1 Unauthorized access (Hacking).....	6
2.2.1.1 Internal and external hacking	6
2.2.1.2 Modes of external attack.....	6
2.2.1.3 Modes of internal attack	7
2.2.2 PHISHING:	8
2.2.2.1 Phishing techniques:.....	9
2.2.2.1.1 Filter evasion	9
2.2.2.1.2 Website forgery	9
2.2.2.1.3 Phone phishing	10
2.2.2.1.4 Other techniques:.....	10
2.2.3 PACKET SNIFFING.....	10
2.2.4 SPYWARE	11
2.2.5 MAN IN THE MIDDLE ATTACKS:.....	11
2.2.6 Attacks on Local Networks	12
2.2.7 SYN Flooding:.....	12
2.2.8 Smurfing:.....	13
2.2.9 Distributed Denial-of-service Attacks:	13
2.2.10 Spam and Address Forgery:	14
2.2.11 Spoofing Attack:.....	14
2.2.11.1 IDN SPOOFING (internationalized domain names).....	15

2.2.11.2 Webpage spoofing	15
2.2.11.3 Caller ID spoofing:	16
2.2.11.4 E-mail addresses spoofing	16
2.2.12 Routing Attacks:	16
2.3 SECURITY RISKS RESPONSES MANAGEMENT:	17
2.3.1 Phishing management:.....	17
2.3.2 Man in the middle attacks:.....	17
2.3.3 Defenses against the attack:.....	17
2.3.4 Quantum cryptography:	18
2.3.5 Beyond cryptography	18
2.3.6 Anti-phishing:.....	18
2.3.6.1 Social responses:.....	18
2.3.6.2 Technical responses	19
2.3.7 Eliminating phishing mail	19
2.3.8 Monitoring and takedown.....	19
2.3.9 INFORMATION SECURITY.....	19
2.3.10 AUTHENTICATING E-BANKING CUSTOMERS.....	24
2.3.10.1 Authenticating New Customers.....	25
2.3.10.2 Authenticating Existing Customers	25
2.3.10.3 Password Administration.....	26
CHAPTER THREE.....	29
METHODOLOGY	29
3.0 Introduction	29
3.1 Research design	29
3.2 Area of study	29
3.3 Study Population.....	29
3.4 Sample Size	29
3.5 Data collection techniques.....	29
3.6 Questionnaires	30
3.7 Interviews	30
3.8 Document analysis.....	30
3.8.1 Advantage of this method.....	30
3.8.2 Disadvantage of this method	30
CHAPTER FOUR	33
FINDINGS, ANALYSIS AND PRESENTATION OF DATA	33
4.0 Introduction	33
4.1 Data Analysis.....	33
4.1.1 Respondents by sex.	33
4.1.2 Respondents by age groups	34
4.1.3 Respondents by Education level.....	35
4.1.4 Classification of respondents by designation	36
4.1.5 Respondents by marital status.	37
4.2 Addressing the security risks in electronic banking.	38
4.3 addressing the security risks responses in electronic banking.....	45
4.4 addressing the security risks measures or management in electronic banking	46

CHAPTER FIVE	49
DISCUSSION, CONCLUSION AND RECOMMENDATION	49
5.0 Introduction	49
5.1 Discussion of the Findings.	49
5.1.1 Addressing the security risks in electronic banking.	49
5.1.2 Addressing the security risks responses in electronic banking.....	50
5.1.3 Addressing the security risks measures or management in electronic banking	51
5.2 Conclusions.	51
5.3 Recommendations.	52
5.4. Areas for Further Research.....	52
5.5 Limitations of the study.....	53
REFERENCE:	54
APPENDICES.....	55
APPENDIX A: QUESTIONNAIRES	55
APPENDIX B: INTERVIEW GUIDE	57

LIST OF TABLES

Table 4.1(a).....	34
Table 4.1(b).....	35
Table 4.1(c).....	36
Table 4.1(d).....	37
Table 4.1(e).....	38
Table 4.2(a).....	39
Table 4.2(b).....	40
Table 4.2(c).....	41
Table 4.2(d).....	42
Table 4.2(e).....	44
Table 4.2(f).....	45
Table 4.3(a).....	46
Table 4.4(a).....	48

LIST OF FIGURES

Figure 1.0.....	13
Figure 4.1(a).....	35
Figure 4.1(b).....	36
Figure 4.1(c).....	37
Figure 4.1(d).....	38
Figure 4.2(a).....	40
Figure 4.2(b).....	41
Figure 4.2(c).....	42
Figure 4.2(d).....	43
Figure 4.2(e).....	44
Figure 4.2(f).....	45
Figure 4.3(a).....	47
Figure 4.4(a).....	49

CHAPTER ONE:

INTRODUCTION

1.0 Introduction

With the market more aware of the internet, and the desire for online real time information growing with a very high rate, electronic payment was gaining prominence and with it, the issues of security arose. According to HSBC India Head Global Payment & cash management Arjun Bambawale “As payments increasingly become electronic, banks and financial institutions, business, government and consumers are the ones who will be impacted the most”.

This study addressed the security risks, security risks management and control in electronic banking.

1.1 Background to the study.

E-banking is the automated delivery of new and traditional banking products and services directly to the customer through electronic, interactive communication channels which the system that enable financial institutional customers, individuals or individuals or businesses, to access accounts, transact business or obtain information on financial products and services through a public or private network, including the internet by the use of personal computers, personal digital assistants, ATMs, kiosks or touchtone telephones. (John Leyden, 2005)

Due to the rapid growth of e-banking, e-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments of which this security threats needs monitoring and management. Security issues being a major source of concern for everyone both inside and outside the banking industry necessitated the need to take special attention and caution with the security issues in electronic banking which when ignored could have led to potentially serious financial legal and reputational implications . (John Leyden, 2005)

Equity Bank commenced business on registration in 1984. It has evolved from a Building Society; a Microfinance Institution to now the all inclusive Nairobi Stock Exchange and Uganda Securities Exchange public listed Commercial Bank. With over 4.1 million accounts, accounting for over 52% of all bank accounts in

Kenya, Equity Bank is the largest bank in the region in terms of customer base. The solidness of Equity Bank is underpinned by its shareholder's funds base of over Kshs 19 billion, making Equity Bank one of the most capitalized banks in the region. Equity Bank has received both local and global accolades for its unique and transformational financial model. The bank is credited for taking banking services to the people through its accessible, affordable and flexible service provision. Equity bank Kenya Kikuyu branch is located in Nairobi province, Kabete constituency in Kikuyu town.

This project also addressed on the security risks, responses and security risks management in e-banking thereby minimizing the implications named above.

1.2 Statement of the problem

The rapid growth of individuals accessing e-banking services or advancement of e-banking services had led to many forms of security risks and inefficiencies in e-banking.

Security risks like network attacks, Inefficient authentication processes necessary to initially verify the identities of individuals or businesses applying for new accounts or credit online leading to unauthorized access, emerging threats like phishing, man in the middle schemes, spy ware scams, Pharming, SYN flooding, spam and address forgery, packet sniffing, Smurfing, hackers were common in e-banking.

Addressing these security risks without impairing further development of e-banking, a platform popular with customers and rich in potential for advances in productivity, efficiency, quality and range of services.

This security risks leads to potentially serious financial legal and reputation implications in e-banking.

1.3 Objectives of the study

1.3.1. Main objectives

To address on the security issues in e-banking by verifying the identities of customers and authorizing e-banking activities for faster, efficient and secure banking services as e-banking is a platform popular with customers and rich in potential for advances in productivity and efficiency.

1.3.2 Specific objectives

The following were the objectives under which the research was carried out;

- ✓ To address the security risks in e-banking
- ✓ To address the security responses in e-banking
- ✓ To address the security risks management in e-banking
- ✓ To establish the best practice security control in e-banking

1.4 Research questions

- ✓ Did addressing the security risks minimize the potentially serious financial, legal and reputation implications in e-banking?
- ✓ Did addressing the security responses minimize the potentially serious financial, legal and reputation implications in e-banking?
- ✓ Did addressing the security risk management minimize the potentially serious financial, legal and reputation implications in e-banking?

1.5 Significance of the study

This study was necessary as it addressed the security breaches like breaches with serious criminal intent, breaches by casual hackers of which these threats gave potentially serious financial, legal and reputational implications.

The study also addressed the security responses to be taken once any issue of security in electronic banking arose or was experienced.

1.6 Justification of the study

This study minimized the issues of security experienced in electronic banking since the study addressed on the attention of special management to the security control processes posed by e-banking like establishing appropriate authorization privileges and authentication measures, logical and physical access controls.

This study helped to minimize the potentially serious financial, legal and reputational implications with e-banking activities conducted both domestically and cross border, by making adequate disclosure of information by banks on their websites and taking appropriate measures to ensure adherence to customer privacy requirements. The study also enhanced the safety of financial institutions, as well as the integrity of the nation's payments system and built customers confidence in the system.

1.7 Scope of the study

The study was basically focused on addressing the security breaches/risks like unauthorized access, network attacks, emerging threats like phishing, spear phishing. The study will also address on the special management attention to the security control processes posed by e-banking.

The study also addressed on the security responses to be taken once there was any issue of security in e-banking.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

In this chapter we addressed the security risks, security risks management and security responses encountered in electronic banking.

2.1 Definition of concepts

E-banking is the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. It includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet.

Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone.(Carol Sergeant, 2000)

2.2 SECURITY RISKS:

With the growth of electronic banking had come new forms of security risks. The challenge was to address these risks without impairing further development of electronic banking, a platform popular with customers and rich in potential for advances in productivity, efficiency, and quality and range of services. (John Howard, 1996)

Security risks encountered in electronic banking which were addressed in this study were;

- ⌞ Unauthorized access(Hacking)
- ⌞ Phishing
- ⌞ Pharming
- ⌞ Packet sniffing
- ⌞ Spy ware
- ⌞ Man in the middle attacks
- ⌞ Attacks on local networks
- ⌞ SYN flooding
- ⌞ Smurfing

- ⌞ Distributed denial of service attacks
- ⌞ Spam and address forgery
- ⌞ Spoofing attacks
- ⌞ Routing attacks

2.2.1 Unauthorized access (Hacking)

A hacker is one who hacks.

Hacker (computer security) or *cracker*, who accesses a computer system by circumventing its security system, (Virus Bulletin, 2005)

2.2.1.1 Internal and external hacking

Computer security specialists normally distinguish between internal and external network attacks. This is because intruder profiles, methods of attack and intruder objectives can vary significantly between internal and external attacks.

Attacks where the intruder has no privileges on the target network, and either gains access from outside the network perimeter (usually the firewall), or by evading or undermining the target's physical and/or network security measures to achieve some degree of access to the target's internal network. (Stutz, Michael, 1998). Attacks where the intruder has legitimate privileges on the target network. Access is obtained using existing privileges, privileges the intruder has extended without permission, or privileges stolen from other users. The objective of the intrusion is to gain access to data and resources to which the intruder is not authorized. (Candid Wueest, 2005)

2.2.1.2 Modes of external attack

The principal mode of external hacking seen in Ireland is based on simple credential theft, i.e. stealing or guessing another user's password and using it to gain access (Virus Bulletin, 2005) but there are many other ways of compromising a computer network from the outside:

- ✓ **Access through weak, stolen or lost credentials.** The most common form of attack.
- ✓ **Access through malware infection.** Another common mode of attack. An insider activates a "Trojan Horse" program, intentionally or unintentionally, that opens access to their network.

- ✓ **Access through compromise of remote access systems.** Making use of the target's own remote access connections.
- ✓ **Compromised third-party access.** Instead of hacking the target, the attacker hacks an individual or organisation known to have access to the target's systems.
- ✓ **Access through physical penetration.** Gaining access to computer networks by actually entering the target's premises
- ✓ **Access through modem dial-up.** Some organisations still maintain dial-in connections for legacy systems. These can be very insecure.
- ✓ **Unauthorized access with co-operation of the organisation's staff.** By threatening or subverting members of staff or placing confederates on the staff of the target organisation.
- ✓ **Access through wireless systems.** Wireless (WiFi) connections are particularly problematic as they can be difficult to set up securely, can be cheaply set up on networks by users without the knowledge of IT staff and if compromised can provide direct access to internal systems, bypassing network perimeter security.
- ✓ **Direct penetration through perimeter systems.** Perhaps the most difficult and least common approach.

2.2.1.3 Modes of internal attack

Internal attacks are considerably more common than external ones. "Insiders" already have credentials and privileges on the target network, and have direct access to systems. Computers inside the network's secure perimeter. Insiders usually have more time and Opportunities to discover how to gain access to restricted systems and directories. They are also more likely to know which computers contain the material of most value to them. (Candid Wueest, 2005)

- ✓ **Unauthorized access by IT personnel.** In Irish organisations a disproportionate amount of unauthorised access is carried out by members of the IT staff, largely because they are most likely to have high-level computer security privileges.
- ✓ **Unauthorised access by non-IT staff with high-level privileges.** Non-IT users should not, generally, have high-level network security privileges, but

we occasionally find cases where this has happened. In other cases we have seen non-IT users obtain these privileges through hacking, persuasion, bribery, threats or outright theft.

- ✓ **Access through theft of other users' credentials.** Some ordinary users are given access to systems restricted to others. It is not uncommon to find such credentials stolen from their holders, or even voluntarily shared by them.
- ✓ **Access to inadequately secured systems.** Some sensitive systems are simply not given sufficient protection, and can be straightforwardly compromised by intruders without high level privileges. (Candid Wueest, 2005)

2.2.2 PHISHING:

A Phishing technique was described in detail in 1987, and the first recorded use of the term "Phishing" was made in 1996. The term is a variant of *fishing*, probably influenced by phreaking, and alludes to baits used to "catch" financial information and passwords. (Josang, Audin et al, 2007)

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication, it may require tremendous skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies; Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. (Ollmann Gunter, 2006)

Phishing can also be viewed as a situation where criminals use counterfeit e-mails and fake websites to entice the cardholder into revealing personal account details or online banking access information, like PIN codes. And this is just the start. The fraudsters

are becoming ever more ingenious, their techniques more sophisticated, and their appearance more professional. ((Josang, Audin et al, 2007))

2.2.2.1 Phishing techniques:

Phishers are targeting the customers of banks and online payment services. E-mails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers. Recent research has shown that Phishers may in principle be able to determine which banks potential victims use, and target bogus e-mails accordingly. Targeted versions of Phishing have been termed **spear Phishing**. Several recent Phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term **whaling** has been coined for these kinds of attacks. Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by **Phishers**. (Ollmann Gunter, 2006).

Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site. A further problem with URLs has been found in the handling of internationalized domain names (IDN) in web browsers that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or homograph attack, phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain (Josang, Audin et al, 2007)

2.2.2.1.1 Filter evasion

Phishers use images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails. (Josang, Audin et al, 2007)

2.2.2.1.2 Website forgery

Once a victim visits the phishing website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as **cross-site scripting**) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal. (Josang, Audin et al, 2007)

2.2.2.1.3 Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phishers, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization. (Tan Koon, 1905)

2.2.2.1.4 Other techniques:

Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information. (Josang, Audin et al, 2007)

2.2.3 PACKET SNIFFING

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. (Bill Cheswick, 1994)

In its simple form a packet sniffer simply captures all of the packets of data that pass through a given network interface. Typically, the packet sniffer would only capture packets that were intended for the machine in question. However, if placed into promiscuous mode, the packet sniffer is also capable of capturing **ALL** packets traversing the network regardless of destination.

A packet sniffer can only capture packet information within a given subnet. So, its not possible for a malicious attacker to place a packet sniffer on their home ISP network and capture network traffic from inside your corporate network (although there are ways that exist to more or less "hijack" services running on your internal network to effectively perform packet sniffing from a remote location). In order to do so, the packet sniffer needs to be running on a computer that is inside the corporate network as well. However, if one machine on the internal network becomes compromised through a Trojan or other security breach, the intruder could run a packet sniffer from that machine and use the captured username and password information to compromise other machines on the network. (Bill Cheswick, 1994)

2.2.4 SPYWARE

Spyware is a type of malware that is installed on computers and collects little bits information at a time about users without their knowledge. The presence of Spyware is typically hidden from the user, and can be difficult to detect. Typically, spy ware is secretly installed on the user's personal computer. Sometimes, however, Spyware such as key loggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users. (John Howard, 1996)

Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. In an attempt to increase the understanding of spy ware, a more formal classification of its included software types is captured under the term privacy-invasive software. (John Howard, 1996)

2.2.5 MAN IN THE MIDDLE ATTACKS:

The **man-in-the-middle attack** (often abbreviated **MITM**), or **bucket-brigade attack**, or sometimes **Janus attack**, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle). (Bill Cheswick, 1994)

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, SSL authenticates the server using a mutually trusted certification authority. (Steve Bellovin, 1994)

2.2.6 Attacks on Local Networks

Let's suppose that the attacker is one of your employees; he has a machine attached to Your LAN, and he wants to take over an account in someone else's name to commit a fraud. Given physical access to the network, he can install packet sniffer software to harvest passwords, get the root password, and create a suitable account. However, if Your staff use challenge-response password generators, or are careful enough to only Use a root password at the keyboard of the machine it applies to, then he has to be more subtle. (Steve Bellovin, 1994)

One approach is to try to masquerade as a machine where the target user has already logged on. ARP is one possible target; by running suitable code, the attacker can give Wrong answers to ARP messages and claim to be the victim. The victim machine might notice if alert, but the attacker can always wait until it is down—or take it down by using another attack. One possibility is to use subnet masks. (Stutz, Michael, 1998).

2.2.7 SYN Flooding:

The SYN flood attack is, simply, to send a large number of SYN packets and never Acknowledge any of the replies. This leads the recipient to accumulate more records of SYN packets than his software can handle. This attack had been known to be theoretically possible since the 1980s, but came to public attention when it was used to bring down Panix, a New York ISP, for several days in 1996. A technical fix, the so-called SYNcookie, has been found and incorporated in Linux and some other systems. Rather than keeping a copy of the incoming SYN packet, B simply sends out

as Y an encrypted version of X. That way, it's not necessary to retain state about sessions that are half-open. (Bill Cheswick, 1994)

Figure 1.0

A	→	B:	SYN; my number is X
B	→	A:	ACK; now X+1
			SYN; my number is Y
A	→	B:	ACK; now Y+1
			(start talking)

TCP/IP handshake.

2.2.8 Smurfing:

Another common way of bringing down a host is known as smurfing. This exploits the Internet Control Message Protocol (ICMP), which enables users to send an echo packet to a remote host to check whether it's alive. The problem arises with broadcast addresses that are shared by a number of hosts. Some implementations of the Internet protocols respond to pings to both the broadcast address and their local address (the idea was to test a LAN to see what's alive). So the protocol allowed both sorts of behavior in routers. A collection of hosts at a broadcast address that responds in this way is called a smurf amplifier. (Bill Cheswick, 1994)

The attack is to construct a packet with the source address forged to be that of the victim, and send it to a number of smurf amplifiers. The machines there will each respond (if alive) by sending a packet to the target and this can swamp the target with more packets than it can cope with. Smurfing is typically used by someone who wants to take over an Internet relay chat (IRC) server, so they can assume control of the chat room. The innovation was to automatically harness a large number of "innocent" machines on the network to attack the victim. (Bill Cheswick, 1994)

2.2.9 Distributed Denial-of-service Attacks:

In the distributed denial of service (DDoS) attack, Rather than just exploiting a common misconfiguration as in Smurfing, an attacker subverts a large number of

machines over a period of time, and installs custom attack software in them. At a predetermined time, or on a given signal, these machines all start to bombard the target site with messages. They are even more disruptive, as they target services such as DNS and thus take down the entire Internet. Such an attack might be expected in the event of information warfare; it might also be an act of vandalism by an individual. At the time of writing, the initiative being taken against DDoS attacks is to add ICMP trace back messages to the infrastructure.

The idea is that whenever a router forwards an IP packet, it will also send an ICMP packet to the destination with a probability of about 1 in 20,000. The packet will contain details of the previous hop, the next hop, and as much of the packet as will fit. System administrators will then be able to trace large-scale flooding attacks back to the responsible machines, even when the attackers use forged source IP addresses to cover their tracks. It may also help catch large-scale spammers who abuse *open relays* – relays allowing use by "transit" traffic, that is, messages which neither come from nor go to email addresses for which that SMTP server is intended to provide service. (Bill Cheswick, 1994)

2.2.10 Spam and Address Forgery:

Services such as email and the Web (SMTP and HTTP) assume that the lower levels are secure. The most that's commonly done is a look-up of the hostname against an IP address using DNS. So someone who can forge IP addresses can abuse the facilities. The most common example is mail forgery by spammers; there are many others. For example, if an attacker can give DNS incorrect information about the whereabouts of your company's Web page, the page can be redirected to another site—regardless of anything you do, or don't do, at your end. As this often involves feeding false information to locally cached DNS tables, it's called DNS cache poisoning. (Steve Bellovin, 1994)

2.2.11 Spoofing Attack:

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. (Steve Bellovin, 1994)

2.2.11.1 IDN SPOOFING (internationalized domain names)

This is a type of a spoofing attack whereby there is a problem with URLs in handling of internationalized domain names (IDN) in the web browsers that might allow visually identical web addresses to lead to different, possibly malicious websites despite the publicity surrounding the flaw. (Terry Escamilla, 1994)

We can combine some of the preceding ideas into spoofing attacks that work at long range (that is, from outside the local network or domain). Say that Charlie knows that Alice and Bob are hosts on the target LAN, and wants to masquerade as Alice to Bob. He can take Alice down with a service denial attack of some kind, and then initiate a new connection with Bob [559, 90]. This entails guessing the sequence number Y , which Bob will assign to the session, under the protocol shown in Figure 1. A simple way of guessing Y , which worked for a long time, was for Charlie to make a real connection to Alice shortly beforehand and use the fact that the value of Y changed in a predictable way between one connection and the next. Modern stacks use random number generators and other techniques to avoid this predictability, but random number generators are often less random than expected—a source of large numbers of security failures [774]. (Terry Escamilla, 1994)

If sequence number guessing is feasible, then Charlie will be able to send messages to Bob, which Bob will believe come from Alice (though Charlie won't be able to read Bob's replies to her). In some cases, Charlie won't even have to attack Alice; just arrange things so that she discards Bob's replies to her as unexpected junk. This is quite a complex attack, but no matter; there are scripts available on the Web that does it. (Terry Escamilla, 1994)

2.2.11.2 Webpage spoofing

In this attack, a legitimate webpage such as a bank's site is reproduced in 'look and feel' on another server under control of the attacker. The main intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest usernames and passwords.

This attack is performed with the aid of **URL spoofing**, which exploits web browsers bugs in order to display incorrect URLs in the browsers location bar; or with the DNS cache poisoning in order to direct the user away from the legitimate site and to fake

one. Once the user puts their password, the attack code reports a password error, and then redirects the user back to the legitimate site. (Terry Escamilla, 1994)

2.2.11.3 Caller ID spoofing:

With public telephone networks, it has for a long while been possible to find out who is calling you by looking at the caller ID information that is transmitted with the call. There are technologies that transmit this information on landlines, on cell phones and also with VoIP. Unfortunately, there now technologies especially associated with VoIP that allow callers to lie about their identity, and present false names and numbers, which could of course used as a tool to defraud or harass. (Terry Escamilla, 1994)

2.2.11.4 E-mail addresses spoofing.

The sender information shown in e-mails (the “FROM” field) can be spoofed easily. This technique is commonly used by spammers to hide the origin of their e-mails and leads to problems such as misdirected bounces like e-mail spam backscatter. E-mail address spoofing is done in quite the same way as writing a forged return address using snail mail. As long as the letter fits the protocol, like stamp, postal code, the SMTP protocol will send the message. It can be done using a mail server with telnet. (Terry Escamilla, 1994)

2.2.12 Routing Attacks:

Routing attacks come in a variety of flavors. The basic attack involves Charlie telling Alice and Bob that a convenient route between their sites passes through his. Source level routing was originally introduced into TCP to help get around bad routers. The underlying assumptions—that “hosts are honest” and that the best return path is the best source route—no longer hold, and the only short-term solution is to block source routing. However, it continues to be used for network diagnosis. Another approach involves redirect messages, which are based on the same false assumption.

These effectively say, “You should have sent this message to the other gateway instead,” and are generally applied without checking. They can be used to do the same subversion as source-level routing. Spammers have taught almost everyone that mail forgery is often trivial. Rerouting is harder, since mail routing is based on DNS; but it is getting easier as the number of service providers goes up and their competence goes

down. DNS cache poisoning is only one of the tricks that can be used. (Berners-Lee, Tim, 2006)

2.3 SECURITY RISKS RESPONSES MANAGEMENT:

2.3.1 Phishing management:

Good practice guidelines advise you: check the credibility of an unsolicited email supposedly from your bank or building society; never enter a full password or your PIN details (internet banking systems ask for random characters in order to login); remember rather than note down your security details; choose secure passwords; install and regularly update anti-virus, firewall, anti-spam and anti-spy ware software; check that a secure connection is established via a https:// website and verify there is a security certificate for the web browser. Using a secure computer to access online services is paramount to protecting the contents of an account, especially current accounts that provide instant access to funds. (Josang, Audin et al, 2007)

To combat the phishing problem, the advice for customers is to avoid responding directly to phone calls or links in messages that purport to be from their bank and instead initiate a call to the customer service number themselves to verify that any communication previously received is legitimate. (Josang, Audin et al, 2007)

2.3.2 Man in the middle attacks:

2.3.3 Defenses against the attack:

Various defenses against MITM attacks use authentication techniques that are based on:

- ✓ Public key infrastructures
- ✓ Stronger mutual authentication
- ✓ Secret keys (high information entropy secrets)
- ✓ Passwords (low information entropy secrets)
- ✓ Other criteria, such as voice recognition or other biometrics
- ✓ Diffie-Hellman key exchange, particularly for Off-the-Record Messaging for instant messaging
- ✓ Off-channel verification
- ✓ Carry-forward verification

The integrity of public keys must generally be assured in some manner, but need not be secret. Passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a Certificate Authority, whose public key is distributed through a secure channel (for example, with a web browser or OS installation). Public keys can also be verified by a web of trust that distributes public keys through a secure channel (for example by face-to-face meetings). (Josang, Audin et al, 2007)

2.3.4 Quantum cryptography: Quantum cryptography protocols typically authenticate part or all of their classical communication with an unconditionally secure authentication scheme (e.g. Wegman-Carter authentication). (Tan, Koon, 1905)

2.3.5 Beyond cryptography: MITM should be seen as a general problem resulting from the presence of intermediate parties acting as proxy for clients on either side. If they are trustworthy and competent, all may be well; if they are not, nothing will be. How can one distinguish the cases? By acting as proxy and appearing as the trusted client to each side, the intermediate attacker can carry out much mischief, including various attacks against the confidentiality or integrity of the data passing through it. A notable non-cryptographic man-in-the-middle attack was perpetrated by one version of a Belkin wireless network router in 2003. Periodically, it would take over an HTTP connection being routed through it: it would fail to pass the traffic on to destination, but instead itself respond as the intended server. The reply it sent, in place of the web page the user had requested, was an advertisement for another Belkin product. (Tan, Koon, 1905)

2.3.6 Anti-phishing:

There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing.

2.3.6.1 Social responses:

One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback. One newer phishing tactic, which uses phishing e-mails targeted at a specific company, known as *spear phishing*, has been harnessed to train individuals at various locations. It is a sensible precaution to contact the company from which the e-

mail apparently originates to check that the e-mail is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message. It unsafe to assume that the presence of personal information alone guarantees that a message is legitimate. (Josang, Audin et al, 2007)

2.3.6.2 Technical responses

Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem. (Josang, Audin et al, 2007)

2.3.7 Eliminating phishing mail

Specialized spam filters can reduce the number of phishing e-mails that reach their addressees' inboxes. These approaches rely on machine learning and natural language processing approaches to classify phishing e-mails. (Tan, Koon, 1905)

2.3.8 Monitoring and takedown

Several companies offer banks and other organizations likely to suffer from phishing scams round-the-clock services to monitor, analyze and assist in shutting down phishing websites. Individuals can contribute by reporting phishing to both volunteer and industry groups, such as PhishTank. Individuals can also contribute by reporting phone phishing attempts to Phone Phishing, Federal Trade Commission. (Tan, Koon, 1905)

2.3.9 INFORMATION SECURITY.

E-banking introduces information security risk management challenges. Financial institution directors and senior management should ensure the information security program addresses these challenges and takes the appropriate actions.

- ✓ Ensure the institution has the appropriate security expertise for its e-banking platform.
- ✓ Implement security controls sufficient to manage the unique security risks confronting the institution. Control considerations include

- Ongoing awareness of attack sources, scenarios, and techniques; compromise. Financial institutions should ensure these computers meet security
 - Up-to-date equipment inventories and network maps;
 - Rapid identification and mitigation of vulnerabilities;
 - Network access controls over external connections;
 - Hardened systems with unnecessary or vulnerable services or files disabled or removed;
 - Use of intrusion detection tools and intrusion response procedures;
 - Physical security of all e-banking computer equipment and media; and
 - Baseline security settings and usage policies for employees accessing the e-banking system or communicating with customers.
- ✓ Use verification procedures sufficient to adequately identify the individual asking to conduct business with the institution.
 - ✓ Use authentication methods sufficient to verify individuals are authorized to use the institution's systems based on the sensitivity of the data or connected systems.
 - ✓ Develop policies for notifying customers in the event of a security breach effecting their confidential information.
 - ✓ Monitor and independently test the effectiveness of the institution's security program.

Information security is essential to a financial institution's ability to deliver e-banking services, protect the confidentiality and integrity of customer information, and ensure that accountability exists for changes to the information and the processing and communications systems. (Leyden, John, 2006)

The guidelines require financial institutions to;

- ⊥ Ensure the security and confidentiality of customer information;
- ⊥ Protect against any anticipated threats or hazards to the security or integrity of such information; and
- ⊥ Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The guidelines outline specific measures institutions should consider in implementing a security program. These measures include

- ⊥ Identifying and assessing the risks that may threaten consumer information;
- ⊥ Developing a written plan containing policies and procedures to manage and control these risks;
- ⊥ Implementing and testing the plan; and
- ⊥ Adjusting the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security

Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Effective information security comes only from establishing layers of various control, monitoring, and testing methods. While the details of any control and the effectiveness of risk mitigation depend on many factors, in general, each financial institution with external connectivity should ensure the following controls exist internally or at their TSP. (Tan, Koon, 1905)

- ❖ Ongoing knowledge of attack sources, scenarios, and techniques. Financial institutions should maintain an ongoing awareness of attack threats through membership in information-sharing entities such as the Financial Services - Information Sharing and Analysis Center (FS-ISAC), Infragard, the CERT Coordination Center, private mailing lists, and other security information sources. All defensive measures are based on knowledge of the attacker's capabilities and goals, as well as the probability of attack. Up-to-date equipment inventories and network maps. Financial institutions should have inventories of machines and software sufficient to support timely security updating and audits of authorized equipment and software. In addition, institutions should understand and document the connectivity between various network components including remote users, internal databases, and gateway servers to third parties. Inventories of hardware and the software on each system can accelerate the institution's response to newly discovered vulnerabilities and support the proactive identification of unauthorized devices or software. (Tan, Koon, 1905)

- ❖ Rapid response capability to react to newly discovered vulnerabilities. Financial institutions should have a reliable process to become aware of new vulnerabilities and to react as necessary to mitigate the risks posed by newly discovered vulnerabilities. Software is seldom flawless. Some of those flaws may represent security vulnerabilities, and the financial institution may need to correct the software code using temporary fixes, sometimes called a “patch.” In some cases, management may mitigate the risk by reconfiguring other computing devices. Frequently, the financial institution must respond rapidly, because a widely known vulnerability is subject to an increasing number of attacks. Network access controls over external connections. Financial institutions should carefully control external access through all channels including remote dial-up, virtual private network connections, gateway servers, or wireless access points. Typically, firewalls are used to enforce an institution’s policy over traffic entering the institution’s network. Firewalls are also used to create a logical buffer, called a “demilitarized zone,” or DMZ, where servers are placed that receive external traffic. The DMZ is situated between the outside and the internal network and prevents direct access between the two. Financial institutions should use firewalls to enforce policies regarding acceptable traffic and to screen the internal network from directly receiving external traffic. (Tan, Koon, 1905)
- ❖ System hardening. Financial institutions should “harden” their systems prior to placing them in a production environment. Computer equipment and software are frequently shipped from the manufacturer with default configurations and passwords that are not sufficiently secure for a financial institution environment. System “hardening” is the process of removing or disabling unnecessary or insecure services and files. A number of organizations have current efforts under way to develop security benchmarks for various vendor systems. Financial institutions should assess their systems against these standards when available. Controls to prevent malicious code. Financial institutions should reduce the risks posed by malicious code by, among other things, educating employees in safe computing practices, installing anti-virus software on servers and desktops, maintaining up-to-date virus definition files, and configuring their systems to protect against the automatic execution of

malicious code. Malicious code can deny or degrade the availability of computing services; steal, alter, or insert information; and destroy any potential evidence for criminal prosecution. Various types of malicious code exist including viruses, worms, and scripts using active content. (Tan, Koon, 1905)

Rapid intrusion detection and response procedures. Financial institutions should have mechanisms in place to reduce the risk of undetected system intrusions. Computing systems are never perfectly secure. When a security failure occurs and an attacker is “in” the institution’s system, only rapid detection and reaction can minimize any damage that might occur. Techniques used to identify intrusions include intrusion detection systems (IDS) for the network and individual servers (i.e., host computer), automated log correlation and analysis, and the identification and analysis of operational anomalies. Physical security of computing devices. Financial institutions should mitigate the risk posed by unauthorized physical access to computer equipment through such techniques as placing servers and network devices in areas that are available only to specifically authorized personnel and restricting administrative access to machines in those limited access areas. An attacker’s physical access to computers and network devices can compromise all other security controls. Computers used by vendors and employees for remote access to the institution’s systems is also subject to and configuration requirements regardless of the controls governing remote access.

- ❖ User enrollment, change, and termination procedures. Financial institutions should have a strong policy and well-administered procedures to positively
- ❖ identify authorized users when given initial system access (enrollment) and, thereafter, to limit the extent of their access to that required for business purposes, to promptly increase or decrease the degree of access to mirror changing job responsibilities, and to terminate access in a timely manner when access is no longer needed. Authorized use policy. Each financial institution should have a policy that addresses the systems various users can access, the activities they are authorized to perform, prohibitions against malicious activities and unsafe computing practices, and consequences for

noncompliance. All internal system users and contractors should be trained in, and acknowledge that they will abide by, rules that govern their use of the institution's system. (Tan, Koon, 1905)

- ❖ Training. Financial institutions should have processes to identify, monitor, and address training needs. Each financial institution should train their personnel in the technologies they use and the institution's rules governing the use of that technology. Technical training is particularly important for those who oversee the key technology controls such as firewalls, intrusion detection, and device configuration. Security awareness training is important for all users, including the institution's e- banking customers. (Tan, Koon, 1905)
- ❖ Independent testing. Financial institutions should have a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective action where deficiencies are identified; and provides independent assurance for compliance with security policies. Security tests are necessary to identify control deficiencies. An effective testing plan identifies the key controls, then tests those controls at a frequency based on the risk that the control is not functioning. Security testing should include independent tests conducted by personnel without direct responsibility for security administration. Adverse test results indicate a control is not functioning and cannot be relied upon. Follow-up can include correction of the specific control, as well as a search for, and correction of, a root cause. Types of tests include audits, security assessments, vulnerability scans, and penetration tests. (Tan, Koon, 1905)

2.3.10 AUTHENTICATING E-BANKING CUSTOMERS

E-banking introduces the customer as a direct user of the institution's technology. Customers have to log on and use the institution's systems. Accordingly, the financial institution must control their access and educate them in their security responsibilities. While authentication controls play a significant role in the internal security of an organization. This section of our study will discusses authentication only as it relates to the e-banking customer (Grant Thornton, 2009)

2.3.10.1 Authenticating New Customers

Verifying a customer's identity, especially that of a new customer, is an integral part of all financial services. Consistent with the USA PATRIOT Act, federal regulations require that by October 1, 2003, each financial institution must develop and implement a customer identification program (CIP) that is appropriate given the institution's size, location and type of business. The CIP must be written, incorporated into the institution's Bank Secrecy Act/Anti-Money Laundering program, and approved by the institution's board of directors. The CIP must include risk-based procedures to verify the identity of customers (generally persons opening new accounts). Procedures in the program should describe how the bank will verify the identity of the customer using documents, nondocumentary methods, or a combination of both. The procedures will reflect the institution's account opening processes – whether face-to-face or remotely as part of the institution's e-banking services. As part of its nondocumentary verification methods, a financial institution may rely on third parties to verify the identity of an applicant or assist in the verification. The financial institution is responsible for ensuring that the third party uses the appropriate level of verification procedures to confirm the customer's identity. New account applications submitted on-line increase the difficulty of verifying the application information. Many institutions choose to require the customer to come into an office or branch to complete the account opening process. Institutions conducting the entire account opening process through the mail or on-line should consider using third-party databases to provide (Grant Thornton, 2009)

- ❖ **Positive verification** to ensure that material information provided by an applicant matches information available from third-party sources,
- ❖ **Logical verification** to ensure that information provided is logically consistent.
- ❖ **Negative verification** to ensure that information provided has not previously been associated with fraudulent activity (e.g., an address previously associated with a fraudulent application).

2.3.10.2 Authenticating Existing Customers

A financial institution should also authenticate its customers' identities each time they attempt to access their confidential on-line information. The authentication method a

financial institution chooses to use in a specific e-banking application should be appropriate and “commercially reasonable” in light of the risks in that application. Whether a method is a commercially reasonable system depends on an evaluation of the circumstances. Financial institutions should weigh the cost of the authentication method, including technology and procedures, against the level of protection it affords and the value or sensitivity of the transaction or data to both the institution and the customer. (Grant Thornton, 2009)

Authentication methods involve confirming one or more of three factors:

- ❖ Something only the user should know, such as a password or PIN;
- ❖ Something the user possesses, such as an ATM card, smart card, or token; or
- ❖ Something the user is, such as a biometric characteristic like a fingerprint or iris pattern. (Virus Bulletin, 2005)

Authentication methods that depend on more than one factor are typically more difficult to compromise than single-factor systems therefore suggesting a higher reliability of authentication. For example, the use of a customer ID and password is considered single-factor authentication since both items are something the user knows. A common example of two-factor authentication is found in most ATM transactions where the customer is required to provide something the user possesses (i.e., the card) and something the user knows (i.e., the PIN). Single factor authentication alone may not be adequate for sensitive communications, high dollar value transactions, or privileged user access (i.e., network administrators). Multi-factor techniques may be necessary in those cases. Institutions should recognize that a single factor system may be “tiered” (e.g., require multiple passwords) to enhance security without the implementation of a true two-factor system. (Virus Bulletin, 2005)

2.3.10.3 Password Administration

Despite the concerns regarding single-factor authentication, many e-banking services still rely on a customer ID and password to authenticate an existing customer. Some security professionals criticize passwords for a number of reasons including the need for passwords whose strength places the password beyond the user’s ability to comply with other password policies such as not writing the password down. Password-

cracking software and log-on scripts can frequently guess passwords regardless of the use of encryption. Popular acceptance of this form of authentication rests on its ease of use and its adaptability within existing infrastructures. Financial institutions that allow customers to use passwords with short character length, readily identifiable words or dates, or widely used customer information (e.g., Social Security numbers) may be exposed to excessive risks in light of the security threats from hackers and fraudulent insider abuse. Stronger security in password structure and implementation can help mitigate these risks. Another way to mitigate the risk of scripted attacks is to make the user ID more random and not based on any easily determined format or commonly available information. There are three aspects of passwords that contribute to the security they provide: **password secrecy, password length and composition, and administrative controls.** (Grant Thornton, 2009)

Password secrecy; The security provided by password-only systems depends on the secrecy of the password. If another party obtains the password, he or she can perform the same transactions as the intended user and therefore, passwords and password files should be encrypted when stored or transmitted over open networks such as the Internet. The system should prohibit any user, including the system or security administrator, from printing or viewing unencrypted passwords. In addition, security administrators should ensure password files are protected and closely monitored for compromise because if stolen an attacker may be able to decrypt an encrypted password file.

Financial institutions need to emphasize to customers the importance of protecting the password's confidentiality. Customers should be encouraged to log off unattended computers that have been used to access on-line banking systems especially if they used public access terminals such as in a library, institution lobby, or Internet cafe. (Grant Thornton, 2009)

Password length and composition; The appropriate password length and composition depends on the value or sensitivity of the data protected by the password and the ability of the user to maintain the password as a shared secret. Common identification items, for example, dictionary words, proper names, or social security numbers should not be used as passwords. Password composition standards that

require numbers or symbols in the sequence of a password, in conjunction with both upper and lower case alphabetic characters, provide a stronger defense against password-cracking programs. Selecting letters that do not create a common word but do create a mnemonic. For example the first letter of each word in a favorite phrase, poem, or song can create a memorable password that is difficult to crack.

Systems linked to open networks, like the Internet, are subject to a greater number of individuals who may attempt to compromise the system. Attackers may use automated programs to systematically generate millions of alphanumeric combinations to learn a customer's password (i.e., "brute force" attack). A financial institution can reduce the risk of password compromise by communicating and enforcing prudent password selection, providing guidance to customers and employees, and careful protection of the password file. (Grant Thornton, 2009)

Password administration controls; When evaluating password-based e-banking systems, management should consider whether the authentication system's control capabilities are consistent with the financial institution's security policy. This includes evaluating such areas as password length and composition requirements, incorrect log-on lockout, password expiration, repeat password usage, and encryption requirements, as well as the types of activity monitoring and exception reports in use. Each financial institution must evaluate the risks associated with its authentication methods given the nature of the transactions and information accessed. Financial institutions that assess the risk and decide to rely on passwords, should implement strong password administration standards. (Grant Thornton, 2009)

Therefore, this project will be carried out to address the security risks, security risks responses and security risks management thereby minimizing the potentially serious financial legal and reputational implications in electronic banking

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter discussed the methods and techniques of data collection and analysis which were presented and described.

3.1 Research design

The researchers used both qualitative and quantitative methods of data collection analysis.

3.2 Area of study

The study was conducted at Equity bank Kenya Kikuyu branch. The respondents were got from employees of different departments within the organization

3.3 Study Population

The population of interest will include members of Equity bank Kenya kikuyu branch. The researchers will choose members from the department of information technology, finance department and marketing and public relations department.

3.4 Sample Size

The researchers choose a big sample size which enabled them to acquire information which was accurate. The researchers choose twenty members from the department of information technology, twenty members from the department of finance department and twenty members from the department of marketing and public relations.

3.5 Data collection techniques

Weller and Romney (1988). States that, the purpose of data collection was to obtain information to keep on record, to make decisions about important issues, to pass information on to others. Primarily, data was collected to provide information regarding a specific topic.

Data collection Plan often contains the following activity.

1. Pre collection activity – Agree goals, target data, definitions, methods
2. Collection – data collection
3. Present Findings – usually involves some form of sorting analysis and/or presentation.

(Weimer, 1995). A formal data collection process was necessary as to ensure that data gathered was both defined and accurate and that subsequent decisions based on arguments embodied in the findings were valid. Types of data collection included: documented literature.

3.6 Questionnaires

These are pre-formulated written set of questions to which the respondents recorded their answers. Further more questionnaires can be administered personally or mailed to respondents. The questionnaires were prepared because they save the time especially when the group is big and they are geographically scattered, they can be stored for future reference, will give straight answers as well as easy to evaluate.

3.7 Interviews

It was an oral questionnaire where the investigator gathered data through direct verbal interaction with participants. The researchers carried face to face interviews with the respondents. However, the researcher also explained to the respondents why the study was to be carried out. As a research technique the interviews was a conversation carried out with definite purpose of obtaining certain information.

Interviews were preferred because they created a right type of friendly atmosphere, which was very conducive for obtaining desired data as well as giving assurance and guarantee to the interviewee that the fact was promptly used and safe guarded.

3.8 Document analysis

Documentation was a method of collecting data from other sources such as records, books and publications. The method used to collect data was document analysis. This design involved collecting classes of data and conducting studies to determine principles that might guide future actions.

3.8.1 Advantage of this method

1. This method of data collection was cheap.
2. The source of information with this method was usually reliable.

3.8.2 Disadvantage of this method

1. It was difficult to get detailed information from this method of data collection.

3.9 Research procedure

The researcher obtained an introductory letter from Kampala International University, School of Computer Studies to allow him carry out the research in the organization. Permission was sort from the university authority to allow the researcher conduct the study. Participants willing to provide information were guided with questionnaires filling process and questions were asked by the researchers for clarification.

3.10 Data analysis and presentation

After data collection, only suitable data analysis technique such as questionnaires was coded and analyzed. Analysis was carried out by the use of frequencies by the help of SPSS and Ms Excel.

3.11 Research limitations

The study faced the following problems;

- ❖ Most of the employees in the bank were busy thus too limited time was posed on the researchers.
- ❖ Some of the employees were not be willing to give the correct information to the researchers.
- ❖ The researchers were limited by time. Some respondents were reluctant to fill in the questionnaires and submit the questionnaires which delayed data analysis process and the final report.
- ❖ Confidentiality. The nature of some information was so sensitive that the employees were not willing to reveal to the researchers which in turn limited the amount of data collection.

3.12 Research Design

The type of study in this case was a secondary research (also known as desk research). It involved the summary, collation and/or synthesis of existing research rather than primary research, where data was collected from, for example, research subjects or experiments. The data was collected from journal, articles, internet sources, books, annual ICT workshops and corporate reports.

3.13 Research tools

Ms Excel and SPSS enabled the researchers to graphically summarize data using bar, pie, range of value, graduated symbol, and dot density charts displayed on high-quality maps

Ms Excel and SPSS also helped the researchers to generate various types of statistical process control charts.

This project was undertaken to address on the security risks, responses and the risk management thereby minimizing the potentially serious financial, legal and reputational implications.

CHAPTER FOUR

FINDINGS, ANALYSIS AND PRESENTATION OF DATA

4.0 Introduction

The chapter was about presentation and analysis of the data related to the security issues in electronic banking. The study specifically focused on the security risks, security responses and security risks management in electronic banking.

During data analysis and presentation of findings, tables and figures were used while frequencies and percentages were used to describe the findings. Data was also analyzed and presented by the help of bar graphs and pie charts.

4.1 Data Analysis.

4.1.1 Respondents by sex.

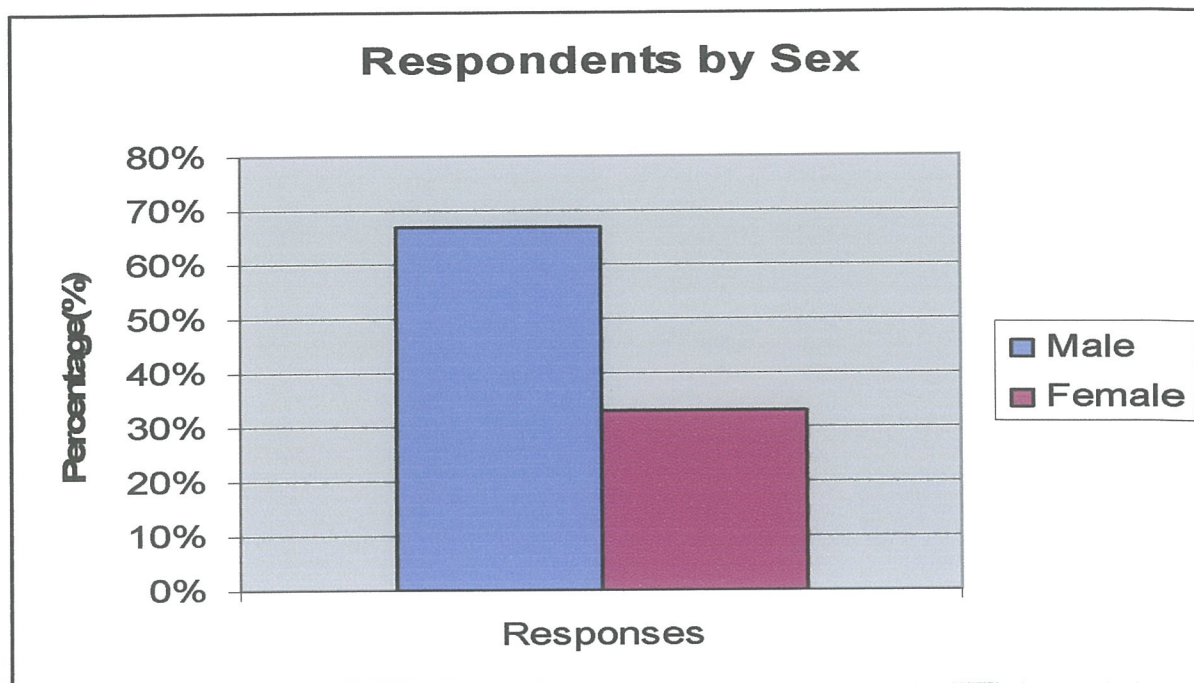
Table 4.1(a) Respondents by sex categories

SEX	FREQUENCY	PERCENTAGES
Male	40	67%
Female	20	33%
Total	60	100%

Source: primary data

Findings showed that majority of the respondents 40(or 67%) were males whereas 20(or 33%) of the respondents were females. This revealed that majority of the respondents were male (67%) while the rest (33%) of the employees were female.

Figure 4.1(a): graphical representation of respondents by sex.



4.1.2 Respondents by age groups

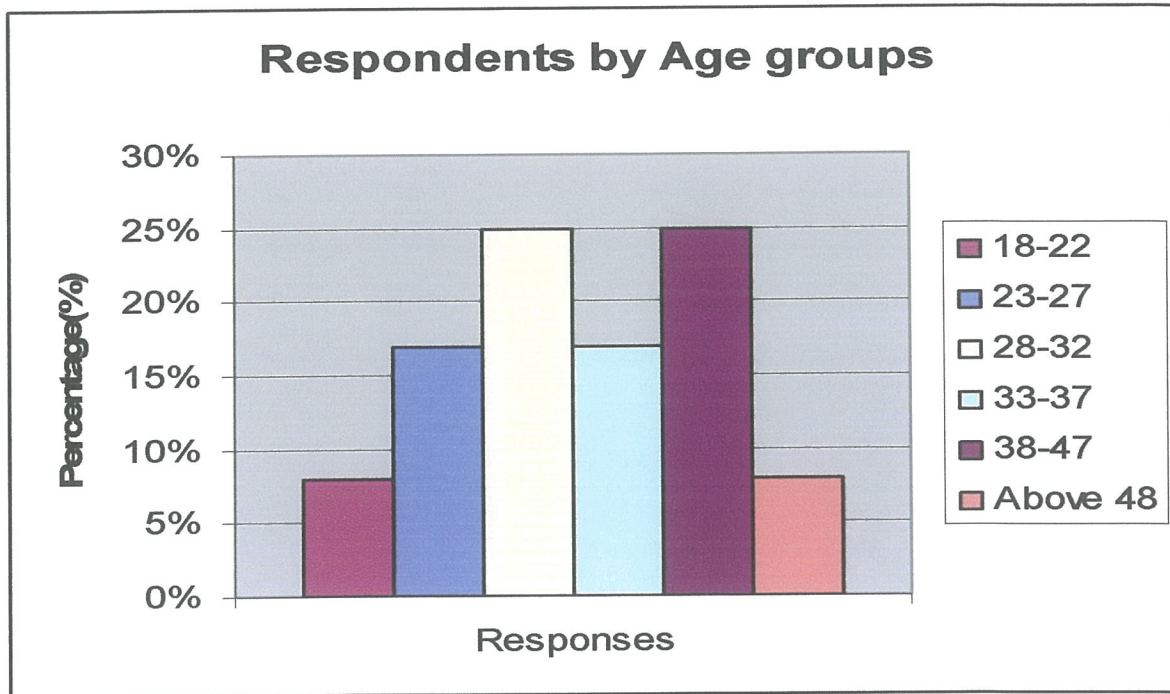
Table 4.1(b) Respondents by age groups

Age group	Frequency	Percentage
18-22	5	8%
23-27	10	17%
28-32	15	25%
33-37	10	17%
38-47	15	25%
Above 48	5	8%
Total	60	100%

Source: primary data

Findings revealed that most of the respondents (25%) were aged between 28-32 years old and also between 38-47 years old while (17%) were aged between 23-27 years old and also 33-37 years old, (8%) of the respondents were aged between 18-22 years old and also (8%) of the respondents were aged above 48 years old.

Figure 4.1(b) graphical representation of respondents by age groups



From the analysis above, it can be deduced that majority of the respondents (25%) are aged between 28-32 years old and also (25%) are aged between 28-32 years old, (17%) aged between 23-27 years old and also between 33-37 years old, (8%) aged above 48 years old and also (8%) aged between 18-22 years old.

4.1.3 Respondents by Education level

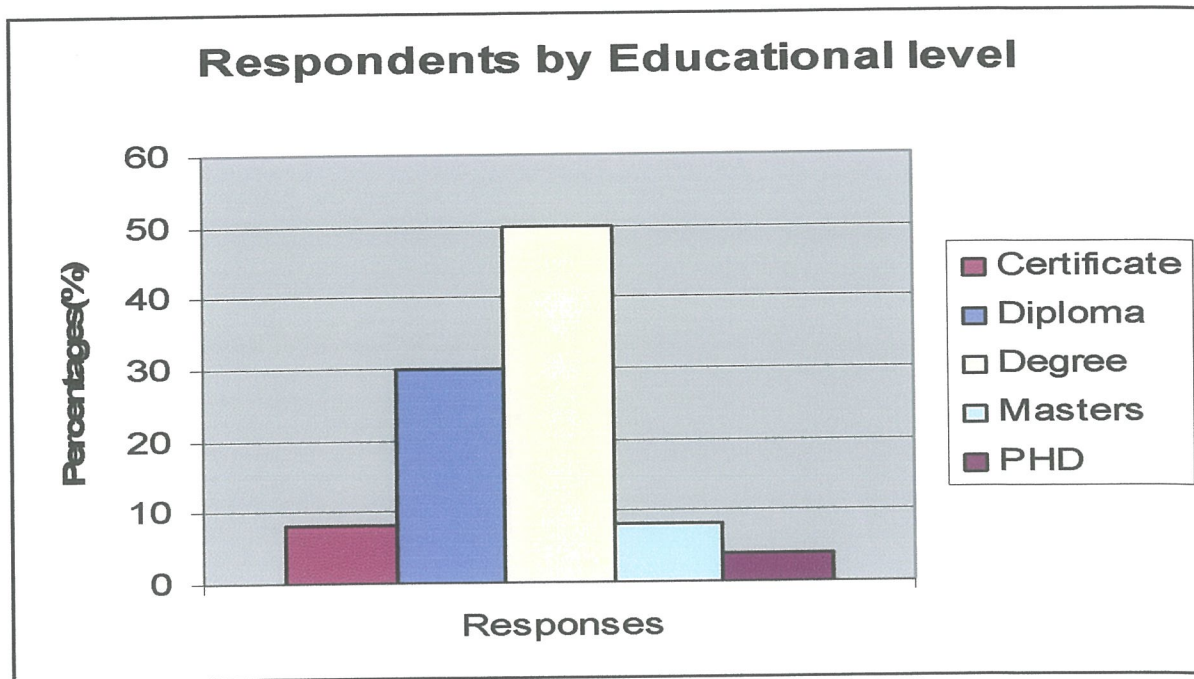
Table 4.1(c). Respondents by Education level

Education Level	Frequency	Percentage
Certificate	5	8
Diploma	18	30
Degree	30	50
Masters	5	8
PHD	2	4
TOTAL	60	100

Source: primary source

Findings from table 3 showed that majority of the respondents (50%) were degree holders, (30%) were diploma holders, (8%) were certificate holders, (8%) were master's holders while the remaining (4%) were PhD holders.

Figure 4.1(c) graphical representation of respondents by level of education



From figure 3 above, it can be seen that majority (50%) of the respondents had degree while (30%) had diploma certificates, (8%) had done certificate courses, (8%) had done masters, and (4%) had done masters.

4.1.4 Classification of respondents by designation

Table 4.1(d) Classification of respondents by designation

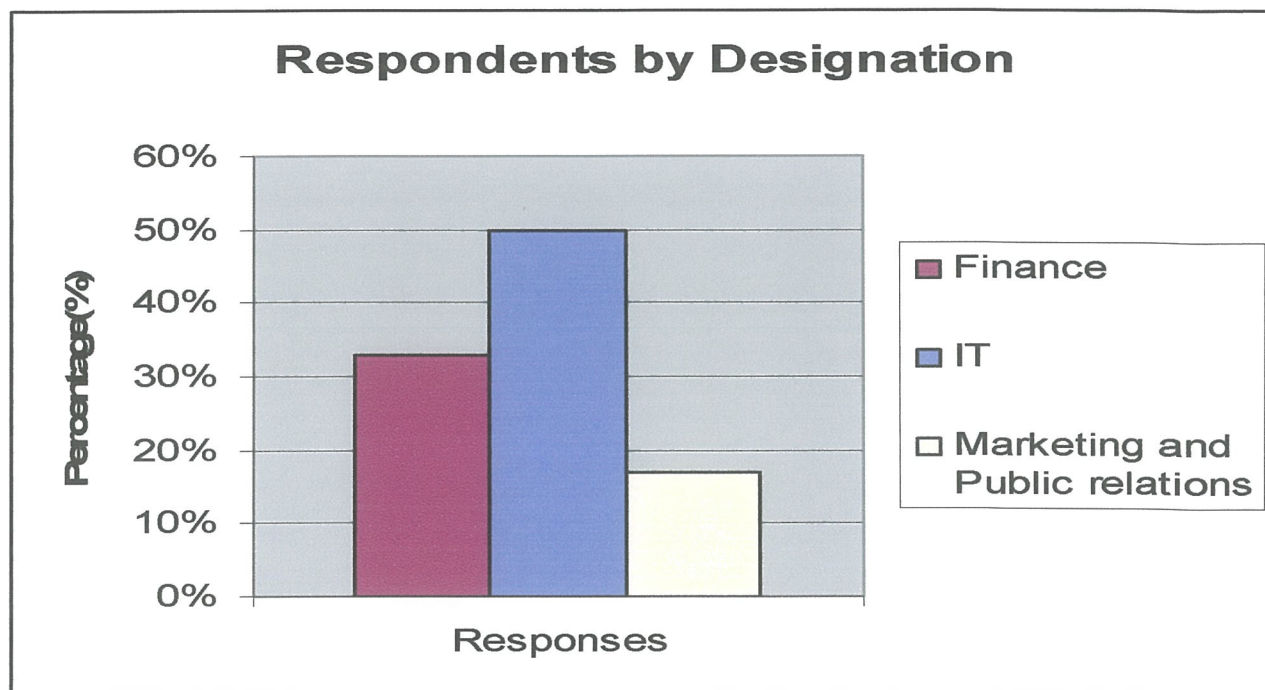
DESIGNATION	FREQUENCY	PERCENTAGE
Finance	20	33%
IT	30	50%
Marketing and Public relations	10	17%
TOTAL	60	100%

Source: primary data

The results in table 4 show that majority of the respondents (50%) came from the Information Technology department, (33%) of the respondents from finance

department, (17%) of the respondents from Marketing and public relations department.

Figure 4.1(d) Graphical presentation of respondents by designation



From the above analysis, it's easily deduced that the highest number of respondents were staffs from the IT department (50%); finance department (33%) and Marketing and public relations department (17%).

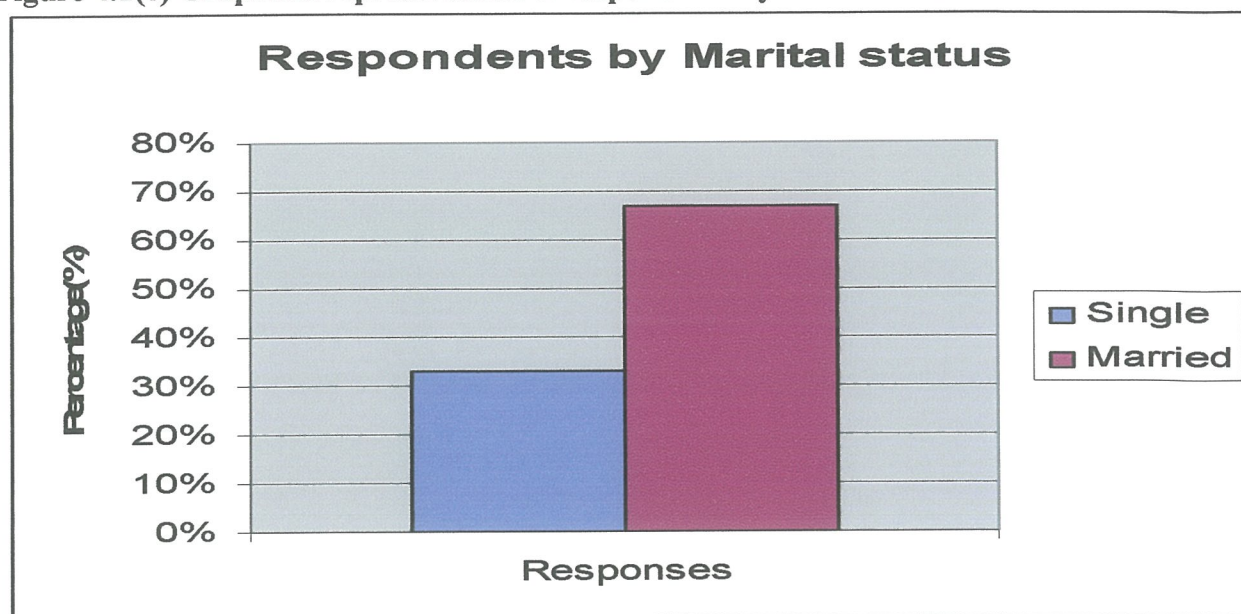
4.1.5 Respondents by marital status.

Table 4.1(e) Respondents by Marital status

MARITAL STATUS	FREQUENCY	PERCENTAGES
Single	20	33%
Married	40	67%
Total	60	100%

Source: primary data

Figure 4.1(e) Graphical representation of respondents by marital status



4.2 Addressing the security risks in electronic banking.

The first objective of the study was to address the security risks in electronic banking in Equity bank Kikuyu branch (Kenya).

The findings were based on the research questions from the specific objective of the study “Will addressing the security risks minimize the potentially serious financial, legal and reputational implications in e-banking?” To achieve this objective, the respondents were asked to tell the number of years they had used e-banking in their institution.

Table 4.2 (a). Results on how many years respondents had used e-banking

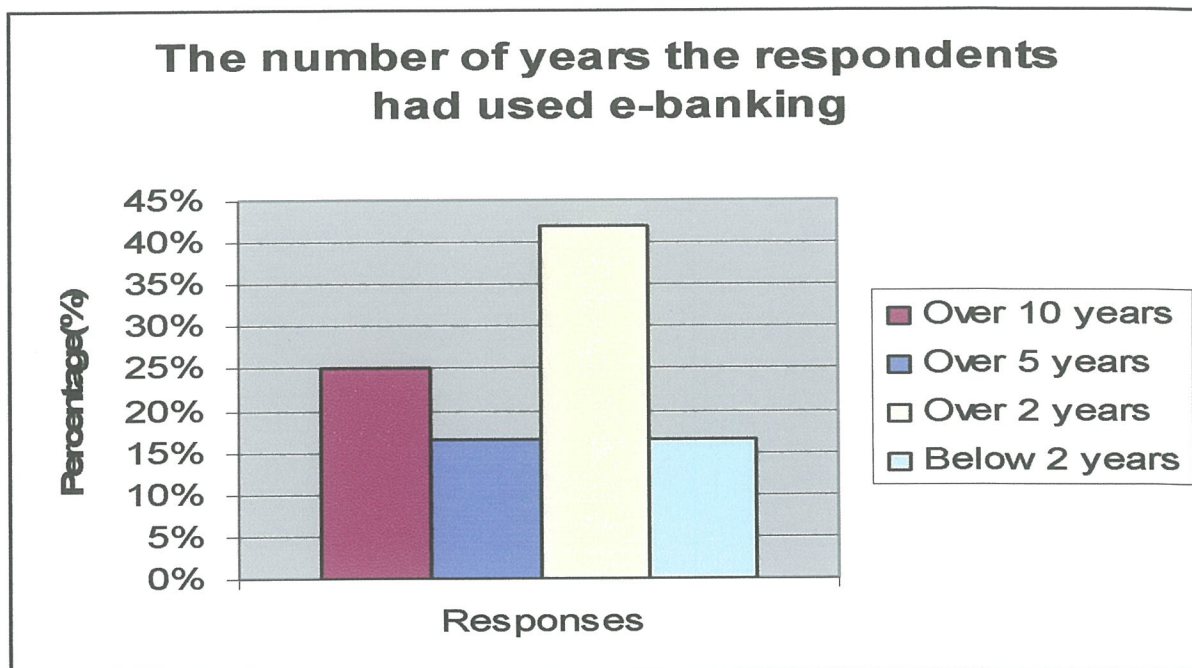
Number of years the respondents had used e-banking	Over 10 years	Over 5 years	Over 2 years	Below 2 years	Total
Frequency (f_o)	15	10	25	10	60
Percentage (%)	25%	16.5%	42%	16.5%	100%

Source: Questionnaire Output

The results in the table 4.2 (a) above revealed that 15 respondents which constituted (25%) had used electronic banking for over 10 years, 10 respondents constituting 16.5% had used e-banking for over 5 years but for less than 10 years, 25 respondents constituting 42% had used e-banking for over 2 years but for less than 5 years while 10 respondents constituting 16.5% had used e-banking for less than 2 years.

The data in the above table 4.2 (a) was analyzed using a bar graph and figure 4.2 (a) summarizes the analysis of the number of years the respondents had used electronic banking in their institution.

Figure 4.2 (a). The number of years the respondents had used e-banking



The respondents were further asked to put forward the modes of banking they thought it was more secure for them. The responses are tabulated in the table below.

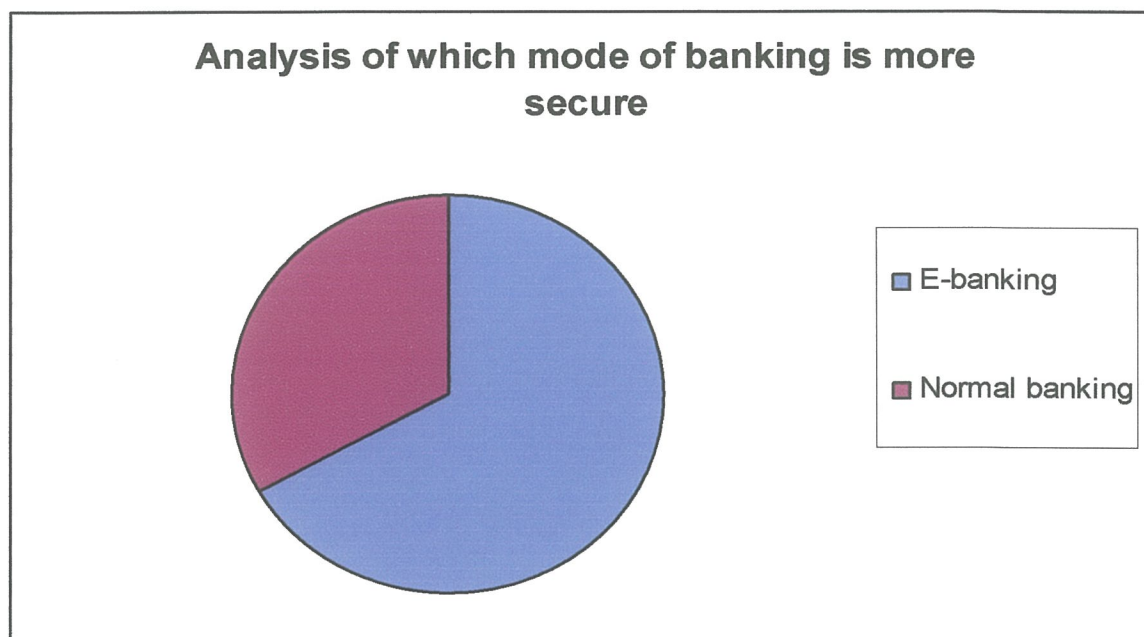
Table 4.2 (b). Results on which mode of banking is more secure.

Which Mode of banking is more secure?	E-banking	Normal banking	total
Frequency (f)	40	20	60
Percentage (%)	67%	33%	100%

Source: Questionnaire Output

The results in the table 4.2 (b) above revealed that 40 employees constituting (67%) of the sample size choose electronic banking (e-banking) as being more secure mode of banking than the normal banking which 20 respondents constituting 33% choose normal banking as being the most secure mode of banking. the table 4.2(b) above summarizes that majority of the respondents chose e-banking as being more secure than the normal banking.

Figure 4.2 (b) Diagrammatic (Pie-chart) presentations showing the mode of banking which is more secure.



The respondents were also asked to put forward whether they experienced unauthorized access (Hacking) or not. The responses are tabulated in the table below.

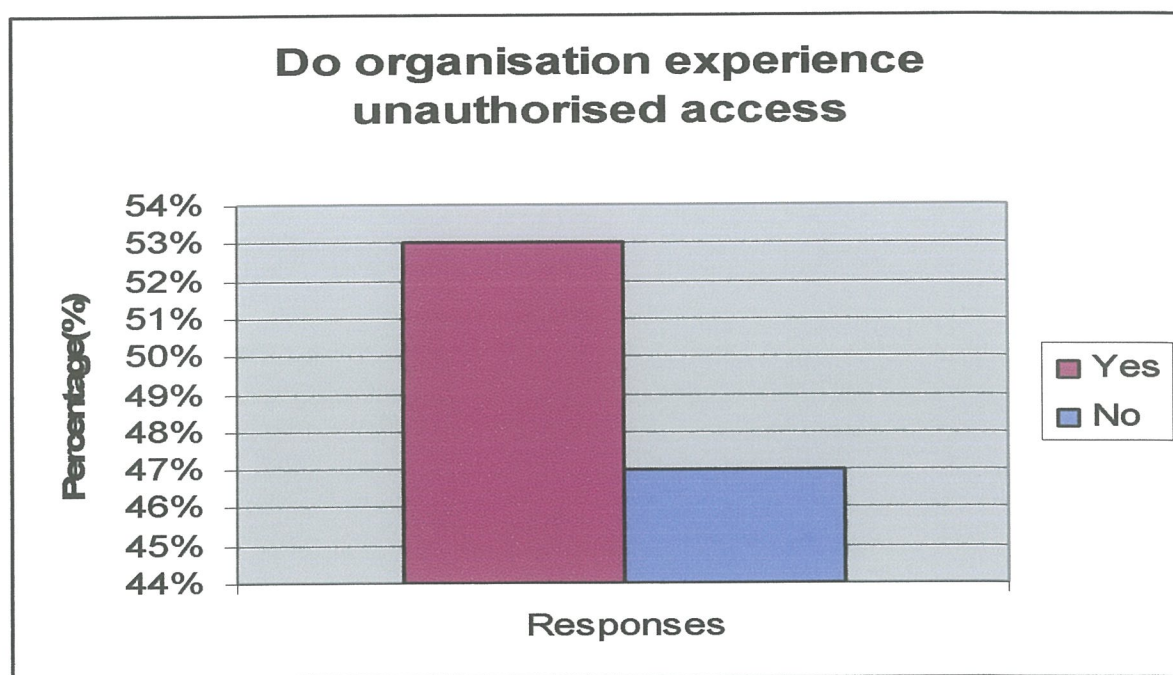
Table 4.2 (c). Results on whether the respondents experienced unauthorized access (Hacking)

Did you experience unauthorised access(Hacking)	Yes	No	Total
Frequency (f)	32	28	60
Percentage (%)	53%	47%	100

Source: questionnaire output

The results in the table 4.2 (b) above revealed that out of the total sample size of 60 respondents, 32 of the respondents constituting 53% experienced unauthorized access which is also known as Hacking while the rest of the respondents (28) constituting 47% did not experience unauthorized access(Hacking)

Figure 4.2 (c) Diagrammatic (Bar-chart) presentations showing the respondents who experienced unauthorized access (Hacking) and who did not.



The respondents were also asked to state whether they experienced attacks on their local networks or not. The results are tabulated in the table below

Table 4.2 (d).results on whether the organization experienced attacks on their local networks or not.

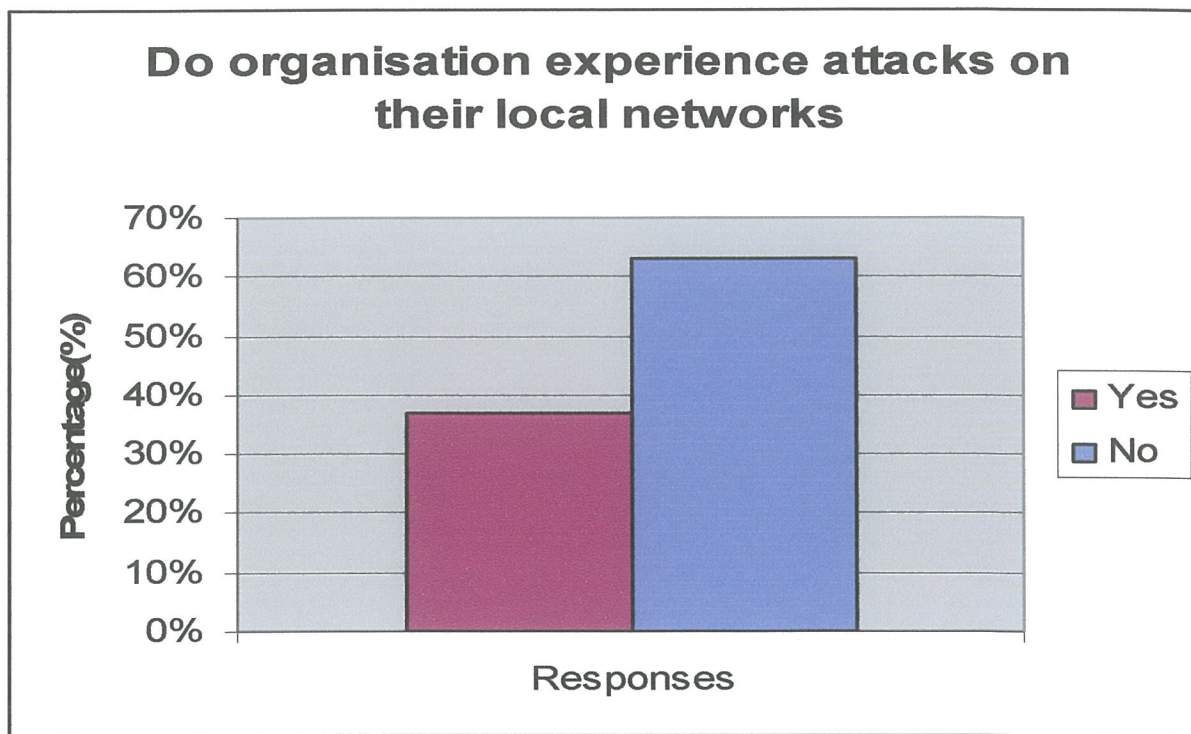
Did you experience Attacks on your local networks	Yes	No	Total
Frequency (f)	22	38	60
Percentage (%)	37%	63%	100%

Source: questionnaire output

The results in the table 4.2 (d) above revealed that out of the total sample size of 60 respondents, only 22 respondents constituting (37%) in the organization experienced attacks in their local network while 38 respondents constituting (63%) of the sample size did not experience attacks on the local network.

The table 4.2(d) above summarizes that the organization did not experience or suffer more on the local network attacks.

Figure 4.2 (d) Diagrammatic (Bar-chart) presentations showing the percentages of the respondents who experienced attacks on their local networks and who did not.



The respondents were also asked to state whether they experienced spywares as a threat in their organisation. The results are tabulated in the table below.

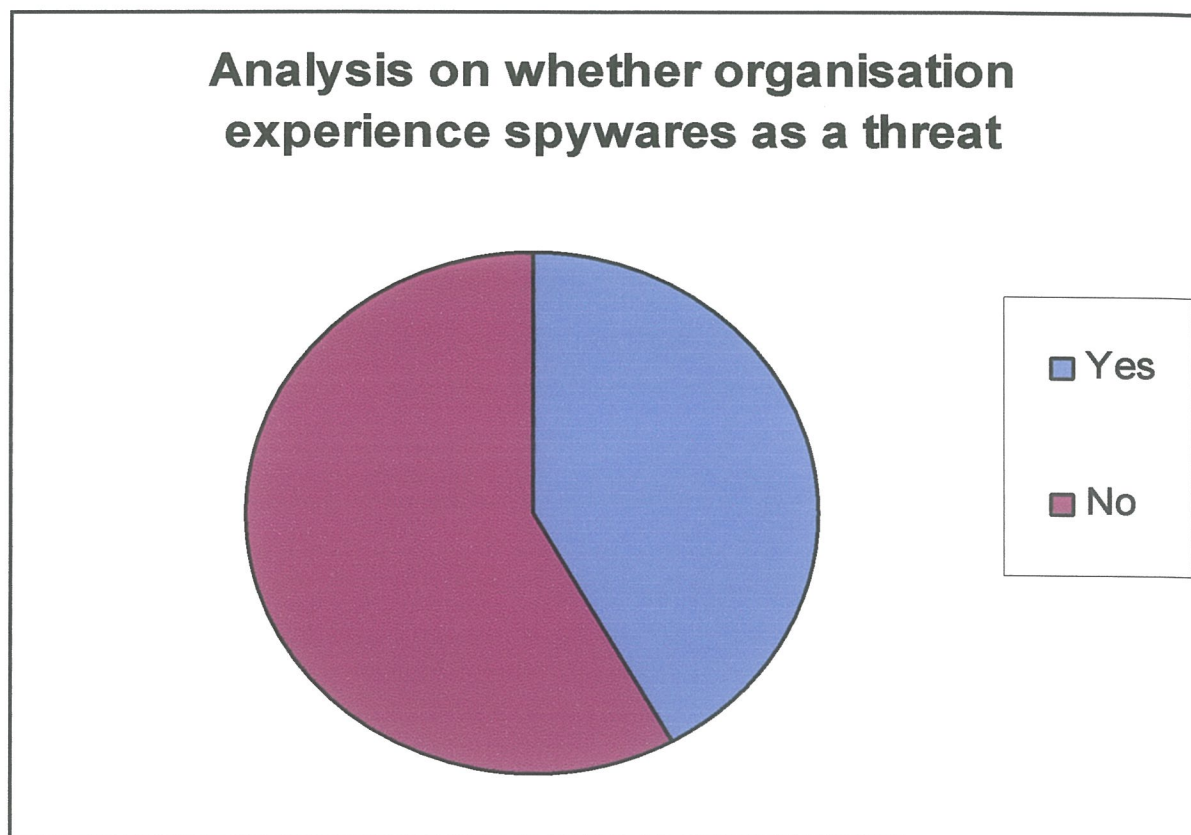
Table 4.2 (e). Results on whether the organization experienced spywares as a threat in their organization.

Did you experience spywares as a threat in the organisation	Yes	No	Total
Frequency (f)	25	35	60
Percentage (%)	42%	58%	100%

Source: questionnaire output

The results in the table 4.2 (e) above revealed that out of the total sample size of 60 respondents, 25 respondents constituting (42%) experienced spywares as a threat in the organization while 35 respondents constituting (58%) did not experience spywares as a threat in the organisation.

Figure 4.2 (e) Diagrammatic (Pie-chart) presentations showing the percentages of the respondents who experienced spywares as a threat in the organisation and who did not.



The respondents were also asked to state other security issues they experience in the institution while using e-banking. The results of their responses were tabulated in the table 4.2(f) below.

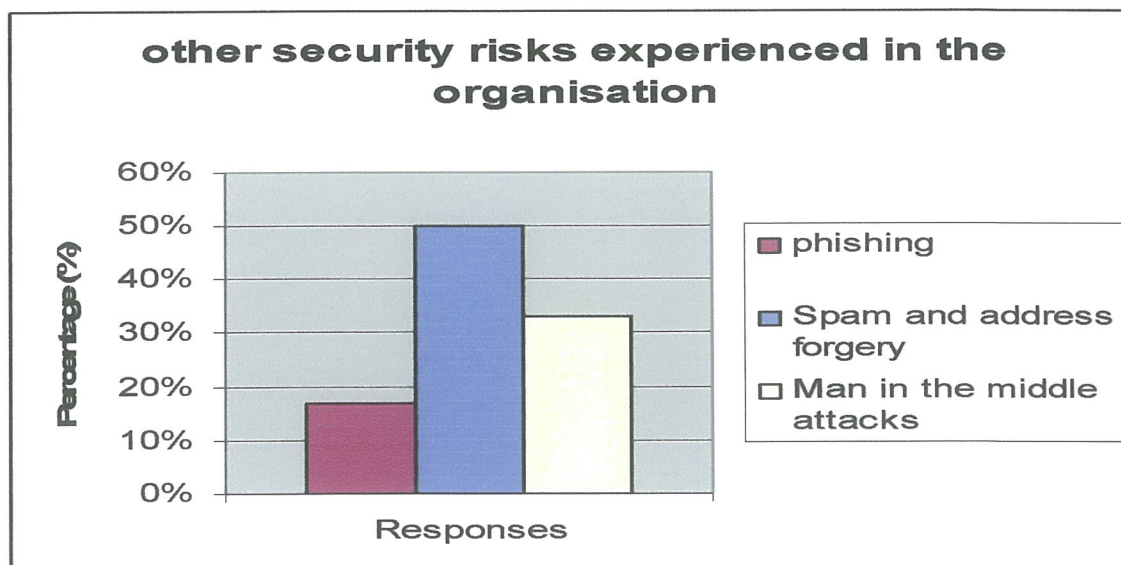
Table 4.2 (f) results on other security risks experienced in the organisation.

Other security risks experienced in the organisation	Frequency (f)	Percentage (%)
phishing	10	17%
Spam and address forgery	30	50%
Man in the middle attacks	20	33%
total	60	100%

Source: questionnaire output

The results tabulated in the table above reveals that there were other security risks experienced in the organisation .10 of the respondents constituting (17%) of the total sample size experienced phishing, 30 of the respondents constituting (50%) experienced spam and address forgery and 20 respondents constituting (33%) experienced man in the middle attacks.

Figure 4.2 (f) Diagrammatic (Bar-chart) presentations showing other security risks experienced in the organisation.



4.3 Addressing the security risks responses in electronic banking

The second objective of this study was to address the security risk responses in e-banking. The findings were based on the research questions from the specific objective of the study two “Will addressing the security risks responses minimize the potentially serious financial, legal and reputational implications in e-banking?” To achieve this objective the respondents were asked to state whether they took any response against the security risks or threats they experienced in their organisation of which the responses to the objectives are given in the table 4.3(a) below.

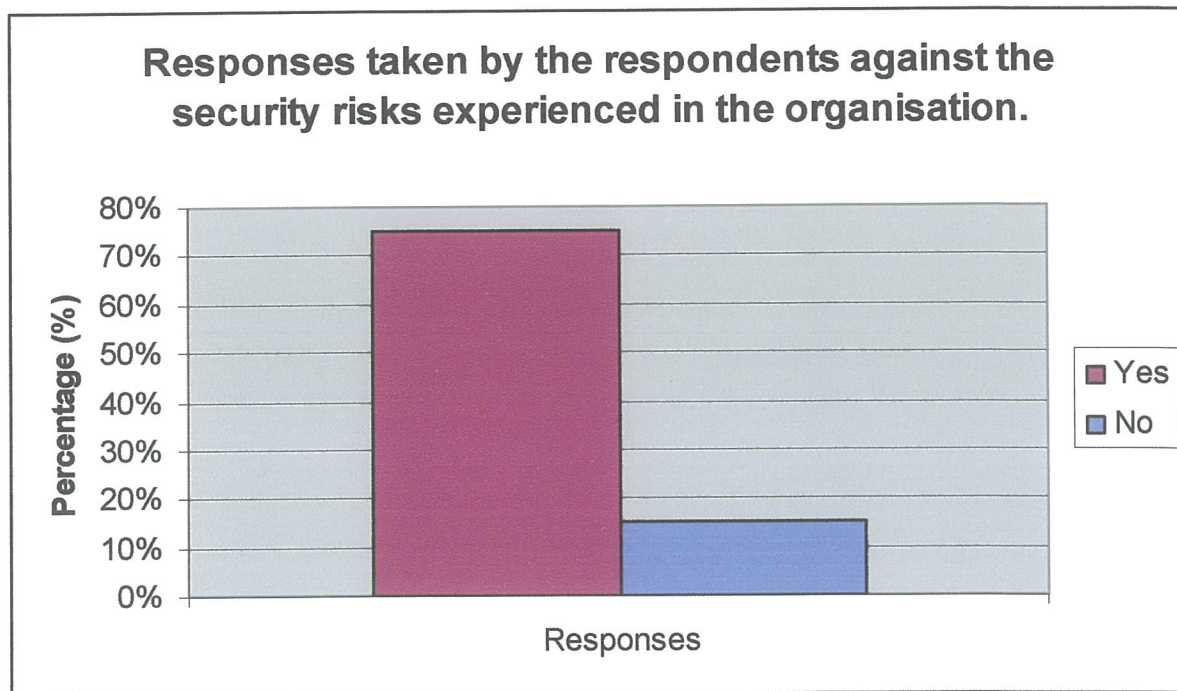
Table 4.3(a) results on whether the respondents took any responses or not against the risks/threats they experienced in the organisation.

Did you take any response against the risks/threats you experienced?	Yes	No	Total
Frequency (f)	45	15	60
Percentage (%)	75%	15%	100%

Source: questionnaire output

The results in the table 4.3(a) above reveals that three quarters of the total sample size (45 respondents) responded against the security risks/threats they experienced while a quarter of the respondents (15) did not respond to the security risks/threats they experienced in the organisation.

Figure 4.3 (a) Diagrammatic (Bar-chart) presentations showing the responses taken by the respondents against the security risks experienced in the organisation.



4.4 addressing the security risks measures or management in electronic banking

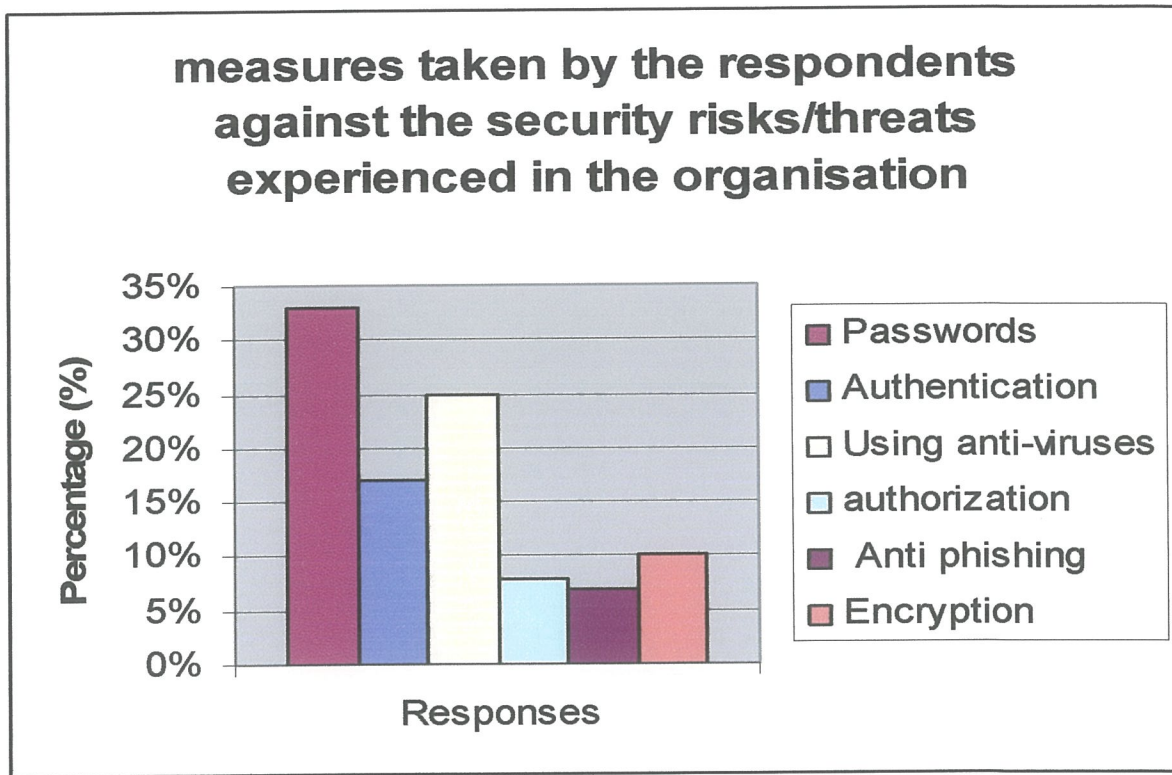
The third objective of this study was to address the security risk management or measures in e-banking. The findings were based on the research questions from the specific objective of the study three “Will addressing the security risks management minimize the potentially serious financial, legal and reputational implications in e-banking?” To achieve this objective the respondents were asked to state the measures they take against the security threats or risks they experience in the organisation of which the responses to the objectives are given in the table 4.4(a) below

Table 4.4(a) results on the measures the respondents took against the security risks/threats they experienced in the organisation.

Responses against risks and threats	Frequency (f)	Percentage (%)
Passwords	20	33%
Authentication	10	17%
Using anti-viruses	15	25%
authorization	5	8%
Anti phishing	4	7%
Encryption	6	10%
total	60	100%

The results tabulated in the table above reveals that the respondents in the organisation used only a small percentage of the security measures against the threats/risks they experienced in the organisation. The table above shows that only 20 respondents used pass words, 10 respondents used authentication, 15 respondents used anti viruses, only 5 used authorization, only 4 used anti phishing, and only 6 used encryption as a measure against the security risks/threats experienced in the organisation. This reveals that majority of the respondents in the organisation used passwords and anti viruses while only a few knew how to use authorization, anti phishing and encryption.

Figure4.4 (a) Diagrammatic (Bar-chart) presentations showing the measures taken by the respondents against the security risks/threats experienced in the organisation.



Therefore, this chapter of findings, analysis and presentation of data was successful through the use of tables and figures in the data analysis and by the help of bar graphs and pie charts in the presentation of findings.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATION

5.0 Introduction

This chapter presents the discussion, conclusion and recommendation with suggestion for future research in line with the study objectives and research question related to the studied topic of the security issues in electronic banking.

5.1 Discussion of the Findings.

The discussions of the findings were presented in accordance with the research objective of the study.

5.1.1 Addressing the security risks in electronic banking.

The first objective of the study was to address the security risks in electronic banking in Equity bank Kikuyu branch (Kenya).

The study revealed that 15 respondents which constituted (25%) of the total sample size had used electronic banking for over 10 years, 10 respondents constituting 16.5% had used e-banking for over 5 years but for less than 10 years, the majority being 25 respondents constituting 42% had used e-banking for over 2 years but for less than 5 years while 10 respondents constituting 16.5% had used e-banking for less than 2 years.

The study also revealed that the majority of the employees (40) constituting (67%) of the total sample size choose electronic banking (e-banking) as being a more secure mode of banking than the normal banking which only 20 respondents constituting 33% choose normal banking as being the most secure mode of banking.

We revealed that out of the total sample size of 60 respondents, 32 of the respondents constituting 53% and being the majority experienced unauthorized access which is also known as Hacking while the rest of the respondents (28) constituting 47% did not experience unauthorized access(Hacking).

After the study, we revealed that only 22 respondents constituting (37%) out of the total sample size of 60 respondents in the organization experienced attacks in their local network while 38 respondents constituting (63%) of the sample size did not experience attacks on the local network clearly indicating that the organization did not experience or suffer more of the local network attacks.

From the study, we also noted that out of the total sample size of 60 respondents, 25 respondents constituting (42%) experienced spywares as a threat in the organization while 35 respondents constituting the majority (58%) did not experience spywares as a threat in the organisation.

Other security risks experienced in the organisation were also discovered by 10 of the respondents constituting (17%) of the total sample size experiencing phishing, 30 of the respondents constituting (50%) experiencing spam and address forgery and 20 respondents constituting (33%) experiencing man in the middle attacks.

5.1.2 Addressing the security risks responses in electronic banking

The second objective of the study was to address the security risk responses in e-banking and the study revealed that three quarters of the total sample size (45 respondents) responded against the security risks/threats they experienced while a quarter of the respondents (15) did not respond to the security risks/threats they experienced in the organisation. The study showed that majority of the respondents (45) responded after experiencing the security threats in the organisation while a few of the respondents were ignorant on the security threats they experienced in the organisation and thus did not take any step against the threat or did not take any response. Further more through the informal interview carried out by the researcher at the organization respondents reported and suggested that the organisation should take instant measures against the employees' responses towards the security threats/risks they experience.

5.1.3 Addressing the security risks measures or management in electronic banking

The third objective of this study was to address the security risk management or measures in electronic banking. The study revealed that the respondents in the organisation used only a small percentage of the security measures against the threats/risks they experienced in the organisation. The study showed that 20 respondents out of the total sample size of (60) used pass words, 10 respondents used authentication, 15 respondents used anti viruses, only 5 used authorization, only 4 used anti phishing, and only 6 used encryption as a measure against the security risks/threats they experienced in the organisation. Basing on this finding it clearly showed that majority of the respondents in the organisation used passwords and anti viruses while only a few knew how to use authorization, anti phishing and encryption.

5.2 Conclusions.

The conclusions of the study are presented in accordance to the research questions.

The first research question was “Will addressing the security risks minimize the potentially serious financial, legal and reputational implications in e-banking?” basing on this, it was found that the respondents of the organisation experienced many security risks like unauthorised access (Hacking) being experienced by the majority, attacks on the local network, spywares, phishing, spam and address forgery and man in the middle attacks.

The second research question was “Will addressing the security risks responses minimize the potentially serious financial, legal and reputational implications in e-banking?” basing on this, it was found that majority of the respondents in the organisation (45 respondents) constituting (75%) of the total sample size responded to the security threats/risks they experienced while the remaining respondents (25%) did not take any response to the security threats/risks they experienced in the organisation.

The third research question was “Will addressing the security risks management minimize the potentially serious financial, legal and reputational implications in e-banking?” basing on this research question it revealed that respondents in the organisation used only a small percentage of the security measures against the

threats/risks they experienced in the organisation. 20 respondents used pass words, 10 respondents used authentication, 15 respondents used anti viruses, only 5 used authorizations, only 4 used anti phishing, and only 6 used encryption as a measure against the security risks/threats they experienced in the organisation.

5.3 Recommendations.

According to the findings and conclusion of the study the researchers found it necessary that the following recommendations be of much importance.

The organisation should be in a position to discover all the security risks/threats not only the ones experienced by the respondents in the organisation but even those threats which seem invisible to the respondents but in one way or the other, they interfere with the normal functioning of e-banking in the organisation.

The organisation should start implementing other security measures against the security risks/threats they experience apart from the ones the respondents took and into depth which may end up minimizing the security threats/risks in the organisation. Example: using all the forms of anti-phishing which includes both the social responses and technical responses, in the case of authentication, the organisation should make sure that they use all forms authentication by authenticating all e-banking customers, both new customers and existing customers. In the case of man in the middle attacks, the organisation should use all the defenses against this security risk.

The organisation should take quicker responses against the security risks/threats the respondents experience while using e-banking so as to minimize the rates at which the threats/risks could have spread or to minimize the rate at which the threat/risk could have affected e-banking operations in the organisation.

5.4. Areas for Further Research.

Despite all the efforts made by the researchers, they can not claim that they has 100% accurately and exhaustively tackled all the problem areas hence bringing in areas requiring future or further research.

First of all, this study mainly focused on the security issues in e-banking. It was however evidently discovered that it's not only security risks which e-banking suffers from but we have other types of risks which includes;

- Strategic risks
- Operational/operational risks
- Organizational risks
- Price/market risks
- Compliance/legal risk
- Financial/cost analysis risks
- Credit risks

All of the above are risks in e-banking of which study or research can be undertaken. This study only confined only on the security issues in e-banking of which there are other issues in e-banking which are not security related but affect e-banking directly or indirectly.

5.5 Limitations of the study.

The study faced the following problems;

- ❖ Most of the employees in the bank were busy thus too limited time was posed on the researchers.
- ❖ Some of the employees were not willing to give the correct information to the researchers.
- ❖ The researchers were limited by time. Some respondents were reluctant to fill in the questionnaires and submit the questionnaires which delayed data analysis process and the final report.
- ❖ Confidentiality. The nature of some information was so sensitive that the employees were not willing to reveal to the researchers which in turn limited the amount of data collection.

Therefore, this research project has addressed the security issues in electronic banking in which the case was Equity bank Kikuyu branch (Kenya)

Reference:

Tan, Koon. "Phishing and Spamming via IM (SPIM)". *Internet Storm Center*. <http://isc.sans.org/diary.php?storyid=1905>. Retrieved December 5, 2006.

Josang, Audun *et al.* "Security Usability Principles for Vulnerability Analysis and Risk Assessment." (PDF). *Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC'07)*. <http://www.unik.no/people/josang/papers/JAGAM2007-ACSAC.pdf>. Retrieved 2007.

Felix, Jerry and Hauck, Chris (September 1987). "System Security: A Hacker's Perspective".

Ollmann, Gunter. "The Phishing Guide: Understanding and Preventing Phishing Attacks". *Technical Info*. <http://www.technicalinfo.net/papers/Phishing.html>. Retrieved July 10, 2006.

"Phishing". *Word Spy*. <http://www.wordspy.com/words/phishing.asp>. Retrieved September 28, 2006.

Stutz, Michael (January 29, 1998). "AOL: A Cracker's Paradise?". *Wired News*. <http://wired-vig.wired.com/news/technology/0,1282,9932,00.html>.

John Leyden, 'Florida man sues bank over \$90k wire fraud', http://www.theregister.co.uk/2005/02/08/e-banking_trojan_lawsuit/.

Candid Wueest, originally by Virus Bulletin (July 2005) Threats to online banking Symantec security response, Dublin
<http://www.virusbtn.com>

Telekurs group, E-banking security solutions (ESS)
Central e-banking authentication using Maestro card

APPENDICES

APPENDIX A: QUESTIONNAIRES

The researchers are in Kampala International University, school of computer studies pursuing Bachelors of computer science. The researchers are conducting research on security issues in electronic banking.

The case study is Equity bank Kenya Kikuyu branch. The purpose of the study is to fulfill the researchers' academic requirements. Therefore, the researchers kindly request you to answer the following questions.

NOTE: Your response will be treated with the highest degree of confidentiality.

Background / personal information

Please tick in the most appropriate box.

1. sex

Male

☐

Female

☐

2. Age

18- 22

☐

33- 37

☐

Above 48

☐

23- 27

☐

38- 47

☐

28- 32

☐

43- 47

☐

3. level of education

Certificate

☐

Diploma

☐

Degree

☐

Masters

☐

PhD

☐

4. Department

Financial department.

☐

Marketing and public relations department.

☐

IT department.

☐

5. marital status

Married.

☐

Single.

☐

1. For how long have you used e-banking in your institution??

Over 10 years over 5 years over 2 years
 Below 2 years
 Others
 (specify).....

2. Which of the given modes of banking do you think is more secure?

E-banking normal banking

Others

(specify).....

3. Do you experience unauthorized access (Hacking)?

Yes

No

Others

(specify).....

...

4. Do you experience attacks on your local networks?

Yes

No

5. Do you experience spywares as a threat in e-banking?

Yes

No

6. What other security issues do you experience while using e-banking?

.....

7. Did you take any response as a customer to e-banking security threat?

.....

8. What measures do you take to the security threats you experience in e-banking?

APPENDIX B: INTERVIEW GUIDE

Interviewees; Employees of Equity bank Kenya Kikuyu branch
Subject; Security issues in electronic banking

Time Allocated	Interviewer Question and objectives	Interviewee response
1-2 minutes	Objective Open the interview -Introduce my self -Thank the interviewee for his/her time -State the purpose of the interview	
5minutes	Question one What security threats do you experience with e-banking? Follow up	
5minutes	Question two What responses do you take to the security threats experienced in e-banking? Follow up	
5minutes	Question three How do you manage the security risks experienced in e-banking? Follow up	
1-3minutes	What do you think should be implemented as security risks in e-banking are concerned? Follow up	
1-3 minutes	Objective Conclude the interview	
28 minutes	Thank the interviewee for his cooperation. Time allocated for the question and answers.	