

**A SURVEY OF INFORMATION SYSTEMS SECURITY PRACTICES ADOPTED
BY COMMERCIAL BANKS IN KENYA**

**A PROJECT BY
OKOKO MICHAEL .O.
D61/P/8895/99**

LOWER KAPETE LIBRARY

**SUBMITTED TO THE DEPARTMENT OF MANAGEMENT SCIENCE IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF
MASTER OF BUSINESS ADMINISTRATION DEGREE – UNIVERSITY OF
NAIROBI**

OCTOBER 2009

To my family and friends, for all their support

ACKNOWLEDGEMENT


I thank my supervisors Kate Litondo and Joel Lelei for their tireless dedication in guiding me through this project, and my family and friends for their support throughout this program. To all my friends, classmates and workmates who helped me in any way – thank you very much.

Most of all, I thank God for staying with me to the completion of this project.

APPROVAL OF PROPOSAL

DECLARATION


This project report is my own original work and has not been submitted in any other university registration.

Signed..........
OKOKO MICHAEL .O.
D61/P/8895/99

Date.....18/11/2009.....

Supervisors Approval

This report has been submitted with our approval as university supervisors

Signed..........
KATE LITONDO
Lecturer, Department of Management Science

Date.....18/11/2009.....

ABSTRACT

Information systems security is a fundamental concept in the present times owing to the great dependency that almost all functions within an organization rely on information systems for their day to day operations to be successful in terms of cycle times, cost, efficiency, accuracy, and so on. Commercial banks perform functions such as safekeeping of money, transfer of money, and so on and they rely on information systems to perform these functions on behalf of their customers. The success of a bank is to a large extent determined by how efficiently, securely and confidentially they undertake these functions. This is determined by the information systems security practices that are put in place by a commercial bank. Some of these practices may be uniform but some may be determined by the characteristics of a particular commercial bank.

The methodology used to identify the information systems security practices adopted by commercial banks in Kenya and the organization characteristics that determine the practices was done via a survey. Questionnaires were distributed to all the commercial banks in Kenya and the data collected analyzed.

The key findings indicate that most banks have information security practices in place, however a high number do not review these practices frequently which should be of concern especially due to the rapid changes in information technology which then introduce new threats.

Commercial banks are aware of the importance of having information security practices and the threats posed to the organization due to weak practices. Banks need to frequently review these practices and share the same with other banks so that they are all up to date. More also needs to be done to make staff aware of information security practices so that they can effectively play their part in protecting the organizations information systems.

TABLE OF CONTENTS

| | Page |
|------------------------|-------------|
| Dedication..... | i |
| Acknowledgements..... | ii |
| Declaration..... | iii |
| Abstract..... | iv |
| Table of contents..... | v |
| List of Acronyms | vi |
| List of Tables..... | vii |
| List of Figures..... | viii |

CHAPTER ONE: INTRODUCTION

| | |
|---|---|
| 1.1. Background..... | 1 |
| 1.1.1 Objectives of Information Security..... | 2 |
| 1.1.2 Importance of Information Security Practices..... | 4 |
| 1.2 Statement of the Research Problem..... | 4 |
| 1.3 Research Objectives..... | 6 |
| 1.4 Importance of the Study..... | 8 |

CHAPTER TWO: LITERATURE REVIEW

| | |
|---|----|
| 2.1 Introduction..... | 9 |
| 2.2 Information Security Practices. | 10 |
| 2.3 Code of practice for Information Security Management..... | 15 |
| 2.4 Research Motivation..... | 16 |

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

| | |
|---------------------------------|----|
| 3.1 Research Design..... | 18 |
| 3.2 Population..... | 18 |
| 3.3 Data Collection Method..... | 18 |
| 3.4 Data Analysis..... | 19 |

CHAPTER FOUR: DATA ANALYSIS, FINDINGS AND DISCUSSION

| | |
|---|----|
| 4.1 Introduction..... | 20 |
| 4.2 Respondents characteristics..... | 20 |
| 4.3 Characteristics of the banks that participated..... | 22 |
| 4.3.1 Ownership of banks..... | 22 |
| 4.3.2 Banks annual turnover..... | 23 |
| 4.3.3 Banks number of customers..... | 24 |
| 4.3.4 Networking of banks branches..... | 24 |
| 4.3.5 Banks with ATM services..... | 25 |
| 4.3.6 Banks with Internet Banking services..... | 26 |

| | |
|---|----|
| 4.4 Information Security Practices..... | 27 |
| 4.4.1 Committed budget for IT department..... | 27 |
| 4.4.2 Banks with dedicated information system security function..... | 28 |
| 4.4.3 Minimum qualification for information security job function..... | 29 |
| 4.4.4 Banks professional certifications for information security personnel..... | 30 |
| 4.5 Information Security procedures..... | 31 |
| 4.5.1 Frequency of review of information security procedures..... | 31 |
| 4.5.2 Ethical hacking tests..... | 32 |
| 4.6 Information Systems components ownership..... | 33 |
| 4.7 Application of Information Security Practices..... | 34 |
| 4.7.1 Information security risk and incident handling..... | 35 |
| 4.7.2 Organization for information security function..... | 36 |
| 4.7.3 Information training and information dissemination..... | 37 |
| 4.7.4 Physical access control..... | 38 |
| 4.7.5 Backup management..... | 40 |
| 4.7.6 Disaster/contingency planning..... | 41 |
| 4.7.7 Licensing and Anti virus..... | 42 |
| 4.7.8 Data security..... | 43 |
| 4.7.9 Password management and system/data access control..... | 44 |
| 4.8 Bank's characteristics relationships..... | 46 |
| 4.8.1 Relationship between banks' characteristics and information systems practices adopted..... | 46 |
| 4.8.2 Relationship between Banks' Characteristics and Frequency of Review of Information Systems Procedures..... | 48 |

CHAPTER FIVE: DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

| | |
|---|----|
| 5.1 Introduction..... | 50 |
| 5.2 Discussion..... | 50 |
| 5.2.1 Information security practices adopted by commercial banks in Kenya.. | 50 |
| 5.2.2 Relationship between the characteristics of a bank and the information security adopted..... | 51 |
| 5.3 Conclusions..... | 53 |
| 5.4 Recommendations..... | 54 |
| 5.5 Limitations of the study..... | 54 |
| 5.6 Suggestions for further research | 54 |

| | |
|------------------------|-----------|
| REFERENCES..... | 55 |
|------------------------|-----------|

| | |
|----------------------|-----------|
| APPENDIX..... | 58 |
|----------------------|-----------|

LIST OF ACCRONYMNS

ATM – Automated Teller Machine

BSI – British Standards Institute

CISA – Certified Information Systems Auditor

CISM – Certified Information Security Manager

DTI – Department of Trade and Industry

EFT – Electronic Funds Transfer

IS – Information Systems

ISACA – Information Systems Audit and Control Association

ISMS – Information Security Management System

ISO – International Organization for Standardization

ISS – Information Systems Security

IT – Information Technology

KBA – Kenya Bankers Association

NISSG - National Information Systems Security Glossary

NIST – National Institute of Standards and Technology

NSTISSC - National Security Telecommunications and Information Systems Security
Committee

RTGS – Real Time Gross Settlement

LIST OF TABLES

| | |
|---|----|
| Table 1: Ernst & Young, Andersen and DTI Studies | 11 |
| Table 2: Respondents' Characteristics..... | 20 |
| Table 3: Information Security Risk and Incident Handling..... | 35 |
| Table 4: Organization of Information Security Function..... | 36 |
| Table 5: Information Security Training and Information Dissemination..... | 37 |
| Table 6: Physical Access Controls..... | 38 |
| Table 7: Backup Management..... | 40 |
| Table 8: Disaster/Contingency Planning..... | 41 |
| Table 9: Licensing and Antivirus..... | 42 |
| Table 10: Data Security..... | 43 |
| Table 11: Password Management and System/Data Access Control..... | 44 |
| Table 12: Relationship between banks' characteristics and information systems security job function..... | 46 |
| Table 13: Relationship between Banks' Characteristics and Information Systems Procedures Review..... | 48 |

LIST OF FIGURES

| | |
|--|----|
| Figure 1: Form of Ownership of Banks..... | 22 |
| Figure 2: Banks' annual Turnover..... | 23 |
| Figure 3: Banks' number of customers..... | 24 |
| Figure 4: Banks' with ATM services..... | 25 |
| Figure 5: Banks with internet banking service..... | 26 |
| Figure 6: Banks with a committed budget for IT Department..... | 27 |
| Figure 7: Banks with a dedicated Information Systems security job function..... | 28 |
| Figure 8: Banks' required minimum education and experience for Information Security job function..... | 29 |
| Figure 9: Banks personnels' professional certifications in Information Security... | 30 |
| Figure 10: Frequency of review of Information Security procedures..... | 31 |
| Figure 11: Banks that regularly conduct ethical hacking tests for network/systems security..... | 32 |
| Figure 12: Banks' information systems components ownership..... | 33 |

CHAPTER ONE: INTRODUCTION

1.1 Background

The U.S National Information Systems Security Glossary (NISSG) defines information security as, “The protection of information against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats” (NSTISSC, 2000).

Information Systems Security (ISS) can thus be seen as the process by which an organization protects and secures systems, media and facilities that process and maintain information vital to its operations. On a broad scale, the banking industry has a primary role in protecting the financial services infrastructure because all other industries interact with it for services such as credit, loans and custody for cash and other valuables such as title deeds. The security of the industry’s information systems is essential to the privacy of customer’s financial information. Banking operations are also made quite complex due to the diversity of their clientele who have different needs. Individual banks and their service providers must therefore maintain effective Information Security (IS) programs adequate for their operational complexity. These information security programs must have strong board and senior management level support, integration of security responsibilities and controls throughout the organization’s business processes, and clear accountability for carrying out security responsibilities.

Previously, the banking process used to be manual based whereby all transactions were captured, processed and stored manually in physical paper files or bank account holder pass books (which show details of transactions that have gone through an account). The banking process has shifted from manual based to electronic based. Transaction capture, processing, storage and retrieval is now mostly in electronic form across the banks. The shift to electronic based processing has introduced new challenges which need to be addressed. These challenges have made banking operations and systems vulnerable to various threats, which Dhillon and Backhouse (2001) have broadly classified as deliberate and includes threats such as hackers, fraud, viruses, and theft; and accidental,

which includes threats such as system errors, data inaccuracy due to incorrect input of data, system failure/crash, natural calamities such as earthquakes and floods.

The counter measures introduced to prevent, detect and react to these threats so as to ensure minimum impact to an organization's resources make up information security practices. The controls are broadly classified as Preventive, Detective, and Corrective and would range from physical controls to administrative controls. Due to the role played by the banking industry in the nation's economy, information security becomes quite critical in this industry.

1.1.1 Objectives of Information Security

Dhillon and Backhouse (2001) identify five objectives of information security. Firstly, there is confidentiality which covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use. Secondly, there is integrity. System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability. Thirdly, there is availability. The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information and/or systems. Fourthly, there is accountability which involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, intrusion detection, recovery, and legal admissibility of records. Lastly there is assurance which addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

Historically, up to 1990, confidentiality was the most important element of information security, followed by integrity, and then availability. By 2001, changing use and

expectation patterns by users of information technology had moved availability to the top of this list. The first goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice and particularly in the face of denial of service attacks (Heather and Neil, 2003).

Information security is not only confined to computer systems, nor to information in an electronic or machine-readable form. Information security applies to all aspects of safeguarding or protecting information or data, in any form. It aims at eradicating all risk of improper or malicious access and use of any information resource. The level of information security sought in any particular situation should be commensurate with the value of the information and the loss, financial or otherwise, that might accrue from improper use, for example, disclosure, degradation, or denial (Heather and Neil, 2003).

Organizations often inaccurately perceive information security as the state or condition of information security controls at a particular point in time. Information security is an ongoing process, whereby the condition of an organization's information security controls is just one indicator of its overall information security position. Other indicators include the ability of the institution to continually assess its position and react appropriately in the face of rapidly changing threats, technologies and business conditions. A bank establishes and maintains effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk tolerance levels. A bank should define information security practices to protect their information by instituting an information security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks. This would then form the organizations information security policy (Heather and Neil, 2003).

Banks developing or reviewing their information security controls, policies, procedures, or processes have a variety of sources to draw upon. First, there are country laws and regulations which address security. Secondly, there are industry regulators such as the Central Bank of Kenya or the Kenya Bankers Association (KBA) who have issued

numerous security related guidance documents. Thirdly, there are a number of third-party or security industry resources to draw upon for guidance, including external auditors, consultancy firms, insurance companies and information security professional organizations. Lastly, many national and international standard-setting organizations are continuously defining information security standards and best practices for Information Technology (IT) aspects such as electronic commerce. The various available standards provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices. Some of the organizations that are continuously setting standards and best practices for IT include National Institute of Standards and Technology (NIST); Information Systems Audit and Control Association (ISACA) who offer certifications such as CISA (Certified Information Systems Auditor) and CISM (Certified Information Security Manager); International Organization for Standardization (ISO) who have come up with specific standards such as the Code of Practice for Information Security Management (ISO/IEC 17799) and Security Techniques (evaluation criteria for IT security - ISO/IEC 15408).

1.1.2 Importance of Information Security Practices

The importance of protecting information system resources has been brought about by the increased reliance of business operations on information systems in carrying out day to day activities. For organizations such as banks that offer a wide variety of services to a diverse range of customers, confidentiality, accuracy and timeliness of information is crucial. This contributes further to the complexity of their operations which in turn makes them vulnerable to threats such as fraud.

Banks also use information systems for internal purposes such as payroll processing, document imaging and electronic filing. In addition, they have to give accurate bank statements to customers at the end of each agreed period. This is one of the most important reports that a bank generates and sends out to its customers. Its accuracy cannot be compromised as it reflects transactions undertaken on a customers account within a certain period. It can also be used in a court of law as evidence of movement of funds between different individuals, organizations or accounts. Transactions such as time

deposits, mortgage repayment schedules and loan repayments require the banks to give their customers accurate transaction details such as principal amount, interest to be paid and contract tenor. This requires high levels of accuracy in methods of data capture, processing and information output.

There have been great advancements in physical security controls such as automatic emergency door locking mechanisms, armed security personnel, armored vehicles and alarm systems. Electronic monitoring mechanisms have also advanced with introduction of surveillance cameras and physical access logs (for doors and safes). These advancements have made it difficult for criminals to continue with the traditional bank robbery styles where they easily gained access to banks, ask for the safes to be opened and make away with physical cash.

In today's high tech and interconnected world, every organization needs a well thought out information security policy to govern the organization's information security practices. Information security is a business issue, not just a technology issue. The reason organizations want to protect information should be for sound business purposes. Corporate knowledge and data are arguably the most important assets of any organization. Corporations must ensure the confidentiality, integrity and availability of their data. This can only be achieved by having sound information security practices throughout the organization (Higgins, 1999).

1.2 Statement of the Problem

Advancements in technology such as availability of the internet, credit cards, high technology printers and inter-connectivity of branches have all opened up new opportunities for criminals to perpetuate fraudulent transactions without leaving behind clues that may lead the authorities to arrest them. The direction being taken by banks in executing transfer of funds is towards electronic methods. This is evidenced in the new products and services being introduced by banks, such as internet banking, mobile phone banking, Automated Teller Machines (ATMs), credit cards and debit cards. The use of Electronic Funds Transfer (EFT) and Real Time Gross Settlement (RTGS) involve

transfer of high value transactions electronically. If adequate information security controls are not put in place for such methods of transferring funds, very huge financial losses can be incurred.

Banks also have sensitive information pertaining to their clients which most customers would not like to be made public. This includes information such as customer credit ratings, assets, liabilities, financial performance reports and shareholding composition/ownership reports. Should information security be compromised and such information ends up with third parties such as competitors or even journalists, the information can be used to the disadvantage of the customer by being made public in the media or being used by competitors in formulating their business strategies. The Banking Act – Exchange of Information Regulation (2004) prohibits banks from disclosing customer information, unless to a regulatory authority such as the Central Bank, Kenya Revenue Authority or the Kenya Anti-Corruption Commission.

The survey conducted by Ernst and Young in 2005 found that the gap continues to widen between the growing risks brought on by rapid changes in the global business environment and what information security is doing to address those risks (Ernst and Young, 2005). The survey identified new technologies as cause for significant security concerns. Among the new technologies found to be cause for concern included mobile computing (53%); removable media (49%); wireless networks (48%); voice over IP telephony (21%); OPEN SOURCE (10%); and server virtualization (8%).

The survey conducted in 2008 had the following ten conclusions. First was that protecting reputation and brand has become a significant driver for information security; second was that despite economic pressures, organizations continue to invest in information security; third was that international information security standards are gaining greater acceptance and adoption; fourth was that many organizations still struggle to achieve a strategic view of information security; fifth was that privacy is now a priority, but actions are falling short; sixth was that people remain the weakest link for information security; seventh was that growing third-party risks are not being addressed;

eighth was that business continuity is still bound to information technology; ninth was that most organizations are unwilling to outsource key information security activities; tenth was that few companies hedge information security risks with cyber insurance (Ernst & Young, 2008).

The background differences amongst banks in Kenya may result in differences in the information security practices adopted by each one of them. Several other factors such as the length of time a particular bank has been in operation, number of customers, number of branches, number of employees, number of electronic devices interacting with the bank, ownership and organization structure may also influence their information security practices. This warrants the need to research on the information systems security practices put in place by banks in Kenya. The importance of information security to customers and banks gives rise to the question, what information systems security practices have banks in Kenya adopted?

Past studies by Richu (1989), Wasilwa (2003) and Ogeto (2004) show that organizations tend to focus on specific information security aspects such as input controls only or processing controls only, and so on. Few organizations have implemented a combination of these controls but none has implemented all of them. Richu (1989) and Wasilwa's (2003) studies focused on the banking industry while Ogeto's (2004) focused on the manufacturing industry. These findings and the ones of Ernst and Young (2008) form the basis of researching on information security practices that have been adopted by Kenyan banks so far. This is further reinforced by the increased rate of adoption of new technologies by Kenyan banks, which Ernst and Young (2005) identified as the cause of significant security concerns.

1.3 Research Objectives

The research objectives are:

1. To establish the information security practices adopted by commercial banks in Kenya.
2. To establish whether there is a relationship between the characteristics of a bank and the information security practices adopted.

1.4 Importance of the Study

It is anticipated that the findings of this study will be of value to the following groups:

1. The management of banks or information security officers who are charged with the responsibility of overseeing implementation of information security policies in their organizations.
2. Bank 'regulatory organizations such as the Central Bank of Kenya and the Kenya Bankers Association in coming up with basic information security practices within the industry.
3. Consultancy/Audit firms who also undertake information security audits, in identifying information systems security practices that they can incorporate in their information security audit checklists and recommendations on improving information security.
4. Scholars, academicians and researchers could use the findings from this study as a reference point in various aspects of information security practices and further study or research.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

It has become a necessity for organizations of all shapes and sizes to enthusiastically embrace information technology if they wish to survive. This is also necessary if an organization expects to thrive in a highly competitive environment, in which effective operational control and strategic direction are increasingly dependent on the availability and exploitation of high quality information. Consequently, it is vital that adequate security and control procedures are introduced to ensure that all the information embedded within organizational information systems retains its integrity, confidentiality and availability (Dhillon and Backhouse, 2001).

However, there is also extensive evidence to suggest that the threats, to the security of organizational information and information systems, are now growing in number, variety and, most importantly, the severity of their impact (Angell, 1996). For example, traditional threats to the security of information and systems include: natural disasters, theft of hardware/software, unauthorized access and human error (Lock *et al.*, 1992), while newer threats include viruses (Post and Kagan, 2000) and hacking and cyber terrorism (Furnell and Warren, 1999). To a large extent, such threats are growing because of higher levels of interconnectivity both within and between organizations (Dinnie, 1999; Barnard and von Solms, 1998; DTI, 2002). In particular, it is the increasing incidence of intra-organizational systems that is creating problems for organizations, as information security is upgraded from being merely a “domestic” issue to one that involves third parties, such as external business partners (von Solms, 1998). The rise of electronic commerce has also heightened awareness among organizations of the security threats to which they are likely to be exposed. Indeed, it has been reported that security threats, and fear of security breaches, constitute the greatest inhibitors to an expansion in the uptake of electronic commerce (Ernst & Young, 2001).

In the world of e-business and extended enterprises, there are no effective geographical and organizational boundaries. If levels of internet protection are not applied equally and everywhere, the weakest link will expose all others in the chain to attack (KPMG, 2002)

Increased interconnectivity is not, however, the only factor making computers, and the information therein, less secure. For example, the widespread recognition that information now constitutes a “key corporate asset”, which is of great commercial value (Gerber *et al.*, 2001), has also brought information security nearer to the top of the management agenda. Perhaps inevitably, the increased risk of information security problems has led to a growing awareness among the managers of organizations of the need for careful and effective information security management. For example, it is widely acknowledged that effective information security management is dependent on a number of key factors (von Solms, 1998; Siponen, 2000), most notable among these being: the need for senior management commitment and support to information security management; the detailed assessment of potential security risks and threats; the implementation of appropriate controls to minimize or guard against those risks and threats; and the thorough communication of security issues to users of both information and information systems through relevant education and training. However, it has also been recognized that effective security management, including all the above factors, is predicated on the formulation, dissemination and operation of an information security policy. As Hone and Eloff (2002) acknowledge, “one of the most important controls is the information security policy”, while Higgins (1999) notes that the information security policy is the start of security management. This is because the information security policy forms the foundation upon which information security practices are built upon.

The importance of the information security policy, as a document of strategic importance within organizations today, is widely acknowledged. This is because the information security policy gives rise to the information security practices prevalent in an organization. The issue of information security practices has now become an integral part of a variety of commercial surveys into information security breaches and safeguards (Andersen, 2001; Ernst & Young, 2001; DTI, 2002).

2.2 Information Security Practices

There is a growing recognition that effective information security management is predicated on the existence and execution of an information security policy. As Higgins

(1999) notes, “without a policy, security practices will be developed without clear demarcation of objectives and responsibilities”. However, there is also a growing concern that too many organizations are failing to heed this advice, as witnessed by the low levels of uptake of formal information security policies (Arnott, 2002), and the inadequacies in policies, where they do exist (Moule and Giavara, 1995; Hone and Eloff, 2002). Some interesting insights about information security policy can be gained from a number of more general studies of information security. Table 1 summarizes some background details about these studies (Heather and Neil, 2003).

Table 1: Ernst & Young, Andersen and DTI Studies

| Study | Sample Size | Location | Research Method |
|----------------------|-------------|--|---|
| Ernst & Young (2002) | 273 | European Businesses | Telephone interviews using structured questionnaires with IT directors and business executives |
| Andersen (2001) | 900 | European Businesses | Questionnaires distributed during business seminars to IT specialists or senior managers |
| DTI (2002) | 1000 | UK organizations (private and public sector) | Telephone interviews using structured questionnaires with individuals responsible for information security management |

Each study explored the prevalence and range of security incidents experienced by European organizations in the past couple of years. They concluded that there is an upward trend in the number of incidents occurring and in the severity of individual incidents. More importantly, the studies also explicitly investigated the uptake of information security policies. For example, the Andersen (2001) study showed that 65 percent of the organizations surveyed (most of which were large organizations) had an information security policy in place, and the DTI (2002) survey showed that 27 percent

of UK businesses have a policy in place. The DTI study further showed that 59 percent of the large organizations surveyed had implemented a policy. Significant in these DTI results is that again an upward trend is noted from earlier studies: the DTI (2000) study, for example, reported that only 14 percent of the organizations surveyed had an information security policy in place. Moreover, the 2002 study noted that a higher proportion of organizations with a policy were undertaking annual policy updates than was the case in 2000.

The Andersen (2001) study is of particular interest, as it highlights the discrepancy between the views of business managers and those of IT managers: 82 percent of the business managers surveyed believed that their organization had a comprehensive policy in place, whereas only 66 percent of the IT managers believed this to be the case. This could suggest that a survey targeting IT managers, who presumably typically have a more detailed knowledge of information security issues than business managers, is likely to yield a more realistic assessment of the information security situation in an organization. The Ernst & Young (2001) survey found that organizations believed “employee awareness” to be the greatest “challenge to achieving the required level of security”, a message that is strongly echoed by Siponen (2000). Given this finding, it seems somewhat disconcerting that, of the 27 percent of organizations in the DTI (2002) survey having an information security policy, only 7 percent of them implemented their policy in order to make employees aware of security issues. The primary motivation for having a policy (as reported by 67 percent of organizations that have a policy) was the recognition that it is considered to be “good practice”. It was further reported in the DTI (2002) survey that few organizations make their employees aware of information security issues on induction. It seems, therefore, that, while policy formulation might be on the increase, an emphasis on dissemination of security concerns to employees and practical policy implementation is very low on the agenda of many organizations.

The surveys undertaken by KPMG from the year 2000 are also of great importance. The 2000 survey had an overall finding that information security requirements are not being adequately addressed, especially in the new fast moving, global, e-business environment

and the overall effect is that this will leave some organizations critically exposed. The survey was conducted on 179 companies and 98% of them said they currently use the internet. This compares with 70% in 1998 and 35% in 1996 (KPMG, 2000). The major findings were new e-risks are not being managed; security is not being taken seriously; security breaches are on the rise; IT is still driving security, and not the business; logical access controls are not getting any better; a modest improvement in traditional IT security was detected.

The KPMG (2002) survey generally concludes that the same findings are still present. However, it is of concern that security breaches were identified to be on the rise compared to 2001. More awareness to information security practices saw an increase in the number of information security metrics. For instance, more companies had dedicated information security officers; security policies were being implemented; firewalls were in place; and internet security practices. On the other hand, a number of key risk areas also increased such as virus incidents (62.5%); email intrusion (49%); theft of equipment (5%); external attack (90%). This means more resources were being channeled towards information security practices (KPMG, 2002).

The Ernst and Young survey conducted in 2004 identified lack of user awareness as the top obstacle to effective information security. More than 50% of the respondents failed to provide employees with on going training in information security and controls. This contributed to the dismal rating of 40% of respondents failing to provide their employees with instruction on classifying data, for example, confidential. It was worth noting that 100% of respondents deployed anti-virus technology to protect themselves. Continuity of business in the event of a disaster was not being given priority since less than 50% agreed that they could continue with their business in the event of a serious disruption (Ernst and Young, 2004).

The KPMG survey of 2006 concluded that the most important overall security issue is now perceived as being data quality and integrity (26%) followed by internet/intranet issues (17%) compared to internet and e-commerce (37%) and virus attacks (15%) in

2004. The greatest threats to organizational information systems are now seen as lack of employee awareness (22%), poor implementation of security policies (18%) and current employees' misconduct (17%). The fact that hackers are now seen as the greatest threat by only 8% (against 24% in 2004), likely reflects the increased attention paid to security measures by many organizations during the last two years (KPMG, 2006).

Of concern in the KPMG survey of 2006 is the fact that 22% of respondents still rated their management as being very aware of security risks (against 20% in 2004) while awareness of IT staff 77% (against 60% in 2004). There's still room for improvement and information security needs to be taken to the strategic management level and be recognized as a major risk area for the organization. Further, the responsibility for security continues to reside in the hands of the IT department (69% against 56% in 2004) and Finance department (12% against 21% in 2004). Only 20% of organizations have a computer security officer (against 16% in 2004 and 15% in 2002). Also of greater concern is that only 31% of organizations now have a formal security policy, down from 38% (2004) and 26% (2002). However, for those with formal security policies, aspects covered by the policies have increased in most areas (KPMG, 2006).

Richu's (1989) study was undertaken with reference to security considerations in banks and financial institutions in Kenya. The study found that within this industry information security practices tended towards physical controls. In terms of importance, physical controls ranked highest followed by procedure controls, then hardware controls and lastly authentication mechanisms. The study further observed that the industry had adopted various information system security practices such as anti-virus software, email logs/filters, system administration logs, encryption, intrusion detection systems, one-time password generators and periodic password change.

Wasilwa's (2003) study was undertaken with reference to computer security vulnerability in the banking industry in Kenya. The study found that the major threat facing computer systems within the industry was the organizations own employees. The study found that most banks have effectively adopted practices to countermeasure computer security

threats. It further found that the introduction of the internet and other technological developments have resulted in greater information systems security risks through the introduction of multiple system entry points.

Ogeto's (2004) study was undertaken with reference to computer based information security in the manufacturing industry. The study found that part of the problems faced with implementing security practices was under financing of the IT departments. It further found that the information systems security teams did not include members from other units.

2.3 Code of Practice for Information Security Management

One of the most widely used information security standards internationally is the ISO Code of Practice for Information Security Management, that is, the ISO 17799 standard. It came from the BS 7799 standard which set out the requirements for an Information Security Management System (ISMS) to identify, manage and minimize the range of threats to which information is regularly subjected (ISO, 2000). According to the ISO 2000, the BS 7799 identifies ten domains of controls.

First is security policy. This provides management with direction and support for information security. It provides guidelines and management advice for improving information security. Second is organizational of information security. This facilitates information security management within the organization. Third is asset classification and control which is to help an organization identify their assets and appropriately protect them. It involves carrying out an inventory of all assets within the organization and effectively protecting these assets. Fourth is personnel security which aims to reduce the risk of human error, theft, fraud or misuse of facilities. This appreciates that personnel also pose a threat to information systems within an organization. Fifth is physical and environmental security which is to prevent unauthorized access, damage and interference to business premises and information. Sixth is communications and operations management to ensure the correct and secure operation of information processing facilities and devices. Seventh is access control. This involves practices aimed at

controlling the access to information. It ensures that only relevant people have access to particular information. Eighth is systems development and maintenance to ensure that security is built into information systems. This ensures that when systems are being developed or implemented, security is also put in the forefront. Ninth is business continuity management. This is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. This ensures that should there be any failure, or disruption to normal business operations and facilities, the business is not interrupted and they are able to recover within the shortest possible time. Lastly is compliance in order to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement;

It should be noted that, while this literature review has focused upon the BS 7799 standard, the work has far wider international relevance, as the British Standard became an international standard in 2000: ISO 17799 (ISO, 2000).

2.4 Research Motivation

Though the importance of information security is being increasingly recognized, a number of significant gaps exist, particularly in the academic literature. An obvious gap is that, while a number of major surveys have been conducted to investigate information security issues, these have largely been commercially oriented, rather than formal academic studies. Moreover, these empirical studies have covered a broad range of information security issues, rather than focusing specifically on information security policies and practices of a particular industry and whether the characteristics of the organization influence information security practices.

It is envisaged that the present academic oriented study will, therefore, make an important contribution to the existing body of literature, providing insights into security and policy issues from an academic perspective. It is anticipated that these findings can, in turn, be fed back to the relevant practitioner communities, as well as to those involved in the compilation of appropriate national and international standards and guidelines.

Another very evident gap is the limited research that has been done in this area locally. Some organizations have themselves conducted a survey to assess their information security standards while others have engaged services of consultants to do the same. These are specific to the organization and are not made public. There are no publicly available results of a survey conducted across the banking industry to assess the information security practices adopted by organizations. As a result, this study will open up a new area whereby further research studies can be undertaken.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1 Research Design

The survey method was used. This was to capture the data required to identify the information systems security practices adopted by banks in Kenya in protecting their information systems resources and also identify the characteristics that have contributed to the adoption of these practices.

3.2 Population

The survey was restricted only to the fully fledged commercial banks and excluded the non-bank financial institutions, mortgage companies, micro-finance institutions, co-operative societies, building societies, savings and loan schemes and trust schemes. Fully fledged commercial banks under Central Bank statutory management were not considered because it would not be possible to get information from them.

This year (2009) there were a total of 43 fully fledged commercial banks in Kenya according to the Central Bank of Kenya published list (Appendix I). The study targeted all of them.

The banks were grouped into three broad categories based on ownership (Appendix I):

- i) Foreign owned commercial banks.
- ii) Commercial banks with Government participation.
- iii) Commercial banks that are wholly locally owned.

3.3 Data Collection Method

The study used primary data collected by means of a questionnaire.

The study targeted the person charged with the information security function. In the absence of a designated Information Security Officer, the Information Technology Manager was targeted or anyone within the information technology department who is responsible for the information security function.

3.4 Data Analysis

The questionnaires received from the respondents were thoroughly checked to ensure that they have been fully completed.

The first objective was attained by use of factor analysis. This was used to determine the most prevalent information security practices as captured by Section C of the questionnaire.

The second objective was attained by use of cross tabulation. This was used to establish if there is a relationship between characteristics of a bank, as captured in Section B of the questionnaire, and the information security practices captured in Section C. Specifically, the relationship between characteristics such as ownership, annual turnover and number of years in operation were cross tabulated with frequency of review of information security procedures and also with having a dedicated information security job function.

CHAPTER FOUR: DATA ANALYSIS, FINDINGS AND DISCUSSION

4.1 Introduction

The data collected from this study was analyzed using SPSS version 17. The response rate of the study was 74%, which represented 32 banks out of the targeted 43 banks. The low response rate can be attributed to unwillingness by respondents to divulge sensitive and private information about their bank on information security practices.

4.2 Respondents Characteristics

The table in the next page provides a summary of respondents' characteristics in terms of department, position, working period, qualifications and age.

Table 2: Respondents' Characteristics

| Characteristic | Descriptive | Percent | Count |
|---------------------------------|-----------------------------------|----------------|--------|
| Department | Information Technology | 72% | 23 |
| | Internal Audit | 9% | 3 |
| | Information Security | 6% | 2 |
| | Systems Support | 13% | 4 |
| | Systems Administration | 35% | 11 |
| Position | Information Systems Officer | 22% | 7 |
| | Information Security Officer | 9% | 3 |
| | Information Technology Manager | 19% | 6 |
| | Information Technology Supervisor | 9% | 3 |
| | Information Technology Assistant | 6% | 2 |
| Working Period | 0 – 5 years | 56% | 18 |
| | 6 – 10 years | 35% | 11 |
| | 11 – 15 years | 9% | 3 |
| Highest Qualification | Diploma | 19% | 6 |
| | Undergraduate | 72% | 23 |
| | Postgraduate | 9% | 3 |
| IT related Qualification | IT related | 91% | 29 |
| | Non IT related | 9% | 3 |
| Age group | Below 30 yrs | 38% | 12 |
| | 31 – 35 yrs | 35% | 11 |
| | 36 – 40 yrs | 13% | 4 |
| | 46 – 50 yrs | 14% | 5 |
| Total | | 100% | |
| | | (Per Category) | 32 (N) |

The respondents were asked to reveal work related details of the banks they were representing in this survey, academic qualifications and their ages. The analysis indicated

that 23 (72%) respondents were working in the Information Technology (IT) departments of their banks, 3 (9%) respondents were working in the Internal Audit departments of their banks, 2 (6%) respondents were working in the Information Security departments of their banks and 4 (13%) respondents were working in Systems Support departments of their banks.

The respondents held different work positions in their banks. It was indicated that 11 (35%) respondents were working as System Administrators, 7 (22%) respondents were working as Information Systems Officers, 3 (9%) respondents were working as Information Security Officers, 6 (19%) respondents were working as IT Managers, 3 (9%) respondents were working as IT Supervisors and 2 (6%) of the respondents were working as IT Assistants.

The participants had worked for different periods in their current banks. The results showed that 18 (56%) respondents had worked between 0 – 5 years, 11 (35%) respondents had worked between 6 – 10 years and 3 (9%) respondents had worked between 11 – 15 years.

The study also sought to establish the highest qualifications of the respondents and whether the qualifications were IT related. The results showed that 6 (19%) respondents had Diploma qualifications, 23 (72%) respondents had undergraduate qualifications and 3 (9%) respondents had post-graduate qualifications. Further, those that had IT related qualifications were 29 (91%) respondents and those that did not have IT related qualifications were 3 (9%) respondents.

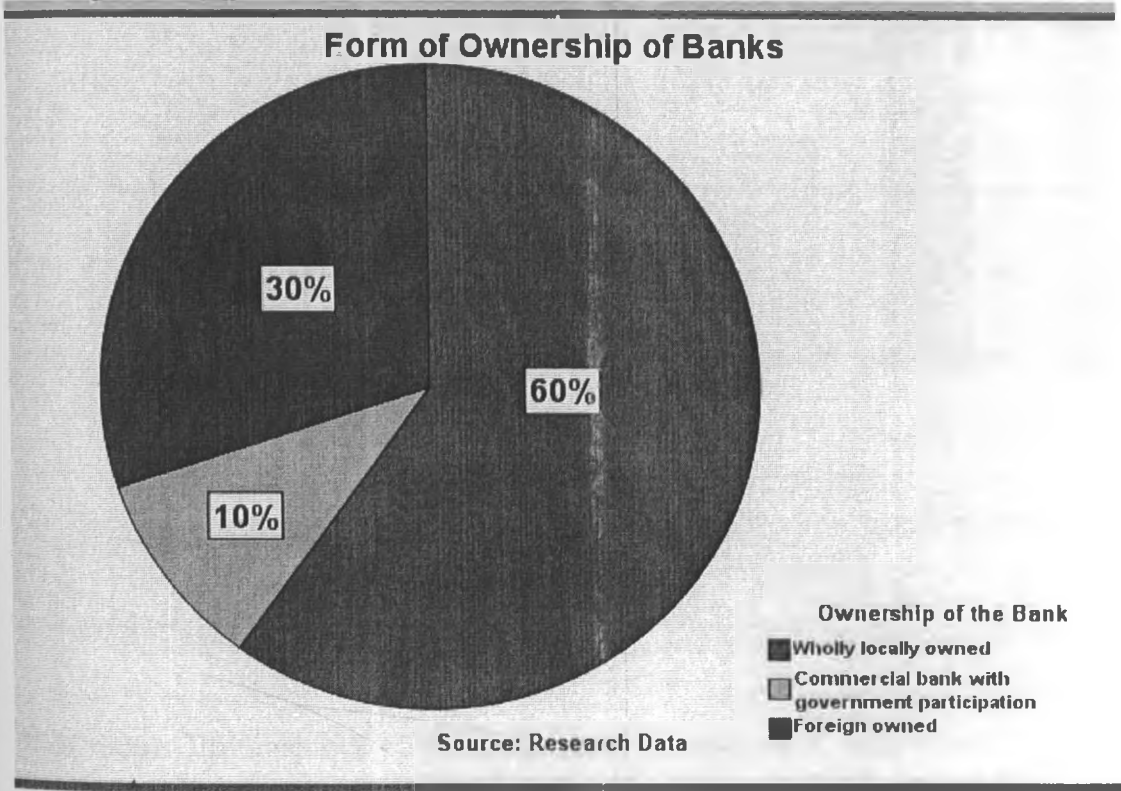
The respondents were asked to reveal their age groups. The results showed that 12 (38%) respondents were below the age of 30 years, 11 (35%) respondents were aged between 31 – 35 years, 4 (13%) respondents were aged between 36 – 40 years and 5 (14%) respondents were aged between 46 – 50 years.

4.3 Characteristics of the Banks That Participated

4.3.1 Ownership of the Banks

The banks were grouped into three broad categories based on ownership. These were foreign owned commercial banks, commercial banks with government participation and commercial banks that are wholly locally owned. The respondents were asked to reveal the category of ownership of their banks. The results indicated that 19 (60%) of the banks were wholly locally owned, 10 (30%) of them were foreign owned and 3 (10%) were commercial banks with government participation. Figure 1 shows the proportions.

Figure 1: Form of Ownership of Banks

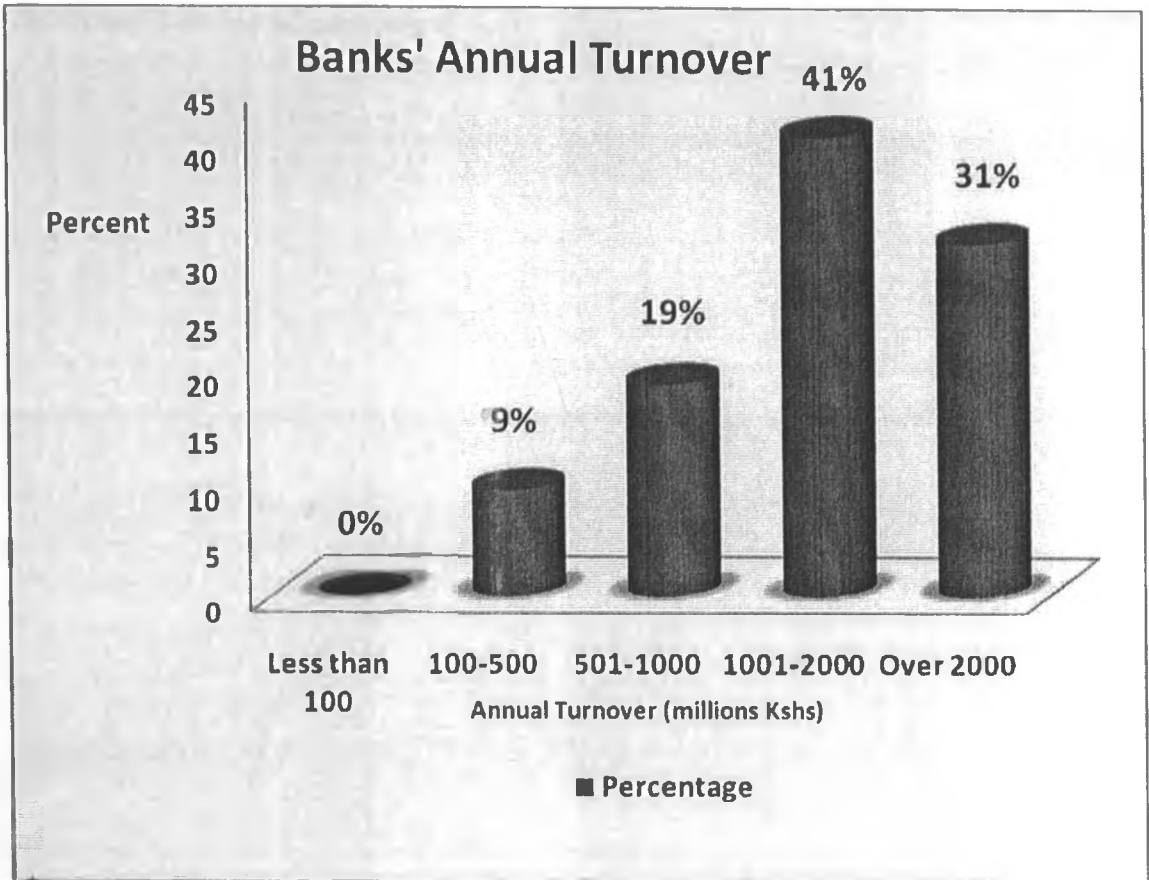


This can be interpreted that majority of the banks that participated in this survey were wholly locally owned banks. Banks with government participation were the least, at only 2.

4.3.2 Banks Annual Turnover

The respondents were asked to reveal details of their bank's annual turnover. The results indicated that 10 (31%) banks had an annual turnover of over Ksh 2,000,000, 13 (41%) banks had an annual turnover of Ksh 1,000,001 – 2,000,000, 6 (19%) banks had an annual turnover of Ksh 500,001 – 1,000,000 and 3 (9%) banks had an annual turnover of Ksh 100,000 – 500,000. Figure 2 shows the proportions.

Figure 2: Banks' annual Turnover

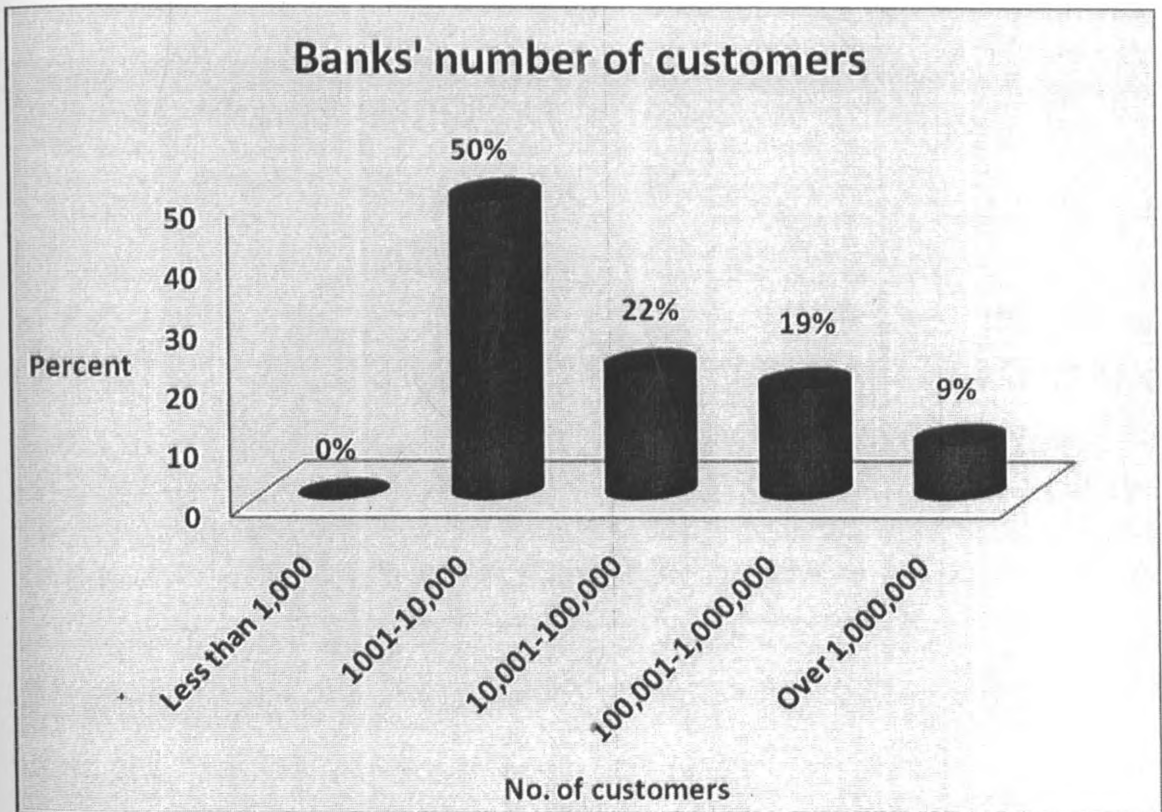


This means that majority of the banks that participated in this survey have annual turnovers within the range of 1 to 2 billion Kenya Shillings.

4.3.3 Banks' Number of Customers

The banks have different services depending on the trust the customers have on their banks of choice. The bank employees who participated in this study were asked to indicate details on the number of customers their banks have. The results indicated that 16 (50%) banks had between 1001 – 10,000 customers, 7 (22%) banks had between 10,001 – 100,000 customers, 6 (19%) banks had between 100,001 – 1,000,000 customers and 3 (9%) banks had over 1,000,000 customers. Figure 3 shows the proportions.

Figure 3: Banks' number of customers



This means the majority of the banks that participated in this survey had a customer base of between 10,000 and 100,000.

4.3.4 Networking of Banks' Branches

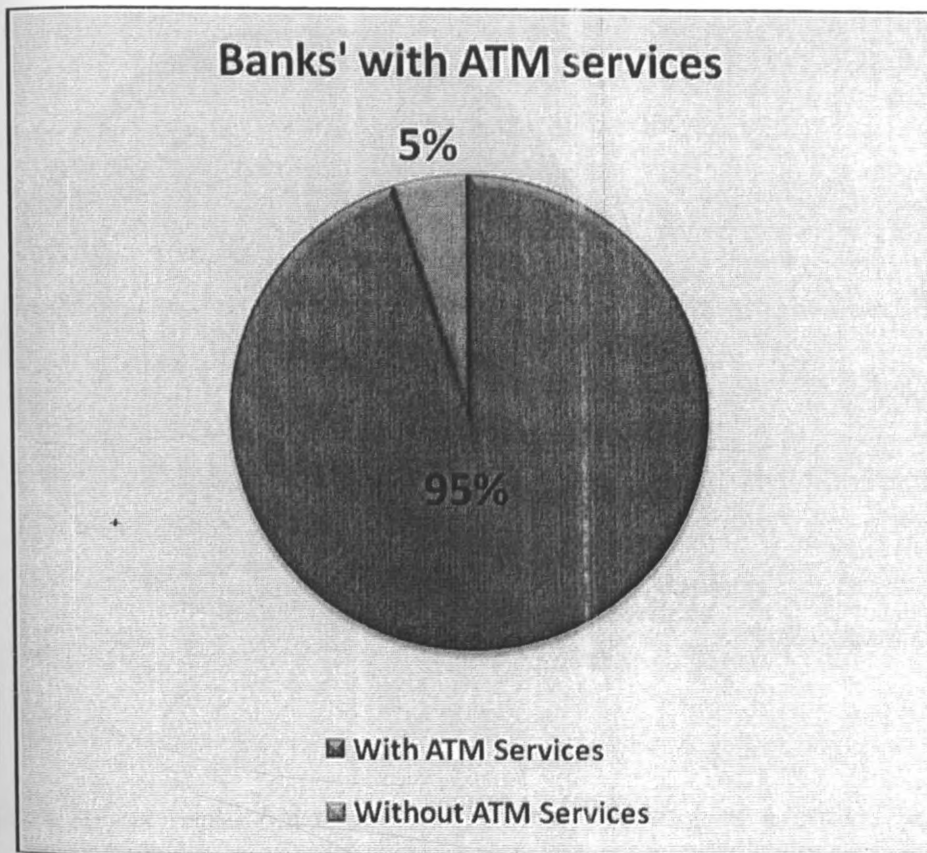
Networking of branches enhances the inter-linking of banks for efficient transactions among the bank's branches. All the 32 banks (100%) that were represented in this survey had their branches networked.

This is an indication that banks have embraced technology and have branches networked to better serve customers and offer competitive services.

4.3.5 Banks with ATM services

Bank ATM services allow customers to access money in 24-hour service beyond the normal bank working hours. The results indicated that 30 (95%) banks had ATM services while 2 (5%) banks did not have ATM services. The proportions are shown in figure 4.

Figure 4: Banks' with ATM services



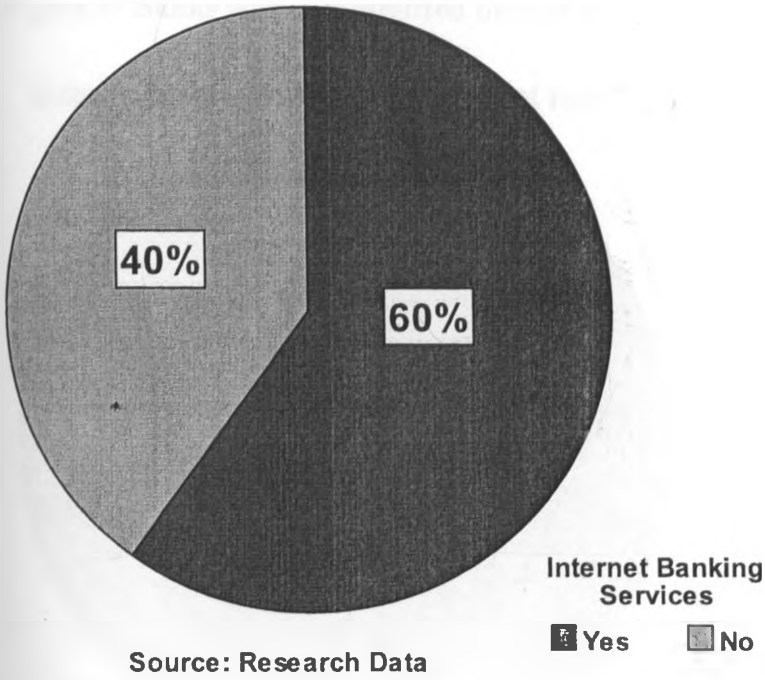
This is an indication that not all banks offer ATM services. This is attributable to banks with few customers who are most likely corporate customers hence no need to invest in ATMs.

4.3.6 Banks with Internet Banking Services

Banks offer Internet Banking Services to enable customers to access their account information and transactions online. The participants were asked whether their banks were offering internet banking services. The results indicated that 19 (60%) banks were having internet banking services and 13 (40%) banks did not have internet banking services. Figure 5 shows the proportions.

Figure 5: Banks with internet banking service

Banks with Internet Banking Service



This means banks have embraced internet banking as a critical service offering to customers.

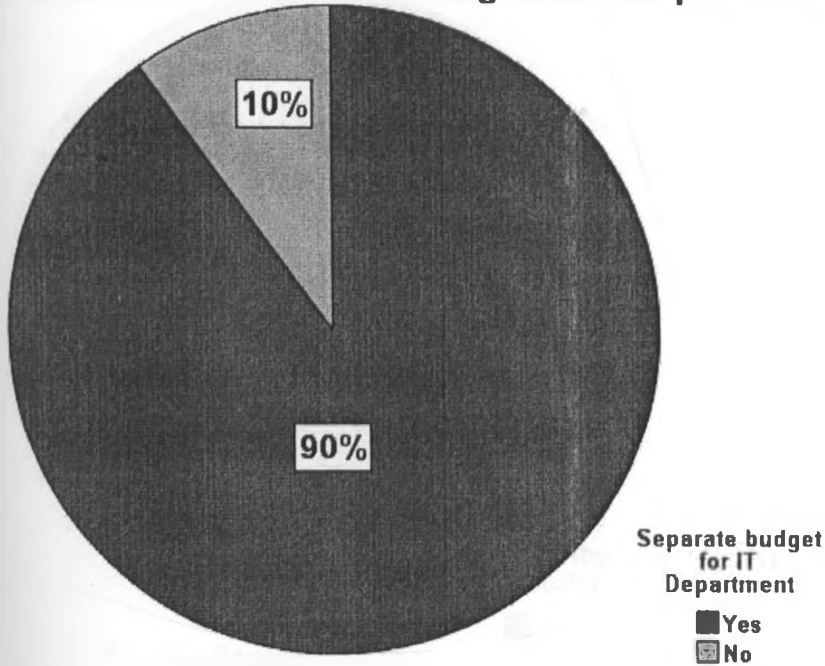
4.4 Information Security Practice

4.4.1 Committed Budget for IT Department

Banks can either allocate or not allocate a financial budget for information technology department. The respondents were asked whether the banks they represented committed financial budget for the IT department. The outcome indicated that 29 (90%) banks had a committed budget for their IT departments while 3 (10%) banks did not have a committed budget for their IT Departments. The proportions are shown in figure 6.

Figure 6: Banks with a committed budget for IT Department

Banks with a committed budget for IT Department



Source: Research Data

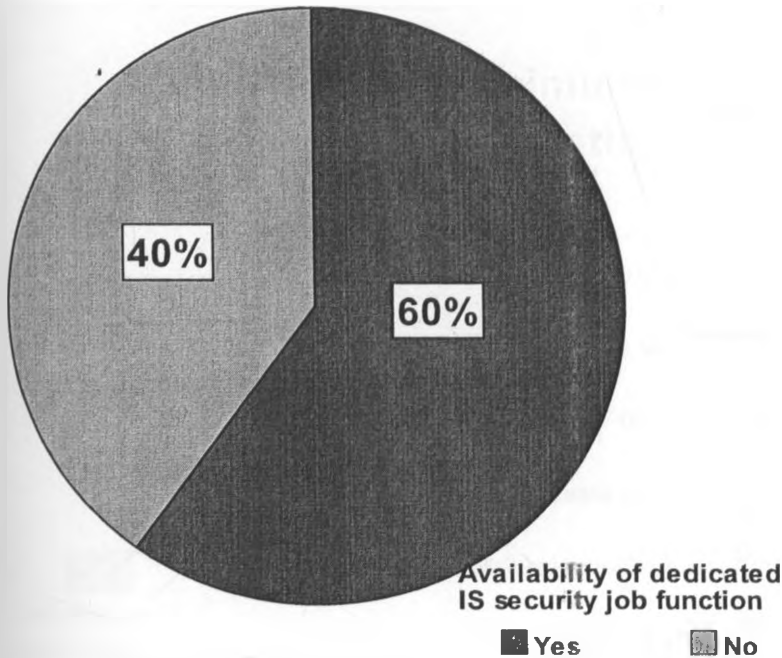
This means the independence of the IT function is being embraced across the banks. This is evidenced by the high percentage of banks that have separate budgets for IT department functions.

4.4.2 Banks with a Dedicated Information Systems Security Job Function

Information security is an important core bank function. However, different banks vary in their dedication of information security function. The respondents were asked whether their banks had a dedicated information security job function. The outcome indicated that 19 (60%) banks had a dedicated information systems security job function while 13 (40%) banks did not have a dedicated information systems security job function. Figure 7 shows the proportions.

Figure 7: Banks with a dedicated Information Systems security job function

Banks with dedicated Information Systems security job function



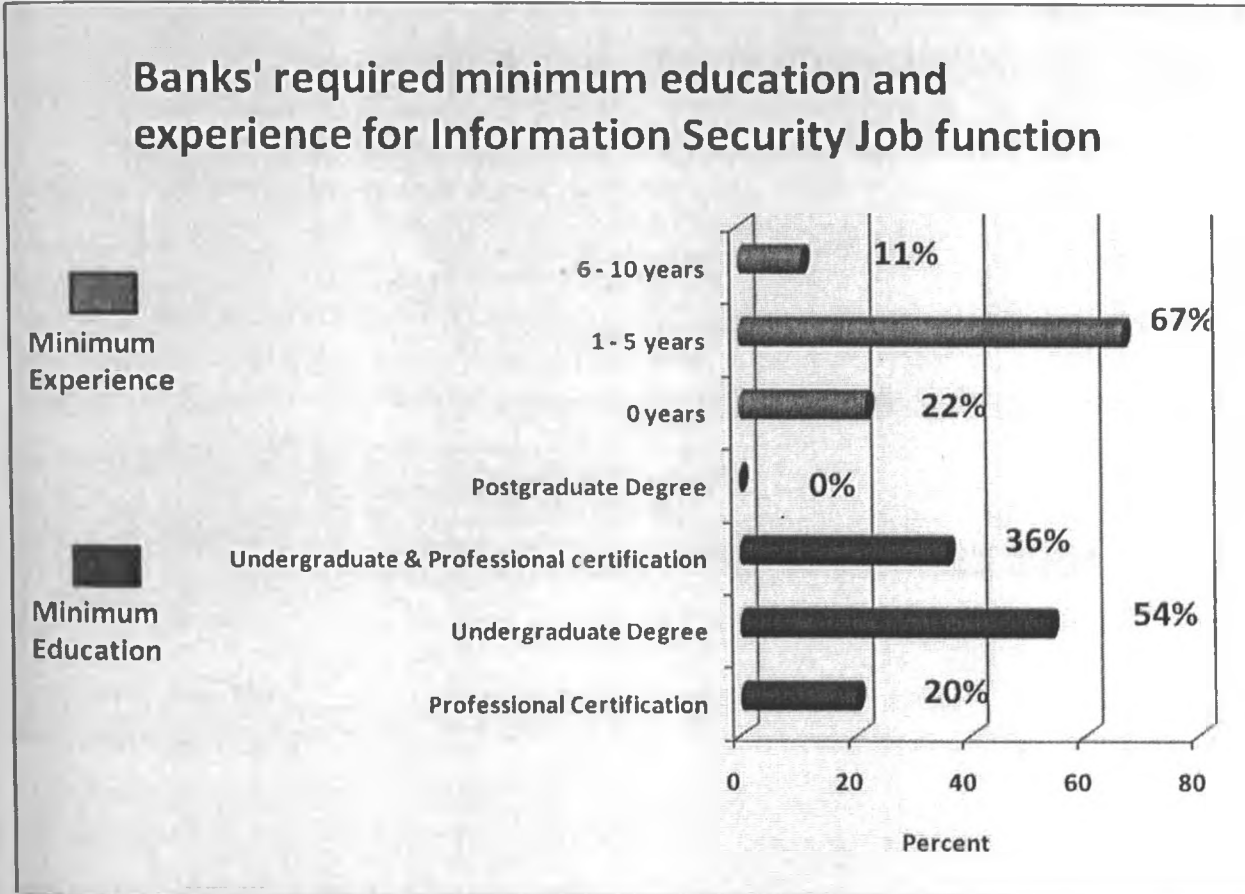
Source: Research Data

This means the importance of having a dedicated information security function is being embraced amongst the banks. However, it seems there still a lot that needs to be done to make the function more independent.

4.4.3 Minimum Qualifications for Information Security Job Function

Banks have minimum education qualifications and experience that they require for the highly specialized information security job function. Respondents indicated the educational requirements and experience that their banks required for the Information Security job function. For minimum education: 5 (20%) banks required a professional certification, 17 (54%) banks required an undergraduate degree and 10 (36%) banks required an undergraduate degree with an additional professional certification. For minimum experience: 7 (22%) banks required no experience, 21 (67%) banks required between 1 – 5 years experience and 4 (11%) banks required between 6 – 10 years experience. The proportions are shown in figure 8.

Figure 8: Banks' required minimum education and experience for Information Security job function



This implies that for the information security job function, most banks are leaning towards requiring an undergraduate degree as a basic minimum and a qualification in information security as an added advantage.

4.4.4 Banks Professional Certifications for Information Security Personnel.

Information security job function requires personnel to have professional certifications. The study revealed that 27 (83%) banks had their chief personnel professionally certified in Information security while 5 (7%) banks did not have their chief personnel professionally certified in information security. The respondents were further asked to reveal professional certifications their chief personnels had. It was indicated that 19 (58%) banks had their chief personnel with a CISA certification, 3 (10%) banks had their chief personnel with a CISSP certification and 10 (32%) banks had their chief personnel with a CISM certification. Figure 9 shows the proportions.

Figure 9: Banks personnels' professional certifications in Information Security



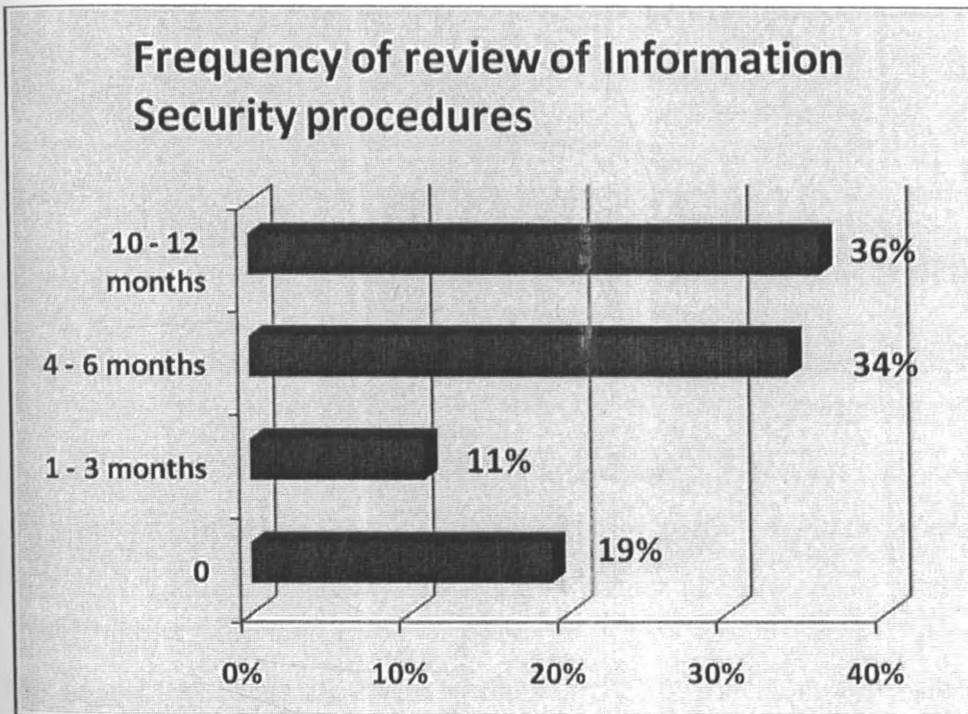
This indicates that CISA and CISM are the most common information security certifications. CISSP is not as common, a fact that can be attributed to it's cost and currently is not offered frequently locally.

4.5 Information Security Procedures

4.5.1 Frequency of Review of Information Security Procedures

The participants were asked how frequent their banks reviewed information security procedures. The outcome indicated that 6 (19%) banks did not review their Information security procedures, 3 (11%) banks reviewed their information security procedures every 1 – 3 months, 11 (34%) banks reviewed their Information security procedures every 4 – 6 months and 12 (36%) banks reviewed their Information security procedures every 10 – 12 months. The proportions are shown in figure 10.

Figure 10: Frequency of review of Information Security procedures

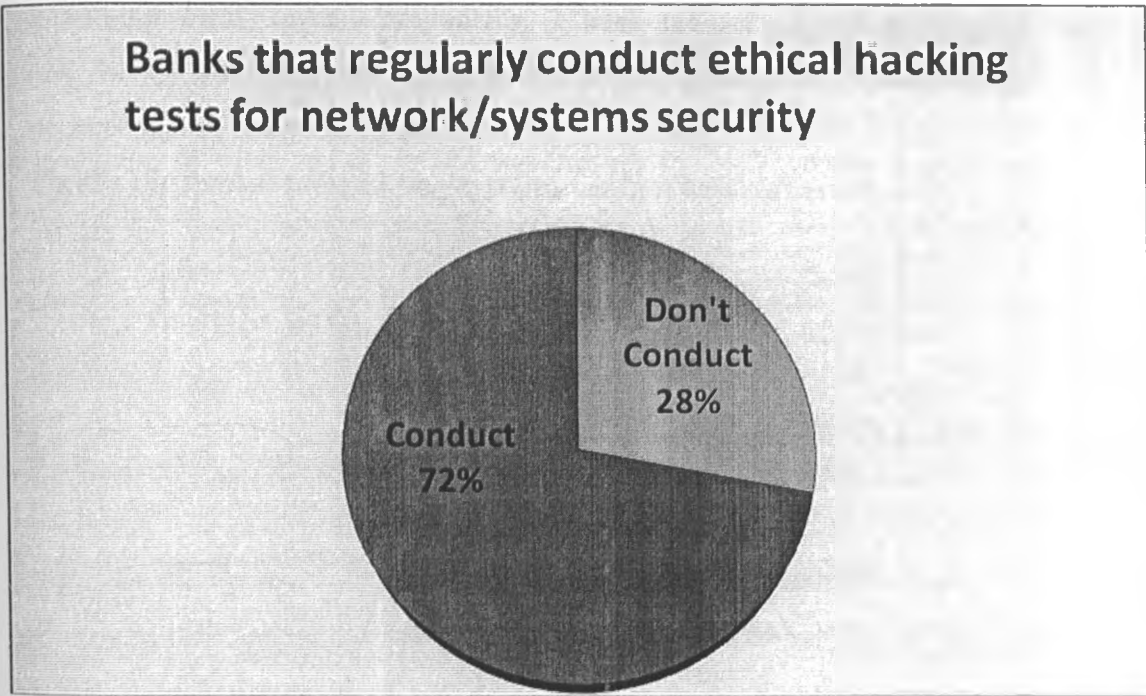


This can be interpreted to mean that banks have appreciated the rapid changes in information security risks hence the frequent review of information security procedures in order to keep up to date.

4.5.2 Ethical Hacking Tests

The respondents were asked whether their banks regularly conducted ethical hacking tests for network and systems security. The analysis indicated that 23 (72%) banks conducted ethical hacking tests for network and systems security and 9 (28%) banks did not conduct ethical hacking tests for network and systems security. Figure 11 shows the proportions.

Figure 11: Banks that regularly conduct ethical hacking tests for network/systems security

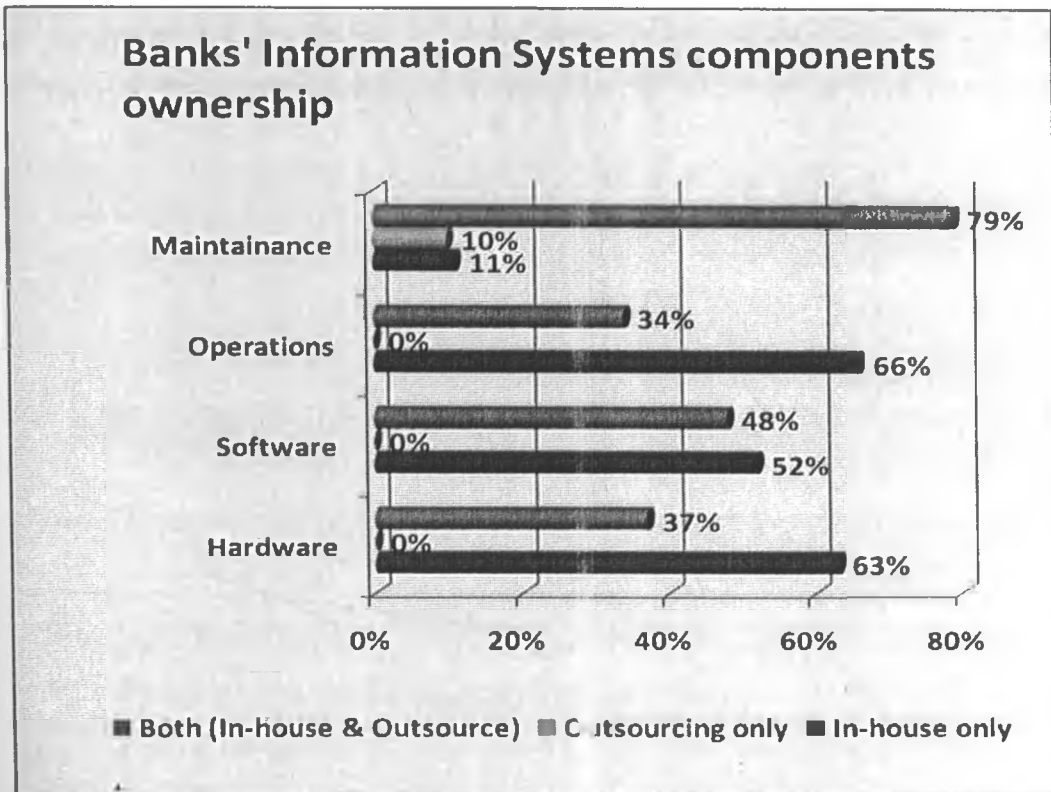


This means that banks are aware of the risk posed by weak security architecture which can result in financial and reputation loss if hackers obtain unauthorized access into the banks systems.

4.6 Information Systems Components Ownership

The study also sought to establish form of ownership of information systems components. The participants indicated that for maintenance components: 4 (11%) banks had in-house only owned components, 3 (10%) banks had out-sourced only owned components and 25 (79%) banks had both in-house and outsourced owned components. For operations processing: 21 (66%) banks had in-house processing, no bank had fully out-sourced processing and 12 (34%) banks had both in-house and some outsourced functions. For software components: 17 (52%) banks had in-house only owned components, no bank had out-sourced only components and 15 (48%) banks had both in-house and outsourced owned components. For hardware components: 20 (63%) banks had in-house only owned components, no bank had out-sourced only owned components and 12 (37%) banks had both in-house and outsourced owned components. The proportions are shown in figure 12.

Figure 12: Banks' information systems components ownership



This shows that most banks have adopted a mix of ownership of components. Some are outsourced and some are insourced. No bank has fully outsourced ownership of their operating components.

4.7 Application of Information Security Practices

The respondents were presented with a list of 67 statements to indicate the extent of their organizations application of information security practices. The participants were instructed to agree/disagree with each of these statements based on a five-point Likert-scale (where 1= Strongly disagree, 2= Disagree, 3= Neutral, 4= Agree and 5= Strongly agree).

A mean score of 0.00 – 1.49 means respondents strongly disagreed, 1.50 – 2.49 means respondents disagree, 2.50 – 3.49 means respondents are neutral/undecided, 3.50 – 4.49 means respondents agree and 4.50 – 5.00 means that respondents strongly agree with statements on their organizations' applications of information security practices. A standard deviation (SD) of > 1 shows significant variability of responses and that of < 1 slight to non-variability of responses.

The researcher categorized the 67 statements into nine broad categories and thereafter analyzed the descriptive statistics of the participants' responses on the following tables.

Table 3: Information Security Risk and Incident Handling

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | Information security risk is assessed periodically | 4.00 | 1.15 |
| 2 | There is a well documented information security policy in place | 3.70 | 1.49 |
| 3 | Systems audit tools are used to monitor information security breaches | 4.10 | 0.72 |
| 4 | The process in place for reporting information security incidents is highly effective | 3.20 | 1.40 |
| 5 | Information security incidents that are reported are effectively followed through to closure | 3.50 | 1.43 |
| 6 | A documented corrective action plan to prevent recurrence of information security incident is always done | 3.20 | 1.32 |
| 7 | There exists a well documented procedure for installing software on computers and servers | 3.20 | 1.14 |
| Category Average Score | | 3.56 | 1.24 |

Under Information security risk and incident handling category, the respondents agreed with three statements. These statements were; "Information security risk is assessed periodically" which had mean score of 4.00 (SD=1.15), "There is a well documented

information security policy in place” which had mean score of 3.70 (SD=1.49), “Systems audit tools are used to monitor information security breaches” which had mean score of 4.10 (SD=0.72) and “Information security incidents that are reported are effectively followed through to closure” which had mean score of 3.50 (SD=1.43). Further, the respondents were undecided on three statements. The statements were; “A documented corrective action plan to prevent recurrence of information security incident is always done” which had mean score of 3.20 (SD=1.32), “There exists a well documented procedure for installing software on computers and servers” which had mean score of 3.20 (SD=1.14) and “The process in place for reporting information security incidents is highly effective” which had mean score of 3.20 (SD) 1.40.

Table 4: Organization of Information Security Function

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | There is an effective information security audit function responsible for information security review and compliance to information security policies | 4.00 | 1.16 |
| 2 | The information security audit function is distinctly independent from the Information Technology department | 3.40 | 1.35 |
| 3 | Senior management is deeply involved in information security initiatives | 3.30 | 1.25 |
| 4 | Employee job descriptions or contracts clearly include accountability of information security | 4.30 | 0.68 |
| Category Average Score | | 3.75 | 1.11 |

In the category for Organization of Information Security function, the respondents agreed with two statements. These statements were; “There is an effective information security audit function responsible for information security review and compliance to information security policies which had mean score of 4.00 (SD 1.16) and “Employee job descriptions or contracts clearly include accountability of information security which had

mean score of 4.30 (SD=0.68). Further, the respondents were undecided on two statements. The statements were; “The information security audit function is distinctly independent from the Information Technology department” which had mean score of 3.40 (SD=1.35) and “Senior management is deeply involved in information security initiatives” which had mean score of 3.30 (SD=1.25).

Table 5: Information Security Training and Information Dissemination

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | Information security policies are routinely communicated to all employees | 3.60 | 1.27 |
| 2 | Employees are trained on information security policies | 3.50 | 1.35 |
| 3 | Employees are fully conversant with the Data Protection Act (legal requirements of retention period of data) | 2.70 | 0.82 |
| 4 | Personnel charged with information security policy implementation continually keep themselves up to date with global trends in information security practices | 4.10 | 0.74 |
| Category Average Score | | 3.48 | 1.05 |

Under Information security training and information dissemination category, the respondents agreed with three statements. These statements were; “Information security policies are routinely communicated to all employees” which had mean score of 3.60 (SD=1.27), “Employees are trained on information security policies” which had mean score of 3.50 (SD=1.35) and “Personnel charged with information security policy implementation continually keep themselves up to date with global trends in information security practices” which had mean score of 4.10 (SD=0.74). Further, the respondents were undecided on one statement. The statement was; ‘Employees are fully conversant with the Data Protection Act (legal requirements of retention period of data)’ which had mean score of 2.70 (SD=0.82).

Table 6: Physical Access Controls

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | All visitors are issued with visitor's identification badges | 4.10 | 0.99 |
| 2 | Staff are issued with identification cards with photos, with no exceptions | 4.50 | 0.53 |
| 3 | Staff and visitor identification cards are clearly distinguishable from each other | 4.30 | 0.95 |
| 4 | Staff and visitor identification cards are laminated or otherwise well designed to prevent easy alteration | 4.30 | 0.95 |
| 5 | There is an enforceable requirement for all staff and visitors to wear their badges at all times | 3.60 | 1.43 |
| 6 | An up to date list of personnel authorized to access various doors or sections of the building is kept | 3.50 | 1.18 |
| 7 | There is an effective process in place to ensure keys and other security access devices are collected immediately upon termination of an employee | 4.20 | 0.92 |
| 8 | Physical access control systems are used for accessing doors | 3.90 | 1.10 |
| 9 | Closed Circuit Television (CCTV) is used to monitor sensitive areas such as Data Center and server rooms | 4.00 | 1.16 |
| 10 | Visual equipments and access control devices are frequently checked to ensure no tampering | 4.00 | 0.82 |
| 11 | An accurate inventory or log is maintained for tracking physical access to premises | 3.70 | 0.68 |
| 12 | There is a well documented process for issuance and return of keys and PIN used for physical access | 3.80 | 0.79 |
| 13 | Employee sign-in procedures during non-scheduled hours is under guard or management supervision | 2.50 | 0.97 |
| Category Average Score | | 3.88 | 0.96 |

In the category for Physical access controls, the respondents strongly agreed one statement. This statement was; “Staff are issued with identification cards with photos, with no exceptions” which had a mean score of 4.50 (SD=0.53). Further, the respondents agreed on eleven statements. The statements were; “All visitors are issued with visitor's identification badges” which had a mean score of 4.10 (SD=0.99), “Staff and visitor identification cards are clearly distinguishable from each other” which had a mean score of 4.30 (SD=0.95), “Staff and visitor identification cards are laminated or otherwise well designed to prevent easy alteration” which had a mean score of 4.30 (SD=0.95), “There is an enforceable requirement for all staff and visitors to wear their badges at all times” which had a mean score of 3.60 (SD=1.43), “An up to date list of personnel authorized to access various doors or sections of the building is kept” which had a mean score of 3.50 (SD=1.18), “There is an effective process in place to ensure keys and other security access devices are collected immediately upon termination of an employee” which had a mean score of 4.20 (SD=0.92), “Physical access control systems are used for accessing doors” which had a mean score of 3.90 (SD= 1.10), “Closed Circuit Television (CCTV) is used to monitor sensitive areas such as Data center and server rooms” which had a mean score of 4.00 (SD=1.16), “Visual equipments and access control devices are frequently checked to ensure no tampering” which had a mean score of 4.00 (SD=0.82), “An accurate inventory or log is maintained for tracking physical access to premises” which had a mean score of 3.70 (SD=0.68) and “There is a well documented process for issuance and return of keys and PIN used for physical access” which had a mean score of 3.80 (SD=0.79). The respondents were undecided on this statement; “Employee sign-in procedures during non-scheduled hours is under guard or management supervision” which had a mean score of 2.50 (SD=0.97).

Table 7: Backup Management

| No | Statement | Mean | SD |
|-------------------------------|--|-------------|-------------|
| 1 | There is a well documented systems backup procedure | 4.00 | 0.82 |
| 2 | The backup procedure document outlines the frequency of each backup | 3.80 | 1.03 |
| 3 | The backup procedure also documents the restore process for each system | 3.40 | 1.08 |
| 4 | The backup procedure is reviewed at least once every 3 months | 3.00 | 1.16 |
| 5 | Data backups are always stored in an offsite location without fail | 4.00 | 0.94 |
| 6 | Records exist to track backup tape movements | 3.60 | 1.27 |
| 7 | Data backup media are always stored in secure fireproof cabinets when not in use | 3.70 | 1.06 |
| 8 | The cabinets where data backups are stored have controlled access | 4.00 | 0.94 |
| 9 | Periodic random tests are undertaken for data backups (test data restores) | 3.90 | 1.20 |
| Category Average Score | | 3.71 | 1.06 |

Under Backup management category, the respondents agreed with seven statements. These statements were; “There is a well documented systems backup procedure” which had a mean score of 4.00 (SD=0.82), “The backup procedure document outlines the frequency of each backup” which had mean score of 3.80 (SD=1.03), “Data backups are always stored in an offsite location without fail” which had mean score of 4.00 (SD=0.94), “Records exist to track backup tape movements” which had mean score of 3.60 (SD=1.27), “Data backup media are always stored in secure fireproof cabinets when not in use” which had mean score of 3.70 (SD=1.06), “The cabinets where data backups are stored have controlled access” which had mean score of 4.00 (SD=0.94) and

“Periodic random tests are undertaken for data backups (test data restores)” which had mean score of 3.90 (SD=1.20). Further, the respondents were undecided on two statements. These statements were; “The backup procedure also documents the restore process for each system” which had a mean score of 3.40 (SD=1.08) and “The backup procedure is reviewed at least once every 3 months” which had a mean score of 3.00 (SD=1.16).

Table 8: Disaster/Contingency Planning

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | Emergency list of phone numbers (management, police, fire department and vendors) are readily available to both staff and guards | 2.90 | 1.10 |
| 2 | There are backup power alternatives such as generators and Uninterruptible Power Supplies (UPS) that can effectively run computer equipment in case of power failures | 4.60 | 0.52 |
| 3 | There is a contingency site that can be used effectively for business continuity in case of a disaster | 4.00 | 0.94 |
| 4 | The business continuity/disaster recovery plan is reviewed at least once semi-annually | 3.10 | 1.29 |
| 5 | There exists a well documented business continuity plan clearly showing various roles and responsibilities should business continuity process be invoked | 3.30 | 1.25 |
| 6 | An effective disaster recovery test is undertaken for the entire business at least semi-annually | 3.20 | 1.03 |
| Category Average Score | | 3.52 | 1.02 |

In the category for Disaster/Contingency planning, the respondents agreed on two statements. These statements were; “There are backup power alternatives such as generators and Uninterruptible Power Supplies (UPS) that can effectively run computer

equipment in case of power failures” which had a mean score of 4.60 (SD=0.52) and “There is a contingency site that can be used effectively for business continuity in case of a disaster” which had a mean score of 4.00 (SD=0.94). Further, the respondents were undecided on four statements. These statements were; “Emergency list of phone numbers (management, police, fire department and vendors) are readily available to both staff and guards” which had a mean score of 2.90 (SD=1.10), “The business continuity/disaster recovery plan is reviewed at least once semi-annually” which had a mean score of 3.10 (SD=1.29), “There exists a well documented business continuity plan clearly showing various rôles and responsibilities should business continuity process be invoked” which had a mean score of 3.30 (SD=1.25) and “An effective disaster recovery test is undertaken for the entire business at least semi-annually” which had a mean score of 3.20 (SD=1.03).

Table 9: Licensing and Antivirus

| No | Statement | Mean | SD |
|-------------------------------|--|-------------|-------------|
| 1 | At least quarterly, a review is undertaken on installed software to ensure compliance with licenses held | 3.50 | 0.85 |
| 2 | Software licenses are stored in a secure controlled location | 3.60 | 0.97 |
| 3 | Elaborate processes and procedures are in place to ensure immediate update and monitor deployment of new anti-virus software updates | 3.70 | 0.82 |
| Category Average Score | | 3.60 | 0.88 |

Under Licensing and antivirus category, the respondents agreed with all the three statements in this category. The statements were; “At least quarterly, a review is undertaken on installed software to ensure compliance with licenses held” which had a mean score of 3.50 (SD=0.85), “Software licenses are stored in a secure controlled location” which had a mean score of 3.60 (SD=0.97) and “Elaborate processes and

procedures are in place to ensure immediate update and monitor deployment of new anti-virus software updates” which had a mean score of 3.70 (SD=0.82)

Table 10: Data Security

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | Internet security measures are in place such as firewalls and data encryption | 4.30 | 0.68 |
| 2 | Electronic data being transferred out of the organization is always encrypted | 3.60 | 1.27 |
| 3 | Computer equipment that leaves the building for maintenance have the hard disks formatted | 3.20 | 1.23 |
| Category Average Score | | 3.70 | 1.06 |

In the category for Data security, the respondents agreed with two statements. These statements were; “Internet security measures are in place such as firewalls and data encryption” which had a mean score of 4.30 (SD=0.68) and “Electronic data being transferred out of the organization is always encrypted” which had a mean score of 3.60 (SD=1.27). Further, the respondents were undecided on one statement. The statement was; “Computer equipment that leaves the building for maintenance have the hard disks formatted” which had a mean score of 3.20 (SD=1.23).

Table 11: Password Management and System/Data Access Control

| No | Statement | Mean | SD |
|-------------------------------|---|-------------|-------------|
| 1 | PINs and profiles are immediately deleted for terminated employees | 4.00 | 1.25 |
| 2 | Employees are required to seek advance management approval to use computer equipment during non scheduled hours | 2.40 | 0.97 |
| 3 | A well documented policy is in place on internet and email usage | 4.00 | 0.47 |
| 4 | Public internet access is strictly restricted to only those individuals who require it for purposes of their jobs | 3.40 | 1.17 |
| 5 | User profiles are reviewed at least quarterly to ensure users have entitlements only to the rights required to undertake their current job functions | 3.30 | 1.49 |
| 6 | Password policy is in place that enforces complex password construction such as mixed characters, alphanumeric and minimum number of characters | 3.60 | 1.27 |
| 7 | Password policy enforces password change at least once every 30 days | 4.10 | 0.57 |
| 8 | Password policy ensures profiles not logged into the system for more than 2 weeks consecutively are automatically deleted or disabled | 3.20 | 1.23 |
| 9 | Clearly documented policy is in place for system access using privileged users such as administrators and backup users | 3.50 | 1.27 |
| 10 | System access using privileged users requires management approval | 3.90 | 0.99 |
| 11 | Passwords for privileged users are held at least under dual control | 4.20 | 0.63 |
| 12 | System access activities undertaken by privileged users are logged by the system with details | 4.00 | 0.94 |
| 13 | System access logs are reviewed at least daily and a report submitted to management | 3.10 | 1.37 |
| 14 | Rights/permissions are always assigned in the most restrictive manner to ensure users can only access resources that they need to access for their job function | 3.30 | 1.34 |
| 15 | All printers used for printing sensitive or confidential material are located in a secure controlled location | 3.20 | 1.23 |
| 16 | There is controlled access to sensitive stationery such as account statement papers and securities papers | 3.40 | 1.17 |
| 17 | Confidential documents are destroyed in a secure manner | 3.60 | 1.08 |
| 18 | Computer printouts are signed for by the people who collect them | 3.30 | 1.06 |
| Category Average Score | | 3.53 | 1.08 |

Under Password management and system or data access control category, the respondents agreed with eight statements. These statements were; "PINs and profiles are immediately deleted for terminated employees" which had a mean score of 4.00 (SD=1.25), "A well documented policy is in place on internet and email usage" which had a mean score of 4.00 (SD=0.47), "Password policy is in place that enforces complex password construction such as mixed characters, alphanumeric and minimum number of characters" which had a mean score of 3.60 (SD=1.27), "Password policy enforces password change at least once every 30 days" which had a mean score of 4.10 (SD=0.57), "Clearly documented policy is in place for system access using privileged users such as administrators and backup users" which had a mean score of 3.50 (SD=1.27), "System access using privileged users requires management approval" which had a mean score of 3.90 (SD=0.99), "Passwords for privileged users are held at least under dual control" which had a mean score of 4.20 (SD=0.63) and "System access activities undertaken by privileged users are logged by the system with details" which had a mean score of 4.00 (SD=0.94).

Further, the respondents were undecided on six statements. These statements were; "Public internet access is strictly restricted to only those individuals who require it for purposes of their jobs" which had a mean score of 3.40 (SD=1.17), "User profiles are reviewed at least quarterly to ensure users have entitlements only to the rights required to undertake their current job functions" which had a mean score of 3.30 (SD=1.49), "Password policy ensures profiles not logged into the system for more than 2 weeks consecutively are automatically deleted or disabled" which had a mean score of 3.20 (SD=1.23), "System access logs are reviewed at least daily and a report submitted to management" which had a mean score of 3.10 (SD=1.37), "Rights/permissions are always assigned in the most restrictive manner to ensure users can only access resources that they need to access for their job function" which had a mean score of 3.30 (SD=1.34); "All printers used for printing sensitive or confidential material are located in a secure controlled location" which had a mean score of 3.20 (SD=1.23) and "There is controlled access to sensitive stationery such as account statement papers and securities papers" which had a mean score of 3.40 (SD=1.17).

The respondents disagreed with statement; “Employees are required to seek advance management approval to use computer equipment during non scheduled hours” which had a mean score of 2.40 (SD=0.97).

4.8 Bank’s characteristics relationships

4.8.1 Relationship between banks’ characteristics and information systems practices adopted

Table 12: Relationship between banks’ characteristics and information systems security job function

| Characteristics of Banks | Information Systems practice | |
|---|--|---|
| | Banks with a dedicated IS security job function | Banks without a dedicated IS security job function |
| 1. Ownership of the Bank | Banks with a dedicated IS security job function | Banks without a dedicated IS security job function |
| Foreign owned | 32% | 25% |
| Commercial bank with government participation | 14% | 0% |
| Wholly locally owned | 21% | 8% |
| 2. Annual turnover | Banks with a dedicated IS security job function | Banks without a dedicated IS security job function |
| Less than 100 | 28% | 8% |
| 100 – 500 | 0% | 0% |
| 501 – 1000 | 0% | 0% |
| 1001-2000 | 11% | 12% |
| Over 2000 | 17% | 24% |
| 3. Banks’ years of operation | Banks with a dedicated IS security job function | Banks without a dedicated IS security job function |
| Less than 10 years | 0% | 19% |
| 10 -20years | 13% | 7% |
| 21 - 30 years | 0% | 0% |
| 31 - 40 years | 42% | 0% |
| 41 - 50 years | 1% | 8% |

The banks were foreign owned, commercial banks with government participation and wholly locally owned. Foreign owned banks; 32% had a dedicated IS security job function and 25% did not have a dedicated IS security job function. Commercial bank with government participation owned banks; 14% had a dedicated IS security job function and none that did not have a dedicated IS security job function. Wholly locally owned banks; 14% had a dedicated IS security job function and banks none that did not have a dedicated IS security job function.

Banks with an annual turnover of less than 100 (million Kshs); 28% had a dedicated IS security job function while 8% did not have a dedicated IS security job function. Banks with an annual turnover of between 100 to 500 (million Kshs) and those ones that had an annual turnover of between 501 to 1000 (million Kshs) did not have a dedicated IS security job function. Banks with an annual turnover of between 1001 to 2000 (million Kshs); 11% had a dedicated IS security job function while 12 % did not have a dedicated IS security job function. Banks with an annual turnover over 2000 (million Kshs); 17% had a dedicated IS security job function while 24% did not have a dedicated IS security job function.

Banks that had been in operation for less than 10 years; none had a dedicated IS security job function while 19% did not have a dedicated IS security job function. Banks that had been in operation for between 10 to 20 years; 13% had a dedicated IS security job function while 7% did not have a dedicated IS security job function. Banks that had been in operation for between 21 to 30 years; none had a dedicated IS security job function. Banks that had been in operation for between 31 to 40 years; 31% had a dedicated IS security job function while none that did not have a dedicated IS security job function. Banks that had been in operation for between 41 to 50 years; 11% had a dedicated IS security job function while 8% did not have a dedicated IS security job function.

4.8.2 Relationship between Banks' Characteristics and Frequency of Review of Information Systems Procedures

Table 13: Relationship between Banks' Characteristics and Information Systems Procedures Review

| Characteristics of Banks | Frequency of review of Information Systems procedures | | | |
|---|---|--------------|--------------|---------------|
| | 0 months | 1 - 3 months | 4 - 6 months | Over 6 months |
| 1. Ownership of the Bank | | | | |
| Foreign owned | 18% | 8% | 11% | 20% |
| Commercial bank with government participation | 0% | 0% | 0% | 7% |
| Wholly locally owned | 8% | 0% | 3% | 0% |
| 2. Annual turnover | | | | |
| Less than 100 | 0% | 0% | 7% | 6% |
| 100 – 500 | 0% | 9% | 0% | 0% |
| 501 – 1000 | 8% | 0% | 0% | 0% |
| 1001-2000 | 21% | 0% | 0% | 7% |
| Over 2000 | 0% | 0% | 27% | 14% |
| 3. Banks' years of operation | | | | |
| Less than 10 years | 9% | 8% | 0% | 0% |
| 10 -20years | 11% | 0% | 7% | 0% |
| 21 - 30 years | 0% | 0% | 6% | 0% |
| 31 - 40 years | 0% | 0% | 13% | 21% |
| 41 - 50 years | 12% | 0% | 0% | 13% |

Foreign owned banks; 18% did not review their IS procedures, 8% reviewed their IS procedures after 1 to 3 months, 11% reviewed their IS procedures after 4 to 6 months and

20% reviewed their IS procedures after over 6 months. Commercial bank with government participation owned banks; all of them reviewed their IS procedures and would do this after 4 to 6 months. Wholly locally owned banks; 8% did not review their IS procedures, none reviewed their IS procedures after 1 to 3 months, 3% reviewed their IS procedures after 4 to 6 months and none reviewed their IS procedures after over 6 months.

Banks with an annual turnover of less than 100 (million Kshs); 7% reviewed there IS procedures after 4 to 6 months and 6% reviewed there IS procedures after over 6 months. Banks with an annual turnover of between 100 to 500 (million Kshs); 9% reviewed there IS procedures after 1 to 3 months. Banks with an annual turnover of between 501 to 1000 (million Kshs); 8% did not review there IS procedures. Banks with an annual turnover of between 1001 to 2000 (million Kshs); 21% did not review there IS procedures and 7% reviewed their IS procedures after over 6 months. Banks with an annual turnover over 2000 (million Kshs); 27% reviewed their IS procedures after 4 to 6 months and 14% reviewed their IS procedures after over 6 months.

Banks that had been in operation for less than 10 years; 9% did not review there IS procedures and 8% reviewed their IS procedures after 1 to 3 months. Banks that had been in operation for between 10 to 20 years; 11% did not review there IS procedures, and 7% reviewed their IS procedures after 4 to 6 months. Banks that had been in operation for between 21 to 30 years; 6% reviewed their IS procedures after 4 to 6 months. Banks that had been in operation for between 31 to 40 years; 13% reviewed their IS procedures after 4 to 6 months and 21% reviewed their IS procedures after over 6 months. Banks that had been in operation for between 41 to 50 years; 12% did not review there IS procedures and 13% reviewed their IS procedures after over 6 months.

CHAPTER FIVE: DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

From the analysis of the data collected, the following discussions, conclusions and recommendations were made.

5.2 Discussion

This study established the information security practices adopted by commercial banks in Kenya. The study was also to establish whether there is a relationship between the characteristics of a bank and the information security practices adopted.

5.2.1 Information Security Practices Adopted By Commercial Banks in Kenya.

The first objective of the study was to establish security practices adopted by commercial banks in Kenya. The results indicated that most banks were having internet banking services as well as ATM services. From the results it was also established that majority of the banks had a committed budget for their IT Departments. However, slightly less than half of the banks represented did not have a dedicated information systems security job function.

In terms of academic qualifications, the study revealed that most of banks had their chief personnel professionally certified in information security practices. Out of this professionally certified personnels it was revealed that most banks had their chief personnels with CISA certifications and very few chief personnels had CISSP certifications.

The outcome indicated that most banks reviewed their Information Security procedures. However, the frequency of review varied with different banks. Most banks reviewed their information security procedures every 10 - 12 months while very few banks reviewed their information security procedures every 1 - 3 months.

It was also established that most banks conducted ethical hacking tests for network and systems security. Only a very small proportion of banks did not conduct ethical hacking tests for network and systems security.

The study revealed that for maintenance components, most banks had both in-house and outsourced owned components. For operations components it was established that most banks had in-house only owned components. For software components, most banks had in-house only owned components. For hardware components, most banks had in-house only owned components.

5.2.2 Relationship between the characteristics of a bank and the information security practices adopted

The study revealed that most of the banks were wholly locally owned. It was further revealed that most of the banks had an annual turnover of Ksh 1,000,001 – 2,000,000. The results also indicated that half of the banks had between 10,001 – 100,000 customers. Therefore in an effort to serve these customers well, the banks need to be networked. The study indicated all the banks that were represented in this survey had their branches networked. The results indicated that majority of the banks had ATM services. Further, it was established that more than half of the banks had internet banking services.

It was clearly confirmed by the participants that information security risk and incident handling assessments are done periodically and corrective actions put in place. Systems audit tools are used to monitor information security breaches.

Most banks were found to have an organized information security function. The outcome indicated that there is an effective information security audit function responsible for information security review and compliance to information security policies. It was also noted that employee job descriptions or contracts clearly include accountability of information security.

The study revealed that Information security training and information dissemination was not effectively undertaken. The study was able to establish that the employees are not fully conversant with the Data Protection Act (legal requirements of retention period of data). However, on a good note, it was the personnel charged with information security policy implementation continually keep themselves up to date with global trends in information security practices on their own initiative.

The study indicated there was adequate utilization of physical access controls. The most commonly adopted was staff being issued with identification cards with photos. Others were laminating staff and visitor identification cards are laminated to prevent easy alteration, an effective process in place to ensure keys and other security access devices are collected immediately upon termination of an employee, Closed Circuit Television (CCTV) to monitor sensitive areas and Visual equipments and access control devices are frequently checked to ensure no tampering.

It was also indicated that there was effective back up management. This was commonly done by having well documented systems backup procedure. Further, data backups were always stored in an offsite location without fail. Moreover, the cabinets where data backups are stored have controlled access and periodic random tests are undertaken for data backups (test data restores).

Most banks had put in place disaster or contingency planning strategies. This was by having backup power alternatives such as generators and Uninterruptible Power Supplies (UPS) that can effectively run computer equipment in case of power failures. Additionally majority of the banks had a contingency site that can be used effectively for business continuity in case of a disaster.

The study indicated that software licensing and antivirus management is effectively carried out. This includes like undertaking a review on installed software to ensure compliance with licenses held. The software licenses are also stored in a secure controlled location. The banks also have elaborate processes and procedures are in put in

place to ensure immediate update and monitor deployment of new anti-virus software updates.

The findings indicated that data security measures are done. This is carried out by Internet security measures being put in place such as firewalls and data encryption. Banks also ensure that electronic data being transferred out of the organization is always encrypted.

It was also revealed that the banks have password management, system and data access control. This included controls such as PINs and profiles being immediately deleted for terminated employees. Additionally a well-documented policy is in place on internet and email usage on passwords, password policy enforces password change at least once every 30 days and passwords for privileged users are held at least under dual control. System access activities undertaken by privileged users are logged by the system with details is also carried out.

5.3 Conclusions

Conclusions that can be drawn from this study is that banks are aware of the importance of robust information security practices but not enough is being done to keep up with the rapid changing threats in the industry. Banks need to constantly review their information security procedures and communicate the same effectively to all staff.

Foreign owned banks appear to be ahead of the rest when it comes to information security practices. This may be attributed to the sharing of information across branches in different countries, or directives from the head office.

5.4 Recommendations

A number of information security practices are adopted by commercial banks in Kenya. Based on the findings of this study the following suggestions are recommended:

1. Banks should strive to hire people with information security certifications to perform this function. This is a critical function that requires people who are committed to the field of study and willing to keep up to date with developments in the industry.
2. The information security function should be made independent from the IT department, preferably with its own budget and reporting lines. This ensures that staff charged with this responsibility totally dedicate their time to this critical function with no interference from another department such as IT.
3. Banks can find a way of sharing the information security practices that they have implemented, in order to assist those that may be lagging behind to improve on their practices.

5.5. Limitations of this study

The study noted that there was unwillingness by respondents to divulge sensitive and private information about their banks on information security practices. The area of study is a sensitive area in a bank function. The respondents therefore felt uneasy to give information that would affect their bank's competence.

5.6 Suggestions for further research

Further research should be undertaken to determine how fast the banks are keeping up with information systems security changes. This is because of the rapid constant change in the IT industry which would require fast adaptation in order to keep ahead of the threats. Also, factors that determine the effectiveness of information security practices can be researched on further. This may explain why there are disparities and may provide ways of improving information security across all commercial banks.

REFERENCES

- Andersen, I.T. (2001), "Security in Europe", *Status Quo, Trends, Perspectives*, Dusseldorf.
- Angell, I.O. (1996), "Economic crime: beyond good and evil", *Journal of Financial Regulation & Compliance*, Vol. 4 No. 1.
- Arnott, S. (2002), "Strategy Paper", *Computing*, Vol. 16, 28 February.
- Barnard, L. and von Solms, R. (1998), "The evaluation and certification of information security against BS 7799", *Information Management & Computer Security*, Vol. 6 No. 2.
- British Standards Institute (BSI) (1999), *Information Security Management BS 7799-1:1999*, BSI, London.
- Department of Trade and Industry (DTI) (2000), *Information Security Breaches Survey 2000*, Technical Report, April, DTI, London.
- Department of Trade and Industry (DTI) (2002), *Information Security Breaches Survey 2002*, Technical Report, April, DTI, London.
- Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11.
- Dinnie, G. (1999), "The Second Annual Global Information Security Survey", *Information Management & Computer Security*, Vol. 7 No. 3.
- Ernst & Young (2001), *Information Security Survey*, Ernst & Young, London.
- Ernst & Young (2004), *Information Security Survey*, Ernst & Young, London.

Ernst & Young (2005), *Information Security Survey*, Ernst & Young, London

Ernst & Young (2008), *Information Security Survey*, Ernst & Young, London.

Furnell, S.M. and Warren, M.J. (1999), "Computer hacking and cyber terrorism: the real threats of the new millennium?", *Computers and Security*, Vol. 18 No. 1.

Gerber, M., von Solms, R. and Overbeek, P. (2001), "Formalizing information security Requirements", *Information Management & Computer Security*, Vol. 9 No. 1.

Heather Fulford and Neil F. Doherty (2003) "The application of information security policies in large UK-based organizations: an exploratory investigation", *Information Management & Computer Security*, Vol. 11 No. 3.

Higgins, H.N. (1999), "Corporate system security: towards an integrated management Approach", *Information Management & Computer Security*, Vol. 7 No. 5.

Hone, K. and Eloff, J.H.P. (2002), "Information security policy what do international security standards say?", *Computers & Security*, Vol. 21 No. 5.

International Standards Organization (ISO) (2000), "Information technology. Code of practice for information security management ISO 17799", ISO, Geneva.

KPMG (2000), *Information Security Survey*, KPMG International, UK.

KPMG (2002), *Information Security Survey*, KPMG International, UK.

KPMG (2006), *Information Security Survey*, KPMG International, UK.

Lock, K.D., Carr, H.H. and Warkentin, M.E. (1992), "Threats to information systems today's reality, yesterday's understanding", *MIS Quarterly*, Vol. 16 No. 2.

Moule, B. and Giavara, L. (1995), "Policies, procedures and standards: an approach for Implementation". *Information Management & Computer Security*, Vol. 3 No. 3.

National Security Telecommunications and Information Systems Security Committee (2000), "National Information Systems Security (Infosec) Glossary, No. 4009

Ogeto, V.M.K (2004), "A Survey of Computer Based Information Systems Security Implemented By Large Manufacturing Companies In Kenya", *Unpublished MBA Thesis. University of Nairobi*

Post, G. and Kagan, A. (2000), "Management trade-offs in anti-virus strategies", *Information & Management*, Vol. 37 No. 1.

Richu, P.G (1989), "Security Considerations for Computer Based Financial Systems In Kenya: The Case of Banks and Financial Institutions", *Unpublished MBA Thesis. University of Nairobi*

Siponen, M. T. (2000), "A conceptual foundation for organizational information security Awareness", *Information Management & Computer Security*, Vol. 8 No. 1.

von Solms, R. (1998), "Information security management (1): why information security is so important", *Information Management & Computer Security*, Vol. 6 No. 5.

Wasilwa, M.O (2003), "A Survey of Computer Security Vulnerability In The Banking Industry In Kenya", *Unpublished MBA Thesis. University of Nairobi*

APPENDIX

5.1 APPENDIX I – CLASSIFICATION OF BANKS IN KENYA

i) FOREIGN OWNED

1. Habib AG Zurich
2. Bank of Africa Ltd.
3. Stanbic Bank Ltd.
4. Bank of India
5. Citibank N.A
6. Bank of Baroda Kenya Ltd.
7. Middle East Bank Kenya Ltd.
8. Standard Chartered Bank Kenya Ltd.
9. Barclays Bank of Kenya Ltd.
10. Dubai Bank Ltd.
11. Gulf African Bank Ltd.
12. First Community Bank Ltd.
13. Ecobank Kenya Ltd.

ii) COMMERCIAL BANKS WITH GOVERNMENT PARTICIPATION

1. Development Bank of Kenya Ltd.
2. Industrial Development Bank Ltd.
3. Consolidated Bank of Kenya Ltd.
4. Kenya Commercial Bank Ltd.

iii) COMMERCIAL BANKS THAT ARE WHOLLY LOCALLY OWNED

1. Investments and Mortgages Bank Ltd.
2. Commercial Bank of Africa Ltd.
3. National Industrial Credit Bank Ltd.
4. Family Bank Ltd.
5. Prime Bank Ltd.
6. Victoria Commercial Bank Ltd.
7. African Banking Corporation Ltd.
8. Chase Bank Ltd.
9. Charterhouse Bank Ltd.

10. City Finance Bank Ltd.
11. Credit Bank Ltd.
12. Equatorial Commercial Bank Ltd.
13. Fina Bank Ltd.
14. Giro Commercial Bank Ltd.
15. Guardian Bank Ltd.
16. Oriental Commercial bank Ltd.
17. Paramount-Universal Bank Ltd.
18. Southern Credit Banking Corporation Ltd.
19. Fidelity Commercial Bank Ltd.
20. Co-operative Bank of Kenya Ltd.
21. K-Rep Bank Ltd.
22. National Bank of Kenya Ltd.
23. Equity Bank Ltd.
24. Trans-National Bank Ltd.
25. Diamond Trust Bank Kenya Ltd.
26. Imperial Bank Ltd.

**UNIVERSITY OF NAIROBI,
SCHOOL OF BUSINESS,
P.O BOX 30197,
NAIROBI.**

Dear Sir/Madam,

**RE: A SURVEY OF INFORMATION SYSTEMS SECURITY
PRACTICES ADOPTED BY COMMERCIAL BANKS IN KENYA**

I am a post-graduate student undertaking a Master of Business Administration (MBA) degree at the University of Nairobi. I am currently carrying out a research study on information security practices adopted by commercial banks in Kenya.

Attached is a questionnaire which I will use to collect the information that I require for the study. The information is purely for academic purposes and will be treated with the strictest confidentiality. A copy of the research project can be made available to you upon request. Your co-operation in this academic exercise will be highly appreciated.

Yours faithfully,

Michael Okoko

**MBA student,
University of Nairobi,
School of Business**

SECTION A

1. Which department do you belong to? _____
2. What is the title of your position? _____
3. a) How long have you been with your organization? _____ years
b) How many years have you been in this department? _____ years
c) How many years have you been in your current position? _____ years
4. From the list below, please choose those that apply to your qualification:
 Diploma
 Undergraduate
 Postgraduate
5. From your qualification(s) above, please indicate whether it is Information Technology related or not:
Diploma Yes No
Undergraduate Yes No
Postgraduate Yes No
6. From the age groups below, please choose where your age lies:
 Below 30
 31-35
 36-40
 41-45
 46-50
 Over 50

SECTION B

1. From the classifications below, tick the one that best describes the ownership of your bank:
 Foreign owned
 Commercial bank with government participation
 Wholly locally owned

2. From the groupings below, tick the one that represents the number of employees in your organization:
 1-30 31-50 51-100 101-200 Over 200

3. From the annual turnover ranges below (millions of Kenya shillings), tick the one that your bank belongs to:
 Less than 100 100 – 500 501-1,000 1,001-2,000 Over 2,000

4. From the groupings below, tick one that describes the number of customers your bank has:
 Less than 1,000 1,001 - 10,000 10,001 - 100,000 100,001 - 1,000,000
 Over 1,000,000

5. How many years has your bank been in operation as a fully fledged bank in Kenya? _____ years

6. How many branches does your bank have in Kenya? _____

7. If your bank has more than 1 branch, are they networked? Yes No

8. Does your bank have branches outside Kenya? Yes No

9. Does your bank offer ATM services? Yes No

10. Does your bank offer internet banking services to customers? Yes No

11. Is your bank listed in the Nairobi Stock Exchange? Yes No

12. Does your bank have a separate budget for IT department? Yes No

13. Does your bank have a dedicated information systems security job function? Yes No

14. How many people are responsible for overseeing that information security policies are implemented?

15. What is the minimum qualification set for one to qualify for information security job function?
 -Education qualification: _____ -Work experience: _____ years

16. (a) Does the person in charge of Information security have professional certification in Information Security? Yes No
 (b) If (a) above is "Yes", which professional qualification do they have? _____

17. Is it a requirement for the information security job function holder to have a professional certification in information security? Yes No

18. How often does your bank review information security procedures? _____ months

19. Does your bank undertake ethical hacking tests to test network/systems security? Yes No

20. Tick against one below, to indicate ownership of your banks information systems components

| IS Component | In-house | Outsourced | Both |
|------------------------|----------|------------|------|
| Hardware | | | |
| Software | | | |
| Operations | | | |
| Maintenance | | | |
| Other (please specify) | | | |

SECTION C

| On a scale of 1 to 5, where 1 represents "Strongly Agree" and 5 represents "Strongly Disagree", please rate the extent to which your organization applies the following information security practices. Select 3 "Does Not Apply" only if the practice does not apply to your organization | 1 Strongly Disagree | 2 Disagree | 3 Neither Agree Nor Disagree | 4 Agree | 5 Strongly Agree |
|---|------------------------------------|-----------------------|---|--------------------|---------------------------------|
| 1. Information security risk is assessed periodically | | | | | |
| 2. There is a well documented information security policy in place | | | | | |
| 3. Information security policies are routinely communicated to all employees | | | | | |
| 4. Employees are trained on information security policies | | | | | |
| 5. There is an effective information security audit function responsible for information security review and compliance to information security policies | | | | | |
| 6. The information security audit function is distinctly independent from the Information Technology department | | | | | |
| 7. Senior management is deeply involved in information security initiatives | | | | | |
| 8. Systems audit tools are used to monitor information security breaches | | | | | |
| 9. The process in place for reporting information security incidents is highly effective | | | | | |
| 10. Information security incidents that are reported are effectively followed through to closure | | | | | |
| 11. A documented corrective action plan to prevent recurrence of information security incident is always done | | | | | |
| 12. Employee job descriptions or contracts clearly include accountability of information security | | | | | |
| 13. All visitors are issued with visitor's identification badges | | | | | |
| 14. Staff are issued with identification cards with photos, with no exceptions | | | | | |
| 15. Staff and visitor identification cards are clearly distinguishable from each other | | | | | |
| 16. Staff and visitor identification cards are laminated or otherwise well designed to prevent easy alteration | | | | | |
| 17. There is an enforceable requirement for all staff and visitors to wear their badges at all times | | | | | |
| 18. An up to date list of personnel authorized to access various doors or sections of the building is kept | | | | | |
| 19. There is an effective process in place to ensure keys and other security access devices are collected immediately upon termination of an employee | | | | | |
| 20. PINs and profiles are immediately deleted for terminated employees | | | | | |
| 21. Physical access control systems are used for accessing doors | | | | | |

| On a scale of 1 to 5, where 1 represents "Strongly Agree" and 5 represents "Strongly Disagree", please rate the extent to which your organization applies the following information security practices. Select 3 "Does Not Apply" only if the practice does not apply to your organization | 1 Strongly Disagree | 2 Disagree | 3 Neither Agree Nor Disagree | 4 Agree | 5 Strongly Agree |
|---|--------------------------------|-----------------------|---|--------------------|-----------------------------|
| 22. Closed Circuit Television (CCTV) is used to monitor sensitive areas such as Data Center and server rooms | | | | | |
| 23. Visual equipments and access control devices are frequently checked to ensure no tampering | | | | | |
| 24. An accurate inventory or log is maintained for tracking physical access to premises | | | | | |
| 25. There is a well documented process for issuance and return of keys and PIN used for physical access | | | | | |
| 26. Employees are required to seek advance management approval to use computer equipment during non scheduled hours | | | | | |
| 27. Employee sign-in procedures during non-scheduled hours is under guard or management supervision | | | | | |
| 28. Emergency list of phone numbers (management, police, fire department and vendors) are readily available to both staff and guards | | | | | |
| 29. There is a well documented systems backup procedure | | | | | |
| 30. The backup procedure document outlines the frequency of each backup | | | | | |
| 31. The backup procedure also documents the restore process for each system | | | | | |
| 32. The backup procedure is reviewed at least once every 3 months | | | | | |
| 33. Data backups are always stored in an offsite location without fail | | | | | |
| 34. Records exist to track backup tape movements | | | | | |
| 35. Data backup media are always stored in secure fireproof cabinets when not in use | | | | | |
| 36. The cabinets where data backups are stored have controlled access | | | | | |
| 37. Periodic random tests are undertaken for data backups (test data restores) | | | | | |
| 38. Employees are fully conversant with the Data Protection Act (legal requirements of retention period of data) | | | | | |
| 39. There are backup power alternatives such as generators and Uninterruptible Power Supplies (UPS) that can effectively run computer equipment incase of power failures | | | | | |
| 40. There is a contingency site that can be used effectively for business continuity incase of a disaster | | | | | |
| 41. The business continuity/disaster recovery plan is reviewed at least once semi-annually | | | | | |

| On a scale of 1 to 5, where 1 represents "Strongly Agree" and 5 represents "Strongly Disagree", please rate the extent to which your organization applies the following information security practices. Select 3 "Does Not Apply" only if the practice does not apply to your organization | 1 Strongly Disagree | 2 Disagree | 3 Neither Agree Nor Disagree | 4 Agree | 5 Strongly Agree |
|---|------------------------------------|-----------------------|---|--------------------|---------------------------------|
| 42. There exists a well documented business continuity plan clearly showing various roles and responsibilities should business continuity process be invoked | | | | | |
| 43. An effective disaster recovery test is undertaken for the entire business at least semi-annually | | | | | |
| 44. There exists a well documented procedure for installing software on computers and servers | | | | | |
| 45. At least quarterly, a review is undertaken on installed software to ensure compliance with licenses held | | | | | |
| 46. Software licenses are stored in a secure controlled location | | | | | |
| 47. Elaborate processes and procedures are in place to ensure immediate update and monitor deployment of new anti-virus software updates | | | | | |
| 48. A well documented policy is in place on internet and email usage | | | | | |
| 49. Internet security measures are in place such as firewalls and data encryption | | | | | |
| 50. Electronic data being transferred out of the organization is always encrypted | | | | | |
| 51. Public internet access is strictly restricted to only those individuals who require it for purposes of their jobs | | | | | |
| 52. User profiles are reviewed at least quarterly to ensure users have entitlements only to the rights required to undertake their current job functions | | | | | |
| 53. Password policy is in place that enforces complex password construction such as mixed characters, alphanumeric and minimum number of characters | | | | | |
| 54. Password policy enforces password change at least once every 30 days | | | | | |
| 55. Password policy ensures profiles not logged into the system for more than 2 weeks consecutively are automatically deleted or disabled | | | | | |
| 56. Clearly documented policy is in place for system access using privileged users such as administrators and backup users | | | | | |
| 57. System access using privileged users requires management approval | | | | | |
| 58. Passwords for privileged users are held at least under dual control | | | | | |
| 59. System access activities undertaken by privileged users are logged by the system with details | | | | | |

| On a scale of 1 to 5, where 1 represents "Strongly Agree" and 5 represents "Strongly Disagree", please rate the extent to which your organization applies the following information security practices. Select 3 "Does Not Apply" only if the practice does not apply to your organization | 1 Strongly Disagree | 2 Disagree | 3 Neither Agree Nor Disagree | 4 Agree | 5 Strongly Agree |
|---|------------------------|---------------|---------------------------------|------------|---------------------|
| 60. System access logs are reviewed at least daily and a report submitted to management | | | | | |
| 61. Rights/permissions are always assigned in the most restrictive manner to ensure users can only access resources that they need to access for their job function | | | | | |
| 62. All printers used for printing sensitive or confidential material are located in a secure controlled location | | | | | |
| 63. There is controlled access to sensitive stationery such as account statement papers and securities papers | | | | | |
| 64. Confidential documents are destroyed in a secure manner | | | | | |
| 65. Computer equipment that leaves the building for maintenance have the hard disks formatted | | | | | |
| 66. Computer printouts are signed for by the people who collect them | | | | | |
| 67. Personnel charged with information security policy implementation continually keep themselves up to date with global trends in information security practices | | | | | |