A VULNERABILITY ASSESSMENT OF INFORMATION SYSTEMS SECURITY AT THE NATIONAL BANK OF KENYA (NBK)

BY

Osiro Caroline

D61/70814/2009

Supervisor

Dr. Kate Litondo

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS IN BUSINESS ADMINISTRATION (MBA), SCHOOL OF BUSINESS

UNIVERSITY OF NAIROBI

November, 2011

DECLARATION

STUDENT

I, the undersigned, declare this proposed project is my original work and that it has not been presented to any other university or institution for academic credit.

Signed ..... Date 10/11/2011

Osiro Caroline

D61/70814/2009

SUPERVISOR

This proposal has been submitted for examination with my approval as a university supervisor

Signed ..... Date 10/11/2011

DR. KATE LITONDO

DEPARTMENT OF MANAGEMENT SCIENCE

DEDICATION

I dedicate this dissertation to my late mum Lucy, who passed on shortly before I could conclude this paper. To my father Bartholomew; brothers George, William, Jim and Mike; sisters Beatrice, Roselyne and Josephine; my colleagues and friends without whom the completion of this work would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

ACKNOWLEDGEMENT

I would like to say thank you to my supervisor Dr. Kate Litondo for her guidance and support; her advice was very valuable in leading me through the often-complex process of drafting and completing this paper. I am very grateful too for her faith in my capacity for completing the master programme.

To all my classmates and lecturers for your commitment and friendship. Without the study sessions and friendship, I would not have completed the process. A sincere appreciation to my family for their prayers and encouragement. To all my colleagues for their understanding and proof-reading of my work, I owe you big.

ABSTRACT

Every environment is susceptible to threats and security systems at NBK are no exceptions. The most common threat is the ease with which virus attack a system. The attack strategies, sophisticated techniques and the opportunities for intruders have increased rapidly as the banking sector embraced the internet. The introduction of internet is believed to have resulted in sudden vulnerability of financial institutions to attacks not only from people physically inside the bank, but from anyone with an internet connection anywhere in the world. Due to this vulnerability, banks now use strong access controls, firewalls, encryptions and other controls as mitigation strategies to protect their most valuable asset-information.

The study conducted aimed at establishing security systems present at NBK as well as assessing how vulnerable these systems are to threats(both internal and external).To address the above objectives, data were collected from NBK ICT division and 10 branches in Nairobi using questionnaires and analyzed using statistical tools. Census was done to ensure data collected was not biased.

The findings showed that effective security measures are in place to safeguard Information systems at National Bank of Kenya. The findings showed that smart cards are widely used in gaining access to almost all sensitive areas within the bank. Properly installed CCTV cameras are also in place to offer all round surveillance within the bank especially at the branches. This indicates that only authorized get access to banks vital resources such as server rooms, strong rooms and ATM lobbies.

The findings revealed that the bank mostly use automated vulnerability assessment tool. This is effective detection systems capable of updating automatically for new threats and scanning periodically based on predefined schedule.

The main challenge in offering effective security to the bank's network may have been attributed to lack of training on system security. This may affect the organization negatively as employees unconsciously delete or tampered with vital files in the system causing system failure. The findings on low security personnel turnover is a good sign as the organization is assured of a more secure and stable network from dedicated expertise.

Some limitations encountered during the undertaking of the study were, first, the nature of this study required sensitive security related information, as a result some of the members in the sample considered it too sensitive and declined to respond to some questions in the questionnaire. Secondly, some of those who responded may not have given the exact security position given the sensitive nature of information. Third, the study only incorporated responses from system administrators, network administrators, database administrators and IT managers. Perhaps richer responses would have been obtained if the study incorporated end-user responses. Finally, the time constraint made it impossible to collect more diverse data from the entire NBK network.

CHAPTER ONE: INTRODUCTION

1.1 Background

The banking industry has undergone a very significant change in the way it conducts its business. Some banks have fully embraced new ways, while others are still thinking about it; however there is a growing awareness of online banking among different players within the industry. According to Nelson (2005), services that banks offer are determined by technology and that banks must adopt new technology to be competitive. The adoption of technologies however dictates the adoption of other new technologies to safeguard the bank from the increased risk due to technology. Technical advancement in banks led to the introduction of new management methods and financial instruments, which have opened up new markets in the industry. There has been intense competition, growing customer satisfaction, and the need to improve profit to cover increasing cost and inflation, factors which gradually bring a wide spread appreciation of the need for strategies (Lee and Suh, 1998).

Musa (2004) contends that banks have embarked on developing new products to lure and retain customers. Today, banks have no choice but satisfy customers' needs. Customers will demand the latest technologies like internet, bill payment, ATMs, mobile banking and unknown future systems (Nelson, 2005).Technology is now seen as a basis of competition and the source of threats and thus countermeasures of such threats. The attack strategies, sophisticated techniques and the opportunities for intruders have increased rapidly as the banking sector embraced the internet. The introduction of internet is believed to have resulted in sudden vulnerability of financial institutions to attacks not only from people physically inside the bank, but from anyone with an internet connection anywhere in the world (Nelson, 2005).Due to this vulnerability, banks now use strong access controls, firewalls, encryptions and other controls as mitigation strategies to protect their most valuable asset-information.

Nelson (2005) argues that system insecurity is associated with organizations connected via Local Area Networks (LANs) to the outside world while others just come up due to poor policy implementation. In effort to meet customer needs of adopting new technologies, organizations are becoming more vulnerable to attacks not only from the people from within but also from outsiders connected to the internet.

To perform vulnerability assessment, organizations need to first understand possible threats and vulnerabilities of the system. The process involves identifying assets in order of priority, identify possible vulnerabilities and threats, and develop security policies and procedures to mitigate against threats. However just investing money without overall strategy to deal with the problem can be both costly and ineffective. Thus, a system vulnerability assessment process that provides organization a cost effective and reliable means for assessing and protecting against possible threats is needed.

1.1.1 Information System Security

Security has proved to be a major challenge in virtually every business environment. System security is viewed in terms of minimizing risks arising as a result of inconsistencies and incoherent behavior with respect to information handling activities of an organization. According to Dhillon (1995), inconsistencies in behavior can lead to occurrences of adverse events ranging from monetary loss to complete disruption of business. With the constant growth in e-commerce, public internet and computer networks, security has been enhanced to safeguard against damaging attacks. Hackers, virus, revengeful employees and even human error all present danger to organizational operation. Maximum system security requires physical, computer, information and operational security. Vulnerability often emerges when one or more of the aforementioned security types are omitted. Physical security is concerned with preventing damage to physical system or theft. The goal of securing the perimeter is to prevent malicious or unauthorized users and application from accessing the company resources and various business functions that they support (Nathtigal, 2009). Organizations reduce such risks by locking their server rooms, installing alarm systems and CCTV cameras.

Firewalls are a fundamental component of any perimeter defense. It is a combination of hardware and software that protects the company's network and computers from possible intrusion by hackers from external network. Canavan (2000) argued that any organization should never connect a company's network or system to an external network such as internet, without a firewall unless it does not care whether those systems or network is attacked. Thus, the essence of an effective firewall is for it to act as a passage through which all incoming and outgoing traffic pass. Firewalls should also be immune to compromise and only allow authorized traffic for it to be effective to the organization.

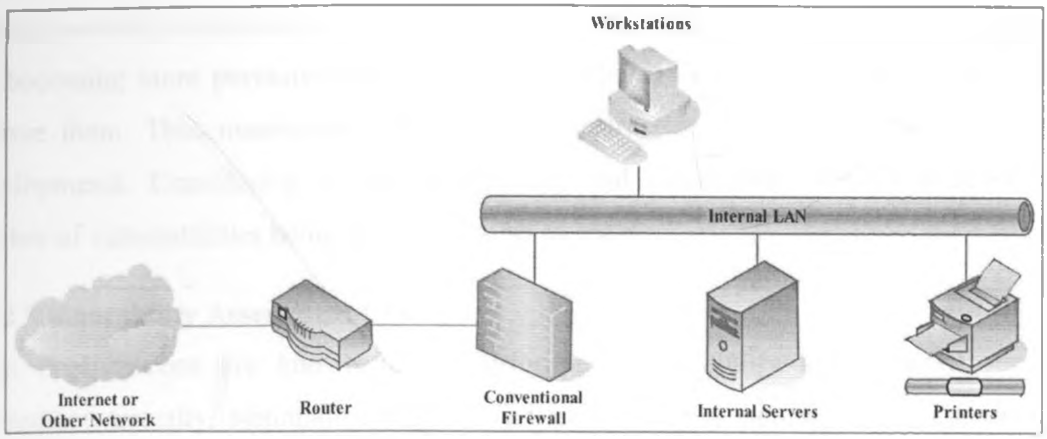


Fig 1. Illustration of firewall concept **Source**: Canavan (2000)

Security infrastructure implemented should always allow sufficient protection without denying users a quick access to the information. Antivirus packages provide protection against virus threats provided it is regularly updated. More and more new viruses generated every month should be minimized by continually updating virus database (Canavan, 2000). Security policies also forms a basis through with system security are guaranteed. The policy that is implemented normally controls who have access to which areas of the network and how unauthorized users are prevented from getting into restricted areas. The policy documents departmental responsibility where an individual is not allowed to have sole accessibility of all sensitive areas such as ATM room in case of banking industry. The display of badge is also documented so as to allow physical entry only to authorized persons.

Routers control the flow of data packets on a network and determine the best way to reach appropriate destination. Their major purpose include: routing of network traffic based on predetermined rules, segmenting frames to transmit between LANs and providing ability to block or deny unauthorized traffic. This mitigates risks of external attackers bombarding traffic thus lowering operations in the organization. Another security system worth discussing is intrusion detection system (IDS) which provides around-the-clock network surveillance. An IDS analyses packet data streams within a network, searching for unauthorized activities, such as attacks by hackers and enabling users to respond to security breach before systems are compromised. When unauthorized activity is detected, the IDS can send an alarm to management console with details of the activity.

The inevitable increasing use of the internet and accommodation of access to user owned devices (laptops, cell phones, etc) from remote and unknown locations create security risks

that can severely disrupt ability of the Bank to function normally. In particular, virus attacks are becoming more pervasive and sophisticated requiring rapid responses to contain and remove them. Thus maintenance of a stable infrastructure is now as important as new developments. Considering network complexity and connectivity always increase, the number of vulnerabilities being discovered also increase.

1.1.2 Vulnerability Assessment Concept

Most organizations are known to be performing vulnerability and network security assessment annually, biannually or quarterly thereby leaving their network vulnerable to intrusion. Vulnerability is defined as inherent weakness in design, configuration, or implementation of systems or network that renders it susceptible to a threat. The growth in number of vulnerabilities and exploits associated with new technology push organizations in conducting a more frequent vulnerability assessment (Rathaus, 2009). According to Bharat (2005), vulnerability assessment is a systematic examination of a system to identify components that may be at risk of attacks and to determine appropriate procedures that can be implemented to reduce such risks. Vulnerability assessment whether manual or automated is a key component of security strategy and recognized as crucial part of network security.

1.1.3 National Bank of Kenya

National Bank of Kenya Limited, herein after referred to as the bank, is one of the largest banks in Kenya. The bank was incorporated on 19th June 1968 and officially opened on Thursday January 14th 1969.The bank was Kenya's first indigenous commercial banks, having an initial authorized share capital of Ksh.20m.The objective for which it was formed was to help indigenous Kenyans to access credit and control their own economy after independence.

The bank has its head office at National Bank House situated at Harambee Avenue in Nairobi. The bank has 47 outlets spread across the country in form of full-time branches and agencies. Currently it has its head office and 10 full branches and an agency located in Nairobi. The rest of the outlets are situated in other major towns in the republic of Kenya totaling to 37 branches in number. In 1985, the National bank revolutionized customer service counters in Kenya by pioneering the introduction of online computerized services making the bank a leader in fast and efficient service delivery. However, this competitive edge was lost due to complacency and lack of investment in the upgrading of its systems.

The bank is a major player in Kenya's banking industry, continuing to give financial services to all sectors of the economy. The bank continues to cover the financial landscape and responding positively to the needs of the customers, shareholders and the economy at large. The bank provides a wide range of services through its head office and network of branches. Besides offering traditional financial services and products, the bank has taken a leading role in the stock market playing multiple roles as an arranger, underwriter and a placing agent. The bank is an appointed fiscal agent, registrar and maker in the secondary market. The bank's latest product is internet banking (NBKOnline) services.

The online banking has had challenges ranging from denial of services and impersonation where money has been transferred fraudulently leaving the bank with huge debts to settle. The bank is pioneered ATM services in Kenya. The technology was embraced positively by customers who bored of queuing in the banking hall to deposit or withdraw cash. However, this new technology did not come without its challenges. Malicious attackers came up with techniques where details of ATM card were copied as the cardholder inserts it to do transactions. Another common vulnerability associated with ATMs is hijacking where cardholders hijacked are forced to withdraw funds from their accounts. The attackers would then use such detail to replicate the card and PIN to withdraw the money. The bank has also documented policies aimed at addressing security requirements of the bank. Such requirements include backups and disaster recovery site to ensure continuity of business operation in event of disaster.

(Source: National Bank of Kenya Financial Reports 2005, 2006, 2007, 2008, 2009 & 2010 and National Bank of Kenya Strategic plans 2009-2011)

1.2 Research Problem

Most organizations have realized that security breach can have a negative influence on business process continuity, public image, cause financial loss or create problems with legal authorities in case of non-compliance. Computer systems especially their protection mechanism must resist intrusion. However, most or perhaps all current systems have security holes which make them vulnerable (Lindskog, 2000).Thus, system owners/organizations often make effort to at least know how secure their systems are. Vulnerabilities will probably always exist in most computer systems. At least with today's software, techniques and tools, it seems to be impossible to completely eliminate flaws (Lindskog, 2000).

Along with the continually increasing number of incidences and the rapid increase of known vulnerabilities, the speed at which systems are attacked is also accelerating. Identifying vulnerabilities and addressing them in a timely manner is crucial in ensuring a secure environment and saves money in the long run. Moore's law states that "as processing power doubles every 18 months, system capabilities also increase". Subsequently, Moore's law implies that new threats will continue to emerge and become easier to accomplish. Connecting systems via Local Area Networks (LANs) to the Internet opens their personnel to a wealth of knowledge of unprecedented magnitude but also exposes organizations to attacks from within and outside organization. Nearly all data loss events resulting from both outside and inside attacks consist of known but unhandled vulnerability (Rathaus, 2009). Protecting computer systems and other devices attached to networks is therefore critical in maintaining positive control over these devices and the data they processed. While various ways have been used to protect and detect system vulnerability, it is not clear if these security systems are assessed for vulnerability against both insider and external threats. Wasilwa (2003) found out that majority of threats facing Information System security was organization's own employees. However, his study did not focus on external threats as a factor towards system vulnerability in the banking industry. Thus, a study on vulnerability assessment of security systems considering both internal and external threats is needed. In view of this, two questions arise:

1. What security systems does the bank has in place?

2. How vulnerable are the systems?

1.3 Research objectives

The general objective of this study is to assess the vulnerability of the security systems at the National Bank of Kenya specifically:

a) To establish security system at the National Bank of Kenya.

b) To determine vulnerability of the systems.

1.4 Value of the study

Considering network complexity and connectivity always increase, the number of vulnerabilities being discovered also increase. This paper will produce a detailed report touching on known system vulnerabilities, new vulnerabilities discovered and possible remedies or solutions to minimize system vulnerability.

This knowledge will be used by organizations, system and network administrators towards effective security system implementation. Researchers may also benefit as they may research further considering the research gap especially on issues related to future unknown weaknesses.

CHAPTER TWO: LITERATURE REVIEW

2.1 Network Security

The need for network security is a relatively new requirement. Prior to 1980s most computers were not networked (Canavans, 2000).When Local Area Networks (LANs) were later deployed, they were relatively secure considering that they were physically isolated. Then came Wide Area Networks (WANs) which were interconnected thereby introducing system vulnerabilities over the shared network. In this networked environment, focus was on providing ease of access and connectivity .Little emphasis was made on security of the system. This resulted in most systems being vulnerable to threats which did not exist previously. Today security is more important compared to ease of access as will be discussed throughout this paper.

Canavans (2000) categorized network security in the bases of protection, detection and response which forms the foundation of security procedures and policies any organization develops and deploy. He argues that security can only be achieved when controls or measures are implemented so as to prevent vulnerability exploitation. Canavans (2000) argue that it is easier, more efficient and cost-effective to prevent security breach than to detect and prevent it. Even though there is no security tool that will prevent all vulnerabilities from being exploited, organizations ought to put in place strong preventive measures to discourage malicious attackers. Systems are believed to be prone to failure and as such, in event of failure in preventive measure, procedures are put in place to detect potential problems .For instance in a situation where unauthorized user accesses restricted sites or files, network administrator is notified on time either through an alarm or alert in the computer system. Response to a security breach often determines system reliability. Organizations often develop strategy that identifies necessary response to security breach. The time it takes any system to resume its normal operations is determined by how effective the response scheme is (Canavans, 2000).The only challenge organizations face is developing security strategy that fits organization's business operations.

2.2 System Vulnerability

Most organizations have realized that security breach can have a negative influence on business process continuity, public image, cause financial loss or create problems with legal authorities in case of non-compliance. Anderson (2001) contends that most security failures are due to incompetence employees, lax security procedures or insider fraud rather than

malicious attacks. Problems associated with people originate from either dishonest or disgruntled employees who lack security awareness programs. They also initiate external problems through accidental or intentional use of affected storage devices such as flash disk which spread virus to the system.

Computer systems especially their protection mechanism must resist intrusion. However, most or perhaps all current systems have security holes which make them vulnerable (Lindskog, 2000).Thus, system owners/organizations often make effort to at least know how secure their systems are. Vulnerabilities will probably always exist in most computer systems. At least with today's software, techniques and tools, it seems to be impossible to completely eliminate flaws (Lindskog, 2000). According to Rathaus (2009), the typical perimeter defense that inspect traffic such as antivirus, firewalls and Intrusion detection Systems (IDS) are now commonplace and malicious attackers and revengeful employees assumes their presence and continuously find ways to bypass them. He also argues that nearly all data loss events resulting from malicious attackers and most losses from insiders consist of exploit of known vulnerabilities which are already documented and solutions found. He found out that nearly all reported exploits were accomplished despite the presence of security expertise, current antivirus, and correctly installed firewalls.

System vulnerabilities according to Rathaus (2009) results either from poor system design, poor implementation or poor management. Hardware and software systems may be created with a security flaws. Possible flaws in design of hardware or software can also render systems vulnerable to attacks. For example, systems with anonymous logins create a weakness where any unauthorized user can easily access organization systems. Poor implementation results from incorrect system configuration. This vulnerability is caused by inexperience network or system administrators who for instance fail to put restricted access privileges to critical files thereby allowing alteration or deletion of these files .On the other hand, poor management due to inadequate policies and procedures render systems vulnerable. The need to document and monitor security controls is thus vital. Even the more basic and routine task such as system backup must be documented and verified .Sensitive areas such as ATM room in banking sector need to practice dual custody as a check in avoiding possible loop holes.

There are many ways in which system vulnerability can be manifested. Canavan (2000) first rule in creating a secure environment is to physically safeguard systems and network. Systems such as servers, routers and backup tapes for instance are to be stored under lock

and key locations where only authorized access is allowed. Apart from securing these systems, organization should also consider their safety in event of natural disasters such as fire, flood and earthquakes. For instance, organizations located in flood prone areas such as Budalangi should not put their computer rooms in basement so as to evade a possible disaster. Storage media are found to be vulnerable since they can be stolen, get lost or corrupted. This exposes organizations at risk considering the sensitive information they contain thereby creating room for such information getting into the hands of competitors who often use them against the organizations affected.

In an effort to increase their effectiveness, organizations often improve on communication. This though does not come without its challenges. A major concern has been about messages and files being intercepted. E-mails are normally intercepted, read and modified or even viruses attached to them. This makes organizations vulnerable .Hackers today use network 'sniffers' to read traffic as it passes the network(Canavan, 2000).According to Tanenbaum (2001), common e-mail lack in-built process to ensure that the sender of the message is who he or she claims to be. To mitigate against such flaws, organizations employ encryption technology, which allows user to store and send files in an encrypted format. The receiver then uses a unique password to decrypt the file, thus denying unauthorized access to the system.

Human vulnerabilities also pose serious threat to organizations. For instance, employees due to ignorance, carelessness, greed or anger may fail to adhere to the laid down policies on security. Users often share or write down passwords thereby creating flaws which when utilized can drastically affect an organization. Employees also affect network through use of flash disks which spread virus across the network. Outside attackers may physically break into a system rendering it vulnerable.

2.2.1 Insider Threats

Trusted employees pose a major threat to information systems. Despite advances in prevention, detection, and response techniques, the number of malicious insider incidents and their associated costs have yet to decline(King,2006).Until recently, organizations allocated most of their network and computer security budgets to securing network perimeters from outside attacks (Schultz, 2002). The majority of their resources were focused on protection against outside attacks leaving information systems vulnerable to threats originating from within. The employees who are trusted and seen as typical users may compromise critical company data by simply copying e-mail or deleting a file from the

server. Cole (2006), found out that users simply use their authorized access logons but with intention of doing harm to the organization.

One major difficulty is that insider can perform malicious actions much easier than outside attackers. Insider threats are more difficult to defend against due to their authorized access to the system, knowledge of processes and security practices, and physical access to the system. According to King(2006), systems security personnel can fairly easily detect outside attackers attempting to break into an organization's information system; however, it is far more challenging to distinguish whether a trusted employee who opens, modifies, copy's, or deletes a file is doing so in the performance of their duties or for malicious purposes.

While the ratio of malicious actions due to insider attacks compared to outsider attacks varies between studies, researchers however agree that malicious attacks have become a great threat to information systems and their associated adverse impacts can no longer be ignored (Anderson, 2004). In fact Richardson, (2005) believes that the number of successful insider attacks is much higher than research indicates because many organizations do not report them due to various reasons. The most common reasons why most attacks are not reported are shown in fig 1.1 below.

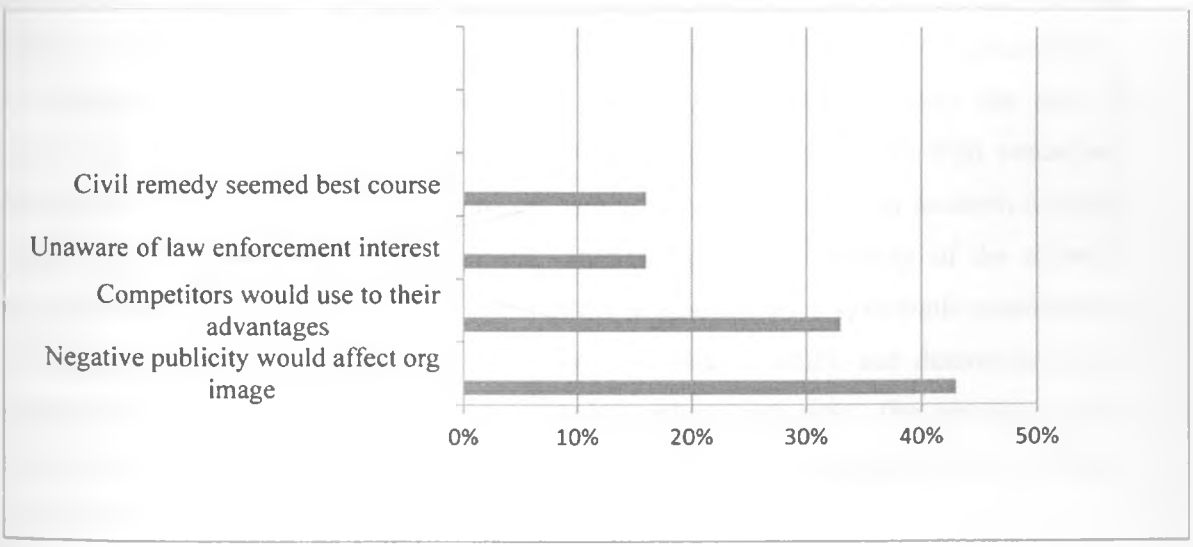


Fig 2: Non reporting trends (639 respondents) **Source**: Computer security Institute, Jan 2006

2.2.2 Outsider Threats

King (2006) concluded that systems security personnel can fairly easily detect outside attackers attempting to break into an organization's information system. However, (Schultz, 2002) differs with this findings revealing that most organizations allocate huge budgets to securing network perimeters from outside attacks which prove very difficult to mitigate against. Hackers also use social engineering to gain access to systems. Malicious individuals often effectively convince legitimate users to provide their passwords or PIN numbers which hackers use in accessing the system.

Hackers often attack organization homepages and replaced by a new home page. Sites which have been hacked include Yahoo, by simple putting some funny text on the page. Numerous sites have also been brought down by denial-of-service attacks in which the attacker floods the site with traffic, rendering it unable to respond to legitimate queries. These attacks are so common these days and can cost the attacked sites a lot of dollars in lost business (Anderson, 2001).Intruders always intercept outgoing or incoming packets, modify them and then sending it to the required destination as legitimate data.

2.3 Vulnerability Assessment

Vulnerability assessment entails programs in the form of policies, procedures, tools and services meant to identify and help organizations in mitigating against system vulnerability. In conducting vulnerability assessment, the security personnel undertakes the task of reviewing documents ,configurations, network diagrams and interviews with concerned individuals in the organization. This process is normally followed by an in-depth network based assessment of workstations, servers, devices and overall security of the network infrastructure. Bharat (2005) defines vulnerability assessment as a systematic examination of a system to identify components that may be at risk of attack and determination of appropriate procedures that can be implemented to reduce such risks. The process aims at determining whether a network device or application is susceptible to a known vulnerability.

Network infrastructure in business environment is rapidly changing with new servers, services and connections with a constant inflow of laptops and storage media such as flash disks and tapes. The growth in number of vulnerabilities and exploits associated with new technology push organizations in conducting a more frequent vulnerability assessment (Rathaus, 2009). Vulnerability assessment whether manual or automated is a key component of security strategy and recognized as crucial part of network security. The

process is designed to explore whether an attack which bypasses a perimeter defense will cause a threat to the network that could affect the confidentiality, availability and integrity of the information. The challenge of staying up to date as Rathaus puts it should be assigned to a solution capable of generating automatic updates and periodic system scan for new threats.

According to Rathaus (2009), vulnerability assessment is performed to determine the actual security posture of a network environment. He argues that the typical perimeter defense that inspects traffic such as antivirus, firewalls and IDS are now common place and even average intruders can exploit them. To compensate, network security administrators especially in the banking industry with valuable assets are now adopting automated vulnerability assessment tools. The industry still faces threats mainly because of lack of current, broad and deep technical expertise with dedicated attention to ensure network scan is complete. The shortage of qualified personnel is compounded by the fact that security is very dynamic. For instance, a vulnerability tool that was previously used to successfully test a network may now be obsolete due to newly discovered vulnerabilities (Rathaus, 2009). Another challenge is lack of vulnerability assessment tools which are expensive to many organizations. Maintaining appropriate level of competency in vulnerability assessment would require multidisciplinary team well knowledgeable in both hardware and software combination in the organization. However, retaining security team to continuously assess security in an organization is difficult and that is why so many organizations in the past used consultants which prove very expensive. This poses another challenge considering that very few organizations can afford to maintain necessary resources to effectively perform vulnerability assessment tasks.

To perform vulnerability assessment, organizations need to first understand possible threats and vulnerabilities of the system. The process involves identifying assets in order of priority, identifying possible vulnerabilities and threats, and developing security policies and procedures to mitigate against threats. However just investing money without overall strategy to deal with the problem can be both costly and ineffective. Thus, a system vulnerability assessment process that provides organization a cost effective and reliable means for assessing and protecting against possible threats is needed.

Vulnerability assessment tools according to Bharat (2005) are used to scan every target within the network. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain access, create denial-of-service or gain

sensitive information about the network. The data is then used to infer vulnerabilities. The analysis and reporting modules categorize results in ways allowing network administrators to view them. Suggestions to correct detected vulnerabilities are also provided. This tool may also attempt to fix vulnerabilities by downloading patches depending on user configuration.

Most organizations are known to be performing vulnerability and network security assessment annually, biannually or quarterly thereby leaving their network vulnerable to intrusion. Rathaus (2009) concluded that this challenge can be minimized by installing automated vulnerability detection systems capable of updating automatically for new threats and scanning periodically based on predefined schedule. The automated vulnerability assessment security scans corporate LANS and WANs from within the organization and internet from outside world and allows tracking, reporting and resolving all vulnerabilities across the entire network and multiple sites. This satisfies the overall aim of vulnerability assessment of determining vulnerabilities of machines monitored by security systems (firewalls, antivirus, IDS) and using the information to mitigate against such risks.

The success of any organization depends on security of its network. Many preventive controls such as user authentication, tight access controls or firewalls are employed by organizations to protect itself from intrusion. However the preventive controls do not provide complete security because of their incapability to detect attacks from disgruntled employees and network attacks which exploit vulnerability in application programs. Thus, IDS comes into play as a second line of defense (Bharat, 2005).The purpose of IDS is to detect illegal and improper use of system resources by unauthorized persons by monitoring network traffic. The technique employed by IDS is categorized as either signature-based detection or anomaly-based detection.

The signature-based detection examines ongoing traffic, activities, transactions or system behavior and tries to find a match with these known patterns of predefined attacks. The strength of the system lies in their signature database .Banks which use this approach are often vulnerable to intrusion considering that in many instances the databases are never updated continuously to incorporate information about new attacks(Bharat, 2005). Anomaly-based IDS on the other hand constructs a profile that represents normal usage and then uses the current behavior data to detect deviations from this profile to recognize possible attack attempts. However, it is non-trivial to define what constitutes a 'normal' behavior and therefore systems based on this approach often generate false alarms. Bharat

(2005) argues that IDS generates thousands of alerts per day thus it becomes critical to prioritize the alerts so that network administrators can focus on major threats. This is done through vulnerability assessment where information about the system to be protected is maintained so that attacks to which the system is known to be vulnerable are given priority.

Intrusion prevention systems (IPS) are controls used to identify potential threats and respond to them swiftly. Like IDS, an IPS monitors network traffic. However, it also has ability to take immediate action, based on a set of rules specified by the security personnel or network administrator. For instance, IPS might drop a packet that it determines to be malicious and block all further traffic from that Internet Protocol (IP) address. Legitimate traffic meanwhile is forwarded to the recipient with no apparent disruption or delay of services. According to Bharat (2005), IPS can be classified either as Host-based or network-based IPS.A host-based IPS is installed on the system to be protected. It works in co-ordination with operation system to block abnormal applications or user behavior. For example, it may monitor system calls in order to detect attacks and may also disable the user account to protect the system. A host-based IPS requires a tight integration with operation system which implies that future upgrades of operation system might cause problems. A network-based IPS is deployed to monitor a single host or entire network segment. It analyses the incoming network traffic for malicious activities. It may drop the malicious packets, reset the network session or block traffic from a particular host depending on user-specified policies. Banks which take this approach may fail to secure their network considering that such systems often loose legitimate traffic whenever there is an inaccurate detection (Bharat, 2005).

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This section provides methods, tools and sources of research data collection, targeted groups and organization where data will be collected. It further discusses how the data will be processed and tools to be used in data analysis.

3.2 Research design

This is a descriptive survey study aimed at investigating system vulnerability level at the National Bank of Kenya (NBK). According to Donald and Pamela(1998),a descriptive study is concerned with finding the what, where and how of a phenomenon.

3.3 Population

The population consists of all users of information systems at the National Bank which includes; network administrators, ICT Managers, database administrators and system administrators. A census was conducted on which 50 questionnaires will be distributed.

3.4 Data collection

Primary data was collected using a structured questionnaire. The questionnaires will be distributed to network administrators and ICT managers and database administrators in ICT Division as well as System administrators at the 10 Nairobi branches. As in Appendix 1, the questionnaires will be divided into three sections where section A handles background information, Section B has Security measures while Section C touches on Vulnerability assessment.

3.5 Data analysis

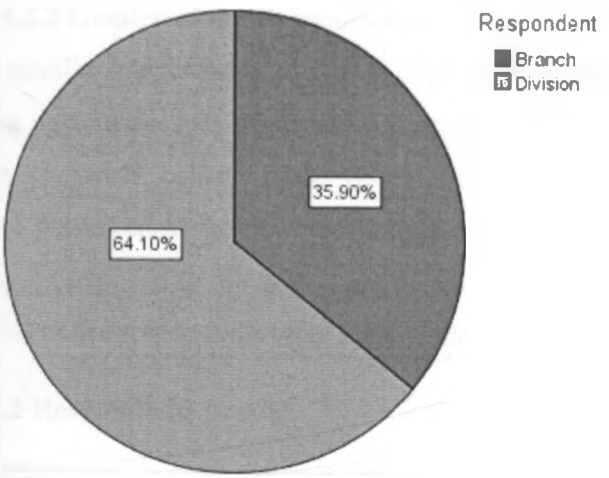
The cumulative data was analyzed using quantitative analysis. Measures of central tendency such as mean, mode and percentages were used. Pie charts, tables and graphs were used to present the results. All data from Appendix 1 was analyzed using SPSS. Mean average was then reached and conclusion made.

CHAPTER FOUR: DATA ANALYSIS, RESULT AND DISCUSSION

4.1 Introduction

The main focus of this chapter was to critically analyze, interpret and present the results of the research study. Data obtained was analyzed to determine the vulnerability of Information systems security at National Bank of Kenya. Descriptive statistics such as frequencies and percentages were used to analyze responses to various items in the questionnaire. The target population for the study was 50 respondents, and the researcher administered 50 questionnaires for the field study. The research census resulted in a response rate of 78% where 39 out of 50 respondents in the target population responded to the questionnaires administered to them. The respondents were drawn both from ICT Division and Nairobi branches.

Fig 4.1 Distribution of respondents according to location



4.2 Demographic Information of the Respondents

To form the basis under which the research can rightly judge the responses, it was important for the study to establish their background information. In addition, the study employed census approach in research that sought to investigate the study variables without manipulating or tampering with them in an attempt to determine how vulnerable security information systems are at NBK. These effects are embedded in the general background of the respondent.

4.2.1 Age group of the Respondents

Age of respondent has turned out to be an important aspect especially where technology is concerned. This was guided by the fact that relatively younger people are perceived to

embrace new technology than older generation even though they may be exposed to the same kind of environment. According to the findings majority 16(41%) of the respondents were between 26-30 years of age while users above 36 years were substantial figure of 14(35.9%).This may be attributed to the experience they have acquired of the years in the field of information systems security.

Table 4.1 Respondents age group

Age group	Frequency	Percent
20-25	1	2.6
26-30	16	41.0
31-35	8	20.5
Above 36	14	35.9
Total	39	100.0

4.2.2 Gender of the Respondents

Gender equality has turned out to be an important consideration in almost all spheres of life, including system security in organizations. As a result it was necessary for the study to establish the gender balance in the system security arena. This was guided by the logic that males are perceived to be more technology-oriented than female counterparts even though they may be exposed to the same kind of environment. According to the findings majority 27(69.2%) of the respondents were male while a mere 12(30.8%) were female.

Table 4.2 Respondents gender

Gender	Frequency	Percent
Female	12	30.8
Male	27	69.2
Total	39	100.0

4.2.3 Respondents Level of Education

Education is/has always been considered the most important factor in understanding and implementing security policy ideas. The level of education was therefore an important aspect of the study given the dynamic nature of security with respect to information systems. As a result, it was important for the study to find out the level of education attained

by each respondent. It emerged that majority 18(46.2%) of the respondents were graduates while a substantial number of respondents 13(33.3%) were postgraduates.

Table 4.3 Respondents level of education

Educational level	Frequency	Percent
Diploma	8	20.5
Graduate	18	46.2
Postgraduate	13	33.3
Total	39	100.0

4.2.4 Respondents position in the organization

Position of a user has been considered vital especially where security policy implementation is concerned. The position was important as it also determines the ease with which management will make decisions especially where budget on IS security is concerned. It emerged that majority 27(69.2%) of the respondents were system administrators while 4(10.3%) were IT managers.

Table 4.4 Respondents position

Position	Frequency	Percent
Db Admin	4	10.3
IT Manager	4	10.3
Network Admin	3	7.7
Sys Admin	27	69.2
Sys Admin & Db Admin	1	2.6
Total	39	100.0

4.3 Security systems and measures in place

Security has proved to be a major challenge in virtually every business environment. One of the major objectives of the study was to establish security systems at the bank in effort to ensure a secure environment. To achieve this, the researcher sought to know from the respondents whether they believed the security systems in place were effective. According

to the findings, a majority 39(100%) of the respondents agreed that there was at least some security measures in the bank.

4.3.1 Physical security systems in place

The goal of securing the perimeter is to prevent malicious or unauthorized users from accessing the company resources and business functions that they support. The researcher having established the presence of security systems in place, the researcher further sought to determine physical security systems at the bank. From the findings it emerged that 17(43.6%) of the respondents agreed that there were smart cards in place to authenticate physical access especially in sensitive areas such as server rooms while 15(38.5%) drawn mainly from branches were of the opinion that CCTV were indeed in place. Only 1(2.6%) acknowledged the presence of biometrics and token as a reinforcement to already established physical security at the bank.

Table 4.5 Physical security in place

Physical security systems	Frequency	Percent
Biometric	1	2.6
CCTV	15	38.5
Smart Card	17	43.6
Smart card& CCTV	3	7.7
Smart cards& Tokens	1	2.6
Smart card, token& CCTV	1	2.6
Token	1	2.6
Total	39	100.0

4.3.2 Alerts while a user accesses restricted sites

Restricted sites often contain sensitive data which when exposed to the competitor affects the organization negatively. Users oblivious to the importance of data may modify or delete them leading to information systems failure. The researcher sought to find out from the respondents some measures which were in place to measure security level in terms of logical access to systems at the bank. It emerged from the findings that 24(61.5%) of the respondents were in agreement that alerts were sent to network administrators every time a

user accesses restricted sites while 15(38.5%) of the respondents were of opinion that users were able to access restricted sites without any alerts to network administrators.

Table 4.6 Alerts while a user accesses restricted sites

Security alerts	Frequency	Percent
No	15	38.5
Yes	24	61.5
Total	39	100.0

4.3.3 Time restrictions in accessing resources

The security procedures in any organization give guidelines on when to access vital systems. This is a check in eliminating fraudulent activities especially in situations where financial transactions are involved like in the banking industry. The researcher found it important to establish the respondent's opinion whether there was time restriction for accessing resources as a measure to enforce system security. It emerged from the findings that 27(69.2%) of the respondents are in agreement that there was time restrictions in accessing resources while 12(30.8%) of the respondents were of the opinion that such control did not exist.

Table 4.7 Time restrictions in accessing resources

Time restrictions	Frequency	Percent
No	12	30.8
Yes	27	69.2
Total	39	100.0

4.3.4 Audit system to monitor user access to the system

Monitoring a user activity enhances systems security especially where a maliciously user accesses information from a resource such as server then denies having access it.The audit trail will show which user accessed the said resource and at what time. The researcher sought to establish from the respondents whether an audit system to keep track of all users accessing the system was in place. A majority 32(82.1%) of the respondents were in agreement whereas a 7(17.9%) believed that such systems did not exist and that there was nothing to keep trail of who accesses which system.

Table 4.8 Audit system to monitor user access to the system

Audit system	Frequency	Percent
No	7	17.9
Yes	32	82.1
Total	39	100.0

4.3.5 Network security systems in place

It is argued that any organization should never connect a company's network or system to an external network for fear of system attack. Network complexity and connectivity increases rapidly and so is the number of vulnerabilities discovered. The researcher found out that 39(100%) of the respondents were in agreement that at least one security system existed to safeguard the bank's network. A majority 15(38.5%) of the respondents acknowledged the presence of all the four network security systems while 6(15.4%) were of the opinion that only firewalls are in place.

Table 4.9 Network security systems in place

Network security systems	Frequency	Percent
Firewalls	6	15.4
Firewall &Antivirus	8	20.5
Firewall,Antivirus &Routers	10	25.6
Firewall,IDS/IPS,Antivirus,Routers	15	38.5
Total	39	100.0

4.3.6 Rating network security systems

Having established the presence of network security systems, the researcher sought to establish the strength of each security system from the respondents. It emerged from the findings that 18(46.2%) of the respondents were in agreement that antivirus were installed properly to safeguard systems. This was followed closely by firewall configuration where 17(43.6%) of respondents agreed that firewalls were configured appropriately to track the incoming and outgoing traffic within the network. The third rating went to security updates in which 16(41%) of the respondents were of the opinion that security updates were downloaded regularly. On the other hand, 16(41%) of the respondents thought the security policy was not very effective in giving security guideline to the users whereas strong passwords scored the least with 12(30.8%) of the respondents in agreement that it was less effective in providing adequate system security.

Table 4.10 (a) Firewall configuration

Firewall configured

Rating	Frequency	Percent
Poor	1	2.6
Fair	2	5.1
Good	17	43.6
Very Good	13	33.3
Excellent	6	15.4
Total	39	100.0

Table 4.10 (b) Antivirus installations

Antivirus installed

Ratings	Frequency	Percent
Poor	1	2.6
Fair	2	5.1
Good	18	46.2
Very Good	16	41.0
Excellent	2	5.1
Total	39	100.0

Table 4.10 (c) Security updates downloaded regularly

Security updates

Ratings	Frequency	Percent
Poor	2	5.1
Fair	7	17.9
Good	16	41.0
Very Good	11	28.2
Excellent	3	7.7
Total	39	100.0

Table 4.10 (d) Security policy implementation

Security policy implemented

Ratings	Frequency	Percent
Poor	4	10.3
Fair	12	30.8
Good	11	28.2
Very Good	10	25.6
Excellent	2	5.1
Total	39	100.0

Strong passwords in place

The choice of a simple password to remember as depicted in table 4.10(e) below may have resulted from lack of training on system security. This is a loophole since such passwords might be easily guessed using password cracking utilities. This is indicated by respondent poor rating on its effectiveness.

Table 4.10 (e) Strong passwords in place

Strong passwords

Ratings	Frequency	Percent
Poor	3	7.7
Fair	16	41.0
Good	9	23.1
Very Good	10	25.6
Excellent	1	2.6
Total	39	100.0

4.3.7 Employee training on system security awareness

Most security failures at the bank are mainly caused by incompetent employees. Security is also believed to be a broad and dynamically changing field, training becomes an vital aspect to be considered. The researcher sought to find out from the respondent whether they underwent frequent training to keep in pace with the constant change. It emerged from the findings that 28(71.8%) of the respondents had not had any training on system security and that their knowledge on security is purely their own effort while only 5(12.8%) of the respondents were in agreement to have had training on annual basis.

Table 4.11 Employee training

Security training	Frequency	Percent
Missing	1	2.6
Monthly	1	2.6
Never	28	71.8
Quarterly	4	10.3
Yearly	5	12.8
Total	39	100.0

4.3.8 Reviewing of security policy

Security policy forms the basis in which any organization implements its strategy in safeguarding its systems. It gives guideline on basic procedures an organization has to follow for a smooth operation. The researcher sought to find out from the respondent the

frequency with which security policy was reviewed. It emerged from the findings that 16(41.0%) agreed that policy review was done after every 2 years while a substantial 8(20.5%) of the respondents believed that policy reviewing was only done after 5 years.

Table 4.12 Reviewing of security policy

Duration in reviewing policy	Frequency	Percent
After 2 yrs	16	41.0
Monthly	2	5.1
More than 5 yrs	8	20.5
Quarterly	5	12.8
Yearly	8	20.5
Total	39	100.0

4.3.9 Extent to which security policy is implemented

Having established the frequency with which security policy is reviewed in the organization, the researcher sought to find out from the respondents their take on its implementation towards ensuring secure environment. It emerged from the findings that 19(48.7%) agreed that policy implementation is relatively good whereas only 4(10.3%) of the respondents were of the opinion that security policy implementation is poor.

Table 4.13 Security policy implementation

Security policy implementation

Rank	Frequency	Percent
Poor	4	10.3
Fair	15	38.5
Good	19	48.7
Very good	1	2.6
Total	39	100.0

4.3.10 Turnover of security personnel

Organizations in the past used consultants which proved to be very expensive since retaining security team to continuously assess security in an organization is difficult. The frequency with which system security personnel leave or enter an organization affects its operation either negatively or positively. It emerged from the findings that 24(61.5%)

agreed that turnover was low whereas only 2(5.1%) of the respondents were of the opinion that security personnel turnover was very high.

Table 4.14 Security personnel turnover

Turnover		Frequency	Percent
Valid		1	2.6
	Low	24	61.5
	Moderate	12	30.8
	Very High	2	5.1
	Total	39	100.0

4.4 Vulnerability assessment

Vulnerability assessment whether manual or automated is a key component of security strategy and recognized as crucial part of network security. One of the main objectives of the study was to determine to what extent information systems are vulnerable to threats. To achieve this, the researcher sought to find out from the respondents whether they believed there are loopholes which make such systems vulnerable. Controls such as storage device safety, disaster discovery sites and time in resuming operations were considered at this point.

4.4.1 Duration before changing password

Passwords determine who get access to the system and thus an important aspect in safeguarding network security. How often passwords are changed eliminate possibility of unauthorized user getting access to confidential data. A majority 20(51.3%) of the respondents were in agreement passwords were changed on a monthly basis whereas only 2(5.1%) believed passwords never expire at all when accessing a system.

Table 4.15 Duration before changing password

Duration of changing passwords		Frequency	Percent
Valid		1	2.6
	Monthly	20	51.3
	Never	2	5.1
	Quarterly	16	41.0
	Total	39	100.0

4.4.2 Attempts before password is locked out of the system

Having established that the passwords indeed expire and are changed monthly, the researcher sought to find out whether there was a control guarding against an authorized user who may want to guess passwords so as to get access. A majority 34(87.2%) of the respondents were in agreement passwords were locked out after the third attempt while only 2(5.1%) believed passwords are never locked out of the system.

Table 4.16 Attempts before password is locked out of the system

Attempts		Frequency	Percent
Valid		2	5.1
	Never	2	5.1
	Second	1	2.6
	Third	34	87.2
	Total	39	100.0

4.4.3 Who unlocks password incase of password lockout

Allocating a responsibility to a particular individual controls a loophole in which any user in effort acquire access to restricted resources would make various attempts and unlocks the password. Who has the authority over passwords was therefore an important aspect of the study given the sensitive nature of passwords in the banking industry systems. It emerged that majority 30(76.9%) of the respondents were in agreement that passwords were only unlocked by system administrators whereas 1(2.6%) of the respondents believe any user could unlock passwords.

Table 4.17 Who unlocks password incase of password lockout

Who unlocks password		Frequency	Percent
Valid		1	2.6
	Any user	1	2.6
	Head of department	6	15.4
	System Admin	30	76.9
	Sys Admin or Head of Dept	1	2.6
	Total	39	100.0

4.4.4 How often storage devices are attacked

Storage devices have been considered vital especially where data or information security is concerned. The safety of such devices especially from viruses attack was important as it ensures important files and documents as well as backup materials are secure. It emerged that majority 25(64.1%) of the respondents were of the opinion that storage devices were rarely attacked while only 9(23.1%) were in disagreement that storage systems were attacked more often.

Table 4.18 How often storage devices are attacked

Storage device attack		Frequency	Percent
Valid		1	2.6
	Never	4	10.3
	Rarely	25	64.1
	Very often	9	23.1
	Total	39	100.0

4.4.5 Extent to which users access restricted sites

The ease with which a user accesses a restricted site renders that particular system vulnerable. Restricted sites are believed to hold sensitive data which when tampered with may paralyze bank's operation. The researcher sought to find out from the respondents whether such sites are out of reach of any unauthorized user. A majority 19(48.7%) of the respondents were in agreement that restricted sites were rarely accessed whereas only 4(10.3%) were of the opinion that users access restricted sites very often.

Table 4.18 Extent to which users access restricted sites

User access	Frequency	Percent
Never	10	25.6
Rarely	19	48.7
Moderate	6	15.4
More often	4	10.3
Total	39	100.0

4.4.6 Average time for resuming operation in event of system failure

The success of any organization depends on its system turnaround time. Any information system will always fail at some point. The time it will take to resume its operation will determine its reliability. It emerged from the findings that a majority 17(43.6%) of the respondents believed it only take 5 hours to resume operation. A substantial 14(35.9%) were in agreement that it only takes an hour for normal operations to resume while 7(17.9%) of the respondents were of the opinion that it takes a day to resume operations in case of system failures.

Table 4.19 Average time for resuming operation in event of system failure

Average time		Frequency	Percent
	1 hour	14	35.9
	5 hours	17	43.6
	1 day	7	17.9
	Total	38	97.4
Missing	System	1	2.6
Total		39	100.0

4.4.7 How often disaster recovery site is tested

Disaster recovery sites are vital to every business environment. It gives a fall back site especially in event of natural disasters and even in case of system failure. The researcher sought to find out from the respondents the frequency with which recovery sites are tested. It emerged from the findings that 19(48.7%) were in agreement that disaster recovery site

was tested annually while 7(17.9%) of the respondents believed that the site was being tested on a monthly basis.

Table 4.20 How often disaster recovery site is tested

Duration		Frequency	Percent
Missing		1	2.6
	Monthly	7	17.9
	Quarterly	7	17.9
	Weekly	5	12.8
	Yearly	19	48.7
	Total	39	100.0

4.4.8 Frequency with which vulnerability assessment is conducted

Vulnerability assessment determines flaws in an information system and thus ways to mitigate against them. The frequency with which such systems are assessed determined how such potential loopholes are avoided before any hindrance to system operation. Most organizations are known to be performing vulnerability and network security assessment annually or biannually thereby leaving their networks vulnerable to intrusion. It emerged from the findings that 14(35.5%) were of the opinion that vulnerability assessment is conducted annually whereas the same margin of 14(35.5%) were in disagreement that vulnerability assessment is not carried at all. Only 4(10.3%) of the respondents were in agreement that assessment is carried out on quarterly basis.

Table 4.21 Frequency with which vulnerability assessment is conducted

Duration	Frequency	Percent
Annually	14	35.9
Monthly	8	20.5
Not at all	14	35.9
Quarterly	3	7.7
Total	39	100.0

4.4.9 Vulnerability assessment tools in place

Network administrators especially in banking industry with valuable assets are now adopting automated vulnerability assessment tool. This is attributed to their capability to update automatically for new threats and scan periodically based on predefined schedule. Having established that vulnerability assessment was carried out to some extent, the researcher sought to find out the kind of tools the organization uses in conducting the assessment. It emerged from the findings that 18(46.2%) were in agreement that the organization uses automated vulnerability assessment tool while a substantial 13(33.3%) of the respondents believed there was no such tool in the organization. Only 1(2.6%) of the respondents was of the opinion that both manual and automated vulnerability tools were in place.

Table 4.22 Vulnerability assessment tools in place

Vulnerability tool	Frequency	Percent
Automated VA	18	46.2
Both	1	2.6
Manual VA	7	17.9
None/Dont know	13	33.3
Total	39	100.0

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATION

5.1. Introduction

The cumulative data was analyzed using quantitative analysis and presented in the form of tables and pie charts. The study sought to determine how vulnerable the systems are at National Bank of Kenya, with specific reference to: What security systems are at place in NBK? How vulnerable are these systems to both internal and external threats? And thus come up with security measures which when properly implemented may reduce such flaws.

5.2 Discussion of Findings

This section discusses the findings of the study in comparison to what other scholars say as noted under literature review. It is broken into: demographic information of the respondents, security measures put in place and anticipated ways of assessing vulnerability of information systems at the bank. The analyzed results are compared against the objectives of the research to assess how far these objectives have been achieved. This evaluation is thus divided into two major parts. First an assessment of outcomes against the objectives is given in Section 5.2, then, recommendation of the research project in Section 5.3, followed by limitations of the study in section 5.4 and suggestions for further studies in section 5.5.

5.2.1 Security measures in place

The study showed that effective security measures are in place to safeguard Information systems at National Bank of Kenya. The findings showed that smart cards are widely used in gaining access to almost all sensitive areas within the bank. Properly installed CCTV cameras are also in place to offer all round surveillance within the bank especially at the branches. This indicates that only authorized get access to banks vital resources such as server rooms, strong rooms and ATM lobbies.

The study also revealed that network administrators do receive alerts every time a user attempts to gain access to restricted sites. Time restrictions on when to access a resource together with audit systems to track users all strengthen security of information systems at the bank. The perimeter defense is enhanced by the presence of firewall, routers, IDS/IPS and antivirus. This means attackers are denied any unauthorized access and only certified traffic are allowed passage.

The study showed that the following IS security measures were highly ranked in NBK. First, the properly installed antivirus, followed by effective firewall then regularly downloaded security updates. The poorly rank systems were strong passwords followed by ineffective policy implementation. The organization seems not to emphasize on training employees on system security. This may affect the organization negatively as employees unconsciously delete or tampered with vital files in the system causing system failure. The findings on low security personnel turnover is a good sign as the organization is assured of a more secure and stable network from dedicated expertise.

5.2.2 Extent to which the information systems are vulnerable to threats

Vulnerability assessment is performed to determine the actual security posture of a network environment .The study showed that the bank conducts vulnerability assessment annually. This is a good sign as threats and new vulnerabilities are mitigated on time before causing havoc to the systems. The expiry of user passwords on monthly basis eliminates loops holes where once unauthorized users who have access to a particular system may fraudulent use it for a long time before it is blocked. The findings on 5hours average turnaround time before resuming operation is a reasonable time. This reduces chances of threats both from employees and customer who may take advantage of such loopholes to fraud the bank. Resuming operation after a long time, say one week reduces credibility of such systems thus loss of business to the organization.

The findings revealed that the bank mostly use automated vulnerability assessment tool. This is effective detection systems capable of updating automatically for new threats and scanning periodically based on predefined schedule.

5.3 Recommendations

The researcher recommends constant training of employees on IS security related issues since the field is dynamic in that a remedy which might have eliminated a particular flaws last year may not work effectively this year.

The researcher also recommends frequent testing of recovery sites. This is a good move considering that recovery sites provide a fall back in events of a natural disaster, theft or system failure.

The frequency with which vulnerability assessment is carried out ought to be improved. Assessing flaws in IS annually creates lapse which may lead to system failure incase urgent

remedy is not put in place. This could expose the organization to various attacks both from internal and external threats.

5.4 Limitations

Some limitations encountered during the undertaking of the study were, first, the nature of this study required sensitive security related information, as a result some of the members in the sample considered it too sensitive and declined to respond to some questions in the questionnaire. Secondly, some of those who responded may not have given the exact security position given the sensitive nature of information. Third, the study only incorporated responses from system administrators, network administrators, database administrators and IT managers. Perhaps richer responses would have been obtained if the study incorporated end-user responses. Finally, the time constraint made it impossible to collect more diverse data from the entire NBK network.

5.5 Recommendations for further study

Vulnerability of IS security has so far been assessed mainly on manufacturing and financial institutions. Particular emphasis has always been on large firms. Interesting findings may be revealed if the research could be conducted on SMEs which have employed IS in their daily operations. Another study could be carried out on parastatals to see how vulnerable such systems are to known threats.

REFERENCE

Anderson (2001). Security Engineering, a guide to Building Dependable Distributed Systems, John Wiley & Sons, Indianapolis.

Anderson (2004). Proceedings of a 2004 workshop: Understanding the insider threats. RAND Corporation, Rockville, MD, March 2004

Anderson R. (2008). Security Engineering, a guide to Building Dependable Distributed Systems, John Wiley & Sons, Indianapolis.

Backhouse, J. (1995). Protecting corporate information assets. Management for fraud prevention; The Dorchester, London, 7th March; The Royal Institute of International Affairs.

Backhouse, J and G. Dhillon (1994). Corporate Computer Crime Management: A research perspective. Tenth IFIP International Symposium on Computer security, IFIP sec 1994, NA

Badenhorst, K and J Ellof (1990). Computer security methodology: risk analysis and project definition. Computers and security.

Bharat J. (2005) Intrusion Prevention and Vulnerability Assessment, Masters in Technology Thesis.

Canavan J. (2000) Fundamentals of network security, Artech House, Inc

Central Bank of Kenya (2006) Annual Report.CBK

CERT Overview Incident & Vulnerability Trends, March 2000

Cole E. (2006) Insider Threats: Protecting the Enterprise from sabotage, Spying and Theft. Syngress Publishing, Rockland, MA, 2006

Common Vulnerabilities and exposures,www.mitre.org/cve/

Dhillon G. (1995) Interpreting the management of information system security, PhD Thesis

King (2006) Development of malicious insider composite vulnerability assessment methodology, MSc thesis.

Lindskog S. (2000) Observations on operating system security vulnerabilities,Thesis for Degree of Lincentiate of Engineering

Musa A. (2004) Responses by commercial Banks to threats operating in Kenya to changes in the environment. A case study of National Bank of Kenya, Unpublished MBA Project.

Nachtigal S. (2009) E- business information system security design paradigm and model.

National Bank of Kenya Information Communication Technology (ICT) Strategy (2009-2011)

National Bank of Kenya Financial Report 2005, 2006, 2007, 2008, 2009 and 2010

Rathaus N. (2009) Vulnerability assessment white paper: Automating Vulnerability Assessment, www.SecuriTeam.com

Richardson R. (2005) 2005 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, March 2003.

Schultz E. (2002) A Framework for understanding and Predicting Insider Attacks. Computer &Security, 21 (6):525-531, October 2002.

Tanenbaum S. (2003) Computer networks, 4th Edition. Published by Pearson Education (India)

Tanenbaum S. (2008) Computer Networks, 4th Edition, Published by Pearson Education & Dorling Kindersley (India).

APPENDIX 1: Questionnaire

SECTION A: Demographic information

1. Name your branch/Division.....

2. What is your age group? (Please tick one)

☐(20-25yrs) ☐(26-30yrs) ☐(31-35yrs)

☐Above 36yrs

3. What is your gender? (Please tick one)

☐Male ☐Female

4. What is your level of education?

☐Diploma ☐Graduate ☐Postgraduate

5. What is your position in the organization?

☐System administrator ☐Network administrator

☐Database Administrator ☐IT Manager

SECTION B: Security measures in place.

1. What physical security is in place? Tick.

Smart cards ☐

Biometrics ☐

Tokens ☐

CCTV ☐

2. Do network administrators receive alerts every time a user access restricted sites?

☐Yes ☐No

3. Is there time restrictions for accessing resources?

☐Yes ☐No

4. Is there audit system to monitor users access to the system?

☐Yes ☐No

5. What security system do you have in place? Please tick.

Firewall ☐

IDS/IPS ☐

Antivirus ☐

Routers ☐

None of the above ☐

6. Rank the following security systems according to their strength in the organization.

Ratings (Please tick)

	Poor	**Fair**	**Good**	**Very Good**	**Excellent**
i.Firewall properly configured.					
ii.Antivirus installed properly.					
iii.Security updates downloaded regularly.					
iv.Security policy implemented.					
v.Strong passwords in place.					

7. How often are the employees trained on security awareness in your organization?

☐Monthly ☐Quarterly ☐Yearly ☐Never

8. How often is security policies reviewed?

- Monthly
- Quarterly
- Yearly
- After 2 yrs
- More than 5 yrs

9. To what extent is documented policy implemented?

	Rank	**(Tick one)**
Poor	1	☐
Fair	2	☐
Good	3	☐
Very good	4	☐
Excellent	5	☐

10. What is the turnover of security personnel in your organization?

- Low
- Moderate
- High
- Very high

SECTION C: Vulnerability assessment

1. How often do you change your passwords?

- Weekly
- Monthly
- Quarterly
- Never

2. After how many attempts does your password locked out of the system?

- First
- Second
- Third
- Fourth
- Fifth
- Never

3. Who unlocks the password in case of password lockout?

System administrator	☐
Auto unlocks itself	☐
Any user	☐
Head of department	☐

4. How often are the storage devices (Backup tapes, Flash disks etc) attacked?

☐Rarely ☐Very often ☐ Never

5. To what extent do users access restricted sites?

	Rank	**(Tick one)**
Never	1	☐
Rarely	2	☐
Moderate	3	☐
More often	4	☐

6. What is the average time for resuming operation in event of system failure?

☐Within 1 hr ☐5 hrs ☐1 day ☐1 week

7. How often is the Disaster Recovery site tested?

Weekly	☐
Monthly	☐
Quarterly	☐
Yearly	☐

8. How frequent do you conduct vulnerability assessment in your organization?

☐Weekly ☐Monthly ☐Quarterly

☐Annually ☐Not at all

9. What kind of vulnerability assessment (VA) tools is used in your organization?

☐Manual VA ☐Automated VA

THANK YOU