SECURITY OF DATA IN MOTION ON A NETWORKED ENVIRONMENT

BY

KWAKU DUAH (B.ED INFORMATION TECHNOLOGY)

A Thesis Submitted to the Department of Computer Science

Kwame Nkrumah University of Science and Technology in Partial Fulfillment of the Requirements for the Degree of

MPHIL INFORMATION TECHNOLOGY

College of Science

JULY 2012

DECLARATION

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

Kwaku Duah PG5093210 ..... 26TH - MARCH - 2014

Student Name and ID Signature Date

Certified by

Dr. Michael Asante 03/04/14

Supervisor's Name Signature Date

Certified by

Dr. J. B. Hayfron-Acquah

Supervisor's Name Signature Date

Certified by

Dr. Michael Asante 03/04/14

Head of Dept. Name Signature Date

ABSTRACT

Data security poses a vital challenge for all organizations. Any breach of security most especially when it occurs in data in motion on a networked environment should not be taken for granted. The general objective of this study was to assess the security strength (strong, weak, breakable, unbreakable etc.) of data in motion, from intrusion perspective, mounting brute force attaches from within the offices premises and outside of office premises.

The study deployed penetration test from the outside of the data network, assess vulnerabilities and threats within the internal network environment using Open Source Security Testing Methodology Manual(OSSTMM) approach, and other standards such as America's National Institute of Standards and Technology (NIST).The standards and the testing methodology specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of an organization's overall business risks. Ultimately, the standards ensure best practice for security controls to protect information assets and data-in-motion.

First, this project showed that the compliance of the standards provides best security for data in motion. The factors and impact of organization security controls for data-in-motion and overall information management system have been analyzed in this study. These factors have brought into practice certain data security measures that are actually not included wholly in many accredited international standards but developed as skill by mostly network systems managers and administrators. In its holistic practice, best security of data-in-motion can be ensured.

ACKNOWLEDGEMENT

Apart from my own efforts, the success of any project depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this project. Dr. Micheal Asante and Dr. Hayfron-Acquah have been the ideal thesis supervisors. Their sage advice, insightful criticisms, and patient encouragement aided the writing of this thesis in innumerable ways.

Special thanks also go to my wife, Diana Adusei Duah and my mum, Mrs. Amoako-Atta Jane and my siblings, Mrs. Jennifer Owusu, Mrs. Naomi Owusu and Mr Amoako-Atta Emmanuel for their good-natured forebearance with my schooling and for their pride in this accomplishment. It was a team effort.

I would also like to show my greatest appreciation to the Head of IT Department of Barclays Bank, Kumasi regional office, Adum and the Managing Director, Laumar Technologies, Accra. I cannot say thank you enough for your tremendous support and help.

I am grateful to all members who contributed to this project for their constant support and help.

DEDICATION

This work is dedicated to my wife, Diana Adusei Duah, without whose caring support, it would not have been possible for me to come this far, and to my son, Sefa Boakye Kingsley.

It is also dedicated to my parents, Mr. and Mrs. Amoako, who taught me that even the largest task can be accomplished if it is done one step at a time.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

1.0 INTRODUCTION

Security is perhaps one of the greatest concerns of the millions of users that routinely exchange data over the Web or store information in computers which may be accessed by unauthorized parties. With the rise of electronic transactions involving sensitive information, such as the transfer of bank data or personal identity information over long distances in an inter-network environment, the need for security of data in motion cannot be over emphasized, knowing that intruders, hackers and crackers are born every day. Therefore the need to ensure safe data transmission, especially in a networked environment, must not be underestimated. Rather, intensive effort to research into more techniques in warding off intrusion and best standard for best practice must be encouraged (Mitchell, 2009).

As information technology has become pervasive, underpinning and supporting almost every aspect of an organization, manipulating and storing the data on which the organization depends for its survival, so the role of IT in corporate governance has become more clearly defined and IT governance is increasingly recognized as a specific area for board and corporate attention. A fundamental aspect of IT governance is the protection of data – and the availability, confidentiality and integrity – on which everything else depends. The worthiness of data is in its ability to be safely transferable, shareable or accessible between sender and receiver (Turnbull, 2003).

Since 1995 when (data) phreaking, cracking and hacking over the internet (or in networked environment) became games of the computer enthusiasts around the world, history has recorded many Information security incidents that had compromised otherwise assumed "secured data". Some of the consequences had been so adverse that victims lost millions of dollars in a day. Personal credit card data (or information) had also been a target for more

than a decade now by computer security invaders. This era gave way to development of serious data security measures by way of regulations and standards compliance, software application enforcements (e.g. proxy, firewall etc.) and hardware level security (Shi et. al., 2012).

Security of data in storage had been the most concern of many security measures more than security of data in motion. Until recently when International organization for standardization and the International Electro technical Commission (IEC) jointly developed a new standard **(ISO/IEC 19772,** *Information technology – Security techniques – Authenticated encryption)* which defines authenticated encryption mechanisms that provide an optimum level of security to protect the confidentiality and integrity of data being transferred or stored (Herzog, 2003).

However, despite enforcement of this standard, wireless crackers continue to turn their assault on data in motion by applying many techniques, testing whether that targeted data still has its original security intact. Hackers and crackers are still devising many means to rip bare the security of data in motion. This project used modern techniques by which hackers' mount dreadful assault successfully to intersect data in motion, in a wireless network environment. It will also evaluate impact of this ISO/IEC 19772 standard compliance.

1.1 RESEARCH FIELD AND SUBJECT OF STUDY

Every institution cannot be secured to the highest level, in spite of the security measures it would put in place. This research is conducted on two Barclays Bank network environments; Adum and KNUST campus branches in the Kumasi metropolis to evaluate security of their data in motion between their branches offering ATM services.

It first investigated which security standard the management had approved and how it is complied with, to ensure well secured data in transmission. It also analyzed the IT infrastructure security policies to ascertain whether there is any agenda for security of data

when in transmission. There was also a look out for intrusion detection measures in place within the network environment. The subject of study was therefore focused on compliance of international security standard (ISO/IEC 19772, or any) and how secure are their data within their network environment (i.e., between the branches in Kumasi metropolis).

1.2 RESEARCH OBJECTIVE

The objective of the research is to assess the security strength (strong, weak, breakable, unbreakable, etc.) of data in motion, from intrusion perspective, mounting brute force attaches from within the offices premises and outside the office premises of Barclays Bank. The main target is to access wireless network infrastructure, intercepting signal and cracking for security ID to be able to access a network resource. Also, Transmission Control Protocol dump trappings were collected to decrypt in an attempt to extract data flowing within the network.

The time taken to break through into the network environment will determine the security strength of the intrusion detection mechanism in place. However, if by using NetBIOS Attack any network node or resources becomes available (perhaps by being enabled for sharing), the security policies of the entire network can easily be rated on lower values, or perhaps without rating at all. The difficulty in succeeding on any attack may depict the strength of security measures in place. It could also be possible that, the security policies may allow intrusion but deny access to any network resources. It is known that many network administrators build their network security in this manner to enable them to access how often attacks are mounted against the network, and even be able to trap sources of intruders (Bace and Mell, 2001).This research also observed this type of culture and assessed the margin of risk involved.

1.3 RESEARCH PROBLEM AND RESEARCH QUESTIONS

It is said that, the only way to stop a hacker is to think like one. It will be difficult though to stop a thief by thinking like a thief. However, a careful implementation of an organization's commitment policy to their customers involves security of the data about the customers. A breach of this security about customers' data would mean multiple loss of confidence in the organization by the customers. To entrust a confidence in an organization such as financial institution begins with a question on how secure is the institutions data network.

In Ghana, for instance, about 90% (or more) of all computer users, use Microsoft Windows operating system. In the United States, on October 27, 2000, CNET News reported that Microsoft computer networked was hacked. The FBI said it has opened an investigation of the break-in to Microsoft's computer network, following the software giant's vow to shore up its internal security. The hackers who broke into the company's computer systems gained access to some of its key programs but did not change them, Microsoft chief executive Steve Ballmer said, according to the report (Festa, 2000).

In the same report, according to *The Wall Street Journal*, hackers with an email address based in St. Petersburg, Russia, had orchestrated the attack in order to steal source code to Microsoft's Windows operating system and Office productivity software suite. Robert Graham, chief technology officer with security software maker Network Ice, explained that the pilfered source code could potentially expose unknown vulnerabilities. He further said; *"Let's say the hacker downloads some, not all, the Microsoft Word source code," he said. "Now let's say he finds some vulnerability no one else knows about. Now he has a secret way to get into Microsoft Word documents. He can now send out Microsoft Word documents that once they're opened would allow him access to everyone's machine"* (Festa, 2000).

The picture is dreadful here, to know that a hacker living far away in Russia can get access to data in other countries such as the United States, because he can exploit the very applications

that created the data. The considerable question is "how secure is the data we generate and transmit in our network environment?" This research study looked at security of data from when it is at rest and when it is in motion, a holistic security solutionpointed out that cryptography is singularly ill-suited to solve the major network security problems of today: denial-of-service attacks, website defacement, theft of credit card numbers, identity theft, viruses and worms, DNS attacks, network penetration, and so on. Most security initiatives are defensive strategies - aimed at protecting the perimeter of the network. But these efforts may ignore a crucial vulnerability - sensitive data stored on networked servers are at risk from attackers who only need to find one way inside the network to access this confidential information. Additionally, perimeter defenses like firewalls cannot protect stored sensitive data from the internal threat - employees with the means to access and exploit this data.

Encryption can provide strong security for data at rest, but developing a database encryption strategy must take many factors into consideration: Where the encryption should be performed, for example - in the database or in the application where the data originates? Who should have access to the encryption keys? How much data must be encrypted to provide security? What's an acceptable trade-off between data security and application performance?(Bouganim and Guo, 2009)

1.3.1 Research Problem

Schneier (2010) has said that legal liability for disclosure is increasing in many countries. For example, in America federal laws have set new standards for the protection of customer information. Regulations required by the Health Insurance Portability and Accountability Act (HIPAA) set standards for the security of medical records and other individually identifiable health information. The Gramm-Leach-Bliley Act (GLBA, Public Law 106-102) sets new requirements on financial institutions regarding the privacy and security of customers' personal financial information. In a recent poll by the Information Technology Association of

America, 75 precent of the Americans surveyed feared having their personal information misused. The problem is very real: over 700,000 cases of identity theft were reported last year according to government and privacy advocacy groups. Worse, in 2001, credit card fraud cost the credit industry billions of dollars. Congress clearly intends to make business liable for the security of customer data and HIPAA and GBLA are just the beginning. HIPAA regulations provide civil and criminal penalties for non-compliance due to willful neglect - fines of up to $50,000 and one year in prison per violation. Congress is also considering the Financial Institution Privacy Protection Act, which would stiffen the Gramm-Leach-Bliley Act to make company officers and directors liable for up to $10,000 for each privacy violation.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure (Mell and Grance, 2011).ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. NIST statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (PL) 107-347, are developing information security standards and guidelines, including minimum requirements for federal information systems.

In Ghana, three regulatory instruments (Act of Parliament) are in force, namely;

1. The Data Protection Bill (discussed by Parliament, yet to be assented to by the President into an Act).
2. The Companies Code 1963 Act 179.

3. The Financial Administration Act 2003, Act 654.

But they do not address guidelines and standards for data security compliance by institutions. There is no independent body credible in Ghana responsible for enforcing data security standards in Institutions. Therefore, one may ask, by what standard do institutions in Ghana ensure data security, either at rest or in motion? This research study therefore reviewed the applicable data security standards comply by institutions in Ghana.

1.3.2 Research Questions

Defense for threat and vulnerability have always been on the agenda of network administrators, where security of data is a major concern. The questions to be asked are as follows:

1. What are the reasons for data breaches?
2. To what extent can companies secure their data?
3. What are the methods or systems appropriate to help companies secure their data?

1.3.3 Information on Research Questions

The following information gives a background on the research questions for this study.

1.3.4 Reasons for data breaches

In order to prevent a data breach, it is essential to understand why they occur. The terms "security breach" and "data breach" have come to signify the failure of controls to maintain the security or privacy of electronic data. Breaches occur for many reasons: hacking, stolen data contained in tapes and computer equipment, lost data contained in tapes and computer equipment, or careless or unthinking disclosure of information. A data breach is the intentional or unintentional release of secure information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill. Incidents range from concerted attack by black hats with the backing of organized

crime or national governments to careless disposal of used computer equipment or data storage media (Thomas, 2011).

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personal identifiable information (PII), trade secrets of corporations or intellectual property (Fletcher, 2012).

According to the nonprofit consumer organization, Privacy Rights Clearinghouse, a total of 227,052,199 individual records containing sensitive personal information were involved in security breaches in the United States between January 2005 and May 2008, excluding incidents where sensitive data was apparently not actually exposed (Privacy Rights Clearinghouse, 1997).

Third-party research into the root causes of data breaches, gathered from the Verizon Business Risk Team and the Open Security Foundation reveal the following sources: well-meaning insiders, targeted attacks, and malicious insiders. In many cases, breaches are caused by a combination of these factors. For example, targeted attacks are often enabled inadvertently by well-meaning insiders who fail to comply with security policies, which can lead to a breach (Baker et. al., 2011).

1.3.4.1 Well-meaning insiders

Company employees who inadvertently violate data security policies continue to represent the largest population of data breaches. According to the Verizon report, 67 percent of breaches in 2008 were aided by "significant errors" on the part of well-meaning insiders. In a 2008 survey of 43 organizations that had experienced a data breach, the Ponemon Institute

found that over 88 percent of all cases involved incidents resulting from insider negligence(Ponemon, 2009).

An analysis of breaches caused by well-meaning insiders yields five main types:

• **Data exposed on servers and desktops.** Daily proliferation of sensitive information on unprotected servers, desktops, and laptops is the natural result of a highly productive workforce. Perhaps the most common type of data breach occurs when well-meaning insiders, unaware of corporate data security policies, store, send, or copy sensitive information unencrypted. In the event a hacker gains access to your network, confidential files stored or used without encryption are vulnerable and can be captured by hackers. As a result of data proliferation, most organizations today have no way of knowing how much sensitive data exists on their systems. Systems that held data the organization did not know was stored on them accounted for 38 percent of all breaches in 2008 - and 67 percent of the records breached (Ponemon, 2009).

• **Lost or stolen laptops.** The 2008 Ponemon Institute study found that lost laptops were the top cause of data breaches, representing 35 percent of organizations polled. In a typical large enterprise, missing laptops are a weekly occurrence. Even when such cases do not result in identity theft, data breach disclosure laws make lost laptops a source of public embarrassment and considerable expense (Ponemon, 2009).

• **Email, Web mail, and removable devices.** Risk assessments performed by Symantec for prospective customers show that on average approximately one in every 400 email messages contains unencrypted confidential data. Such network transmissions create significant risk of data loss. In a typical scenario, an employee sends confidential data to a home email account or copies it to a memory stick or CD/DVD for weekend work. In this scenario, the data is exposed to attack both during transmission and on the potentially unprotected home system or removable media device (Ponemon, 2009).

• **Third-party data loss incidents.** Business relationships with third-party business partners and vendors often require the exchange of confidential information such as 401(k) plan, outsourced payment processing, supply chain order management, and many other types of operational data. When data sharing is overly extensive or when partners fail to enforce data security policies, the risk of data breaches increase. The Verizon report implicated business partners in 32 percent of all data breaches (Ponemon, 2009).

• **Business processes automate the spread of sensitive data.** One reason for proliferation of confidential data is inappropriate or out-of-date business processes automatically distribute such data to unauthorized individuals or unprotected systems, where it can be easily captured by hackers or stolen by malicious insiders. Onsite risk assessments by Symantec find that in nearly half of these cases, outdated or unauthorized business processes are to blame for exposing sensitive data on a routine basis (Ponemon, 2009).

1.3.4.2Targeted attacks

In today's connected world - where data is everywhere and the perimeter can be anywhere - protecting information assets from sophisticated hacking techniques is an extremely tough challenge. Driven by the rising tide of organized cyber-crime, targeted attacks are increasingly aimed at stealing information for the purpose of identity theft. More than 90 percent of records breached in 2008 involved groups identified by law enforcement as organized crime. Such attacks are often automated by using malicious code that can penetrate into an organization undetected and export data to remote hacker sites. In 2008, Symantec created more than 1.6 million new malicious code signatures - more than in the previous 17 years combined - and blocked on average 245 million attempted malicious code attacks worldwide per month (Ponemon, 2009).

Measured by records compromised, by far the most frequent types of hacker attacks in 2008 were unauthorized access using default or shared credentials, improperly constrained access control lists (ACLs), and SQL injection attacks. In addition, 90 percent of lost records were attributed to the deployment of malware.

The first phase of the attack, the initial incursion, is typically perpetrated in one of four ways:

• **System vulnerabilities.** Many times laptops, desktops and servers have do not have the latest security patches deployed which creates a gap in an overall security posture. Gaps or system vulnerabilities can also be created by improper computer or security configurations. Cybercriminals search for and exploit these weaknesses in order to gain access to the corporate network and confidential information(Mell and Grance, 2011).

• **Improper credentials.** Passwords on Internet-facing systems such as email, Web, or FTP servers are often left on factory default settings, which are easily obtained by hackers. Under-constrained or outdated ACLs provide further opportunities for both hackers and malicious insiders (Mell and Grance, 2011).

• **SQL injection.** By analyzing the URL syntax of targeted websites, hackers are able to embed instructions to upload spyware that gives them remote access to the target servers (Mell and Grance, 2011).

• **Targeted malware.** Hackers use spam, email and instant message communications often disguised as known entities to direct users to websites that are compromised with malware. Once a user visits a compromised website, malware can be downloaded with or without the user's knowledge. Gimmicks such as free software deceive users into downloading spyware that can be used to monitor user activity on the web and capture frequently used credentials such as corporate logins and passwords. Remote access tools (RATs) are an example of spyware that is automatically downloaded to a user's machine without their knowledge,

silently providing the hacker control of the user's computer and access to corporate information from a remote location (Mell and Grance, 2011).

Most security teams focus almost exclusively on protecting data by stopping incursions. But incursion is only the first phase of a data breach by targeted attack. To provide complete data protection, all four phases must be addressed.Thefour phases of targeted attacks include incursion, discovery, capture, exfiltration (Dhupar, 2010).

- **Phase 1: Incursion.** Hackers break into the company's network by exploiting system vulnerabilities, using default password violation, SQL injection, or targeted malware.

- **Phase 2: Discovery.** The hacker maps out the organization's systems and automatically scans for confidential data.

- **Phase 3: Capture.** Exposed data stored by well-meaning insiders on unprotected systems is immediately accessed. In addition, components called root kits are surreptitiously installed on targeted systems and network access points to capture confidential data as it flows through the organization.

- **Phase 4: Exfiltration.** Confidential data is sent back to the hacker team either in the clear (by Web mail, for example), wrapped in encrypted packets or zipped files with password protection.

The good news is that a targeted attack on confidential data can be defeated at any one of these four phases. Security professionals who focus only on the incursion phase are making an all-or-nothing bet - a wager that, given the reality of today's wide-open information environment, is likely to fail sooner or later. By taking precautions against the discovery, capture, and exfiltration of data, organizations can significantly bolster their defenses against targeted attacks (Dhupar, 2010).

1.3.4.3 The malicious insider

Malicious insiders constitute drivers for a growing segment of data breaches, and a proportionately greater segment of the cost to business associated with those breaches. The Ponemon study found that data breaches involving negligence cost $199 per record, whereas those caused by malicious acts cost $225 per record.

Breaches caused by insiders with intent to steal information fall into four groups:

- **White collar crime.** The employee who knowingly steals data as part of an identity theft ring has become a highly notarized figure in the current annals of white collar crime. Such operations are perpetrated by company insiders who abuse their privileged access to information for the purpose of personal gain (Dhupar, 2010).

- **Terminated employees.** Given the current economic crisis - in which layoffs are a daily occurrence - data breaches caused by disgruntled former employees have become commonplace. Often, the employee is notified of his or her termination before entitlements such as Active Directory and Exchange access have been turned off, leaving a window of opportunity in which the employee can access confidential data and email it to a private account or copy it to removable media. A recent study of the effects of employee terminations on data security revealed that 59 percent of ex-employees took company data, including customer lists and employee records (Dhupar, 2010).

- **Career building with company data.** It is common for an employee to store company data on a home system in order to build a library of work samples for future career opportunities. While the motives for such actions may not be considered malicious on the order of identity theft, the effect can be just as harmful. If the employee's home system is hacked and the data stolen, the same damage to the company and its customers can ensue (Dhupar, 2010).

• **Industrial espionage.** The final type of malicious insider is the unhappy or underperforming employee who plans to defect to the competition and sends examples of his or her work to a competing company as part of the application and review process. Product details, marketing plans, customer lists, and financial data are all liable to be used in this way (Dhupar, 2010).

Half of businesses have lost sensitive or confidential information due to USB memory sticks, with many incidents involving those infected with malware.In the past two years, 70% of businesses have traced the loss of sensitive or confidential information to USB flash memory sticks. While such losses can obviously occur when the devices get lost or stolen, 55% of those incidents are likely related to malware-infected devices that introduced malicious code onto corporate networks (Schwartz, 2011).

1.3.5 The extent companies can secure their data

The security process is the method an organization uses to implement and achieve its security objectives. The process is designed to identify, measure, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions (Bonnette, 2003).

The process includes five areas that serve as a framework:

•*Information Security Risk Assessment* – This is a process to identify and assess threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes (Bonnette, 2003).

•*Information Security Strategy* – This is a plan to mitigate risk that integrates technology, policies, procedures, and training. The plan should be reviewed and approved by the board of directors (Bonnette, 2003).

•*Security Controls Implementation* - The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-

appropriate controls, and the assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties (Bonnette, 2003).

•*Security Monitoring* - This is the use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These methodologies should verify that significant controls are effective and performing as intended (Bonnette, 2003).

•*Security Process Monitoring and Updating* - This is the process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event (Bonnette, 2003).

1.3.5.1 Governance

Governance is achieved through the management structure, assignment of responsibilities and authority, establishment of policies, standards and procedures, allocation of resources, monitoring, and accountability. Governance is required to ensure that tasks are completed appropriately, that accountability is maintained, and that risk is managed for the entire enterprise (FFIEC, 2006).

1.3.5.2Management Structure

Information security is a significant business risk that demand engagement of the Board of Directors and senior business management. It is the responsibility of everyone who has the opportunity to control or report the institution's data. Information security should be supported throughout the institution, including the board of directors, senior management, information security officers, employees, auditors, service providers, and contractors. Each role has different responsibilities for information security and each individual should be

accountable for his or her actions. Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to bring about appropriate compliance with the institution's policies, standards, and procedures (FFIEC, 2006).

1.3.5.3 Responsibility and Accountability

The board of directors, or an appropriate committee of the board, is responsible for overseeing the development, implementation, and maintenance of the institution's information security program, and making senior management accountable for its actions. Oversight requires the board to provide management with guidance; approve information security plans, policies and programs; and review reports on the effectiveness of the information security program. The board should provide management with its expectations and requirements and hold management accountable for Central oversight and coordination, Assignment of responsibility, Risk assessment and measurement, Monitoring and testing, Reporting, and Acceptable residual risk (FFIEC, 2006).

The board should approve written information security policies and the written report on the effectiveness of the information security program at least annually. A written report to the board should describe the overall status of the information security program. At a minimum, the report should address the results of the risk assessment process; risk management and control decisions; service provider arrangements; results of security monitoring and testing; security breaches or violations and management's responses; and recommendations for changes to the information security program. The annual approval should consider the results of management assessments and reviews, internal and external audit activity related to information security, third-party reviews of the information security program and information security measures, and other internal or external reviews designed to assess the adequacy of information security controls. Senior management's attitude towards security affects the

entire organization's commitment to security. For example, the failure of an institution's president to comply with security policies could undermine the entire organization's commitment to security (FFIEC, 2006).

1.3.5.4 Information Security Risk Assessment

The quality of security controls can significantly influence all categories of risk. Traditionally, examiners and institutions recognized the direct impact on operational/ transaction risk from incidents related to fraud, theft, or accidental damage. Many security weaknesses, however, can directly increase exposure in other risk areas. A strong security program reduces levels of reputation, operational, legal, and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution. Information security risk assessment in its simplest form consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks (Moteff, 2005).

An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities.A risk assessment is a pre-requisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the information security program.Risk assessments for most industries focus only on the risk to the business entity. Telecommunication institutions must also consider the risk to their customers' information. They should protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer (Moteff, 2005).

1.3.5.5 Key Risk Assessment Practices

A risk assessment is the key driver of the information security process. Its effectiveness is directly related to the following key practices:

•*Multidisciplinary and Knowledge Based Approach* - A consensus evaluation of the risks and risk mitigation practices requires the involvement of users with a broad range of expertise and business knowledge. Not all users may have the same opinion of the severity of various attacks, the importance of various controls, and the importance of various data elements and information system components. Management should apply a sufficient level of expertise to the assessment (FFIEC, 2006).

•*Systematic and Central Control* - Defined procedures and central control and coordination help to ensure standardization, consistency, and completeness of risk assessment policies and procedures, as well as coordination in planning and performance. Central control and coordination will also facilitate an organizational view of risks and lessons learned from the risk assessment process (FFIEC, 2006).

•*Integrated Process* - A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide evidence to the risk assessment process that the controls selected and implemented are achieving their intended purpose. Testing can also validate the basis for accepting risks (FFIEC, 2006).

•*Accountable Activities* - The responsibility for performing risk assessments should reside primarily with members of management in the best position to determine the scope of theassessment and the effectiveness of risk reduction techniques.For a mid-sized or large institution, those managers will likely be in the business unit. The information security officer(s) is (are) responsible for overseeing the performance of each risk assessment and the integration of the risk assessments into a cohesive whole. Senior management is accountable

for abiding by the board of directors' guidance for risk acceptance and mitigation decisions (FFIEC, 2006).

•*Documentation* - Documentation of the risk assessment process and procedures assists in ensuring consistency and completeness as well as accountability. This documentation provides a useful starting point for subsequent assessments, potentially reducing the effort required in those assessments. Decisions to mitigate or accept risk should be documented in order to achieve accountability for risk decisions (FFIEC, 2006).

•*Enhanced Knowledge* - Risk assessment increases management's knowledge of the institution's mechanisms for storing, processing, and communicating information, as well as the importance of those mechanisms to the achievement of the institution's objectives. Increased knowledge allows management to respond more rapidly to changes in the environment. Those changes can range from new technologies and threats to regulatory requirements (FFIEC, 2006).

•*Regular Updates* - Risk assessments should be updated as new information affecting information security risks is identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change).At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered (FFIEC, 2006).

1.3.5.6 Information Security Strategy

An information security strategy is a plan to mitigate risks while complying with legal, statutory, contractual, and internally developed requirements (Moteff, 2005). Typical steps to building a strategy include the definition of control objectives, the identification and assessment of approaches to meet the objectives, the selection of controls, the establishment of benchmarks and metrics, and the preparation of implementation and testing plans.

The selection of controls is typically grounded in a cost comparison of different strategic approaches to risk mitigation. The cost comparison typically contrasts the costs of various approaches with the potential gains a financial institution could realize in terms of increased confidentiality, availability, or integrity of systems and data. Those gains could include reduced financial losses, increased customer confidence, positive audit findings, and regulatory compliance. Any particular approach should consider: policies, standards, and procedures; technology design; resource dedication; training; and testing (FFIEC, 2006).

1.3.5.7 Architecture Considerations

Institutions can gain valuable insights into the development of a security architecture and the integration of that architecture into their other technology processes by referencing one or more widely recognized technology standards. Examples of the standards include:

- Control Objectives for Information and Related Technology (COBIT) – provides a broad and deep framework for controls.
- IT Infrastructure Library (ITIL) – provides a list of recognized practices for IT service management.
- ISO 17799 – provides a library of possible controls that can be included in an architecture and guidance in control selection.

Primary considerations in network security architecture are the policies, standards, and procedures employed as a part of the governance structure and the technology design. Other considerations are the necessary resources, personnel training, and testing. Each should be appropriate for the size and complexity of the institution and sufficiently flexible to allow for timely and necessary updates to keep pace with changes in technology and the overall environment (FFIEC, 2006).

1.3.5.8 Policies and Procedures

Policies are the primary embodiment of strategy, guiding decisions made by users, administrators, and managers and informing those individuals of their security responsibilities (FFIEC, 2006). Policies also specify the mechanisms through which responsibilities can be met, and provide guidance in acquiring, configuring, and auditing information systems.

Key actions that contribute to the success of a security policy are:

- Implementing through ordinary means, such as system administration procedures and acceptable-use policies;
- Enforcing policy through security tools and sanctions;
- Delineating the areas of responsibility for users, administrators, and managers;
- Communicating in a clear, understandable manner to all concerned;
- Obtaining employee certification that they have read and understood the policy;
- Providing flexibility to address changes in the environment; and
- Conducting annually a review and approval by the board of directors.

1.3.5.9 Technology Design

Institutions can significantly mitigate the risk of security events by an appropriate technology design that provides for effective network-level monitoring, limits an intruder's ability to traverse the network, offers the minimum level of services required for business needs, and is updated in a timely manner to mitigate newly discovered vulnerabilities.An effective means of accomplishing those goals is through the use of security domains.A security domain is a part of the system with its own policies and control mechanisms.Security domains for a network are typically constructed from routing controls and directories.Domains constructed from routing controls may be bounded by network perimeters with perimeter controls. The perimeters separate what is not trusted from what may be trustworthy (FFIEC, 2006).

The perimeters serve as well-defined transition points between trust areas where policy enforcement and monitoring takes place. An example of such a domain is a demilitarized zone (DMZ), bounded by a perimeter that controls access from outside and inside the institution. Domains constructed from directories may limit access to network resources and applications based on role or function. Directory-driven domains may allow access to different network-driven domains. For example, a network management domain may use the same cabling and network interface cards as other domains, allow access to all computing devices in all domains, but limit the allowed access based on the user's role or function (FFIEC, 2006).

The selection of where to put which control is a function of the risk assessment. Institutions generally should establish defenses that address the network and application layers at external connections, whether from the Internet or service providers. Internally, perimeters can be established at higher-risk security domains, such as wire transfer, and to segregate at a network level those areas of the institution that work with customer information from other areas. Internal perimeters also may be used to create security domains based on geography or other logical or physical separations.Hosts may also include security perimeters. Those perimeters are enforced through authorizations for users and programs. The authorizations can be a part of applications, the file system, and the operating system (FFIEC, 2006).

1.3.5.10 Outsourced Security Services

Security services may be outsourced to obtain greater expertise, a greater range of services, or to decrease cost. The institution retains the same responsibilities for security as if those services were performed in-house should security services be outsourced (FFIEC, 2006).Institutions should ensure they have sufficient expertise to oversee and manage an outsourced security service relationship. The expertise applied to monitor the outsourced security service relationship should be both contract-related, and security-related. The

contract-related oversight addresses contract compliance. The security-related oversight entails understanding the scope and nature of the service sufficiently to identify and appropriately react when the services provided are not at the level indicated in the service level agreement, no longer appropriately coordinate with the security controls at the institution, or no longer provide the risk mitigation desired (FFIEC, 2006).

Institutions should monitor outsourced security service providers appropriate to the level of risk to ensure the service provider fulfills its responsibilities. Monitoring tools include reports from the service provider, independent reviews of the service provider's performance, and independent tests of the service provided (FFIEC, 2006).

1.4 RESEARCH BACKGROUND AND JUSTIFICATION OF THE RESEARCH

This research was based on the assumption that there is adequate security of data in place. However, motivation was on assessment of vulnerability that may give opportunity for exploitation beginning with assessment of internal control measures such as compliance to standards and internal security policies. Further test was directed to wireless network vulnerability.

1.4.1 Research Background

Despite the institution of satisfactory security policies, consistent application, implementation and monitoring are very vital for the maintenance of such a structure. This research will provide importance of consistent maintenance of the security measures in place. This research will start with introduction of the objectives to the head of the IT department of the Barclays Bank branches in Adum and KNUST campus. This will provide room to consider my project as educational rather than as intruder and law breaker. Since it is illegal to perpetuate unauthorized access to a data network, it will be appropriate to introduce this project to the authorities first.

Next, the study will proceed with qualitative method by asking for certification of ISO standard compliance. This will show whether the data security infrastructure is on best practice. The examining of the physical network design follows, to ascertain the security of physical network infrastructure. Exposure of network resources (including wire and wireless devices) beyond close monitoring can also pose security threat and introduce vulnerability. Further work will be focused on wireless distribution system that links the branches together, and disassociates with internet facility of connectivity. One major interesting factor will be the state of firewall in place and intrusion detection measures. This will also be under my scrutiny during my work.

Finally, the project will examine data generation sources and access control security in place, through security configurations and protocols that protect the data in motion within the network environment.

1.4.2 Justification of the Research

Many procedures employed by a firm to sure data-at-rest before transmission are now outdated. Hackers and crackers are borne every day with discovery of vulnerabilities in even the operating systems that run on our data machines all the time. In this age of data transmission and sharing, illicit data swapping, data alteration, malware and data exploits occur all the time without easy detection(Gelbstein and Kamal, 2002). Viruses and worms have now become tools that construct their own virtual circuit networks; hunting for sensitive data and "securely" transmits to remote rogue data exploiting machine (Tomko, Borrett, Kwan and Steffan, 2009). Zeus and Zero-day threats are enough to awaken us about dreaded security of data-in-motion. It is time for reconsideration, security of data-in-motion on end-to-end bases. Thus, to whom, by whom and who receives what. Accordingly, new procedures must be considered and employed (Mockli, 2012).

Forgetfulness and human errors (or mistakes) are common to violation of security policies which might lead to open vulnerability (Kraemer, Carayon and Clem, 2006). This research will show that, consistent assessment of compliance is vital to the well-being of any security for data-in-motion. It will also show that best encryption and cryptography algorithm are not enough to secure data-in-motion. A holistic solution of data security policy and data integrity must move enterprise data security to success end (Brunette, Nagappan, and Weise,2012).

1.5 SUMMARY AND PRESENTATION OF THESIS

This research seeks to find out whether data-in-motion really have security shield from exploits and illegal interception among Ghanaian Institutions. With amount of confidence placed in financial institutions in Ghana, it will be devastating, not only to individuals who hold that confidence, but widely concern if it should come to bear that there was no adequate security of data-in-motion within some institutions in the sector. This work therefore presents a comprehensive research study in the financial institutions industry, taking Barclays Bank branch in Kumasi as case study.

With much information all over the Internet about cyber wars, hackers' break-ins, software application vulnerabilities, data-stealing malware exploits, and data mining fraud; it will be impracticable to assume that Ghana is immune to those exploitations. This research work will deploy penetration test from external network perimeter to verify how much security is with data-in-motion. It will review network data security policies and guidelines in force, data security protection regulation in compliance and finally evaluate integrity of data-in-motion from when the data was at rest.

This research study also considers various technologies in securing data, such as encryption and cryptography techniques. However, it was ironic to perceive that all these knowledge were available yet many financial institutions fall prey to exploitations that cost them

millions of dollars. This study provides premises that holistic approach can lead to achievement of best security of data both at rest and in motion.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

In this chapter, information on the topic was extracted from books, project reports, journals, magazines and articles to review literature on this topic.

2.1 Methods or systems appropriate to help companies secure their data

The security of one's computer and data is crucial for the person and the success of his/her company. Lost or stolen information can reveal company secrets or expose one's confidential or personal information. The more one can do to keep his/her computer secure, the safer one's information will be. Individuals or companies therefore need to come up with appropriate methods or systems to secure their data.

Businesses have a wide range of data security concerns. With the widespread use of electronic data, new security measures have been developed to protect data from uninvited or unwanted intrusion, intentional malice, human error, and physical damage. In larger companies an entire department may be devoted to maintaining data security and establishing policies for employees to follow. In some cases firms may bring in data security consultantsto develop systems and procedures to ensure their data is secure.

General information security management involves taking such steps as announcing and making periodic reminders to the staff about established security policies. Companies may make a registration list of all systems and directories and who has access to them. Data security personnel may work with regular security personnel to ensure that unauthorized personnel are prevented from entering the premises. These procedures help in a general way to prevent data theft or tampering.

Secure communications, the final security measure, means protecting the network or system at the point where it meets the outside world. Techniques to secure communications include leasing private data lines instead of using public lines, using modem management programs to prevent unauthorized dial-ins over the telephone, and encrypting data before sending them over a public network or LAN.

Electronic data must also be made secure from physical as well as human threats. Power failures and surges, hardware failures, and fire and water damage are some of the physical threats against which companies must protect their data. Many companies back up their data on a daily basis and store it off-site to protect it from physical and natural disasters. A disaster recovery plan can help a company prepare for the unthinkable - a natural disaster that destroys all of its data.

The U.S. government is in the process of developing new computer security standards. For many years the existing standards were found in specifications of the U.S. Department of Defense's Orange Book, which was developed essentially for military applications. With the growing use of electronic data in business, industry, and government, a need arose for a commercial computer security standard. The National Institute of Standards and Technology is developing security standards that will address what a secure computer system is supposed to do (functional requirements) as well as how to determine that a system does what it is supposed to (assurance requirements) (Hodell, 1998).

Some of the methods or systems appropriate to help companies secure their data include the following:

- Security Controls Implementation: Access Control
- Access Rights Administration
- Authentication
- Network Access

- Operating System Access
- Application Access
- Physical and Environmental Protection
- Data Center Security
- Physical Security in Distributed IT Environment
- Encryption
- Malicious Code Prevention
- Controls to Protect against Malicious Code
- Data Encryption: Applications and Limits
- Using File Encryption Software for Data in Motion Security

2.1.1 Security Controls Implementation: Access Control

The goal of access control is to allow access by authorized individuals and devices and to disallow access to all others.Authorized individuals may be employees, technology service provider (TSP) employees, vendors, contractors, customers, or visitors. Access should be authorized and provided only to individuals whose identity is established, and their activities should be limited to the minimum required for business purposes. Authorized devices are those whose placement on the network is approved in accordance with institution policy. Change controls are typically used for devices inside the external perimeter, and to configure institution devices to accept authorized connections from outside the perimeter. An effective control mechanism includes numerous controls to safeguard and limits access to key information system assets at all layers in the network stack (Mohare, Lanjewar and Parekh, 2012).

One of the most challenging problems in managing large networks is the complexity of security administration. Role based access control (also called role based security), as formalized in 1992 by David Ferraiolo and Rick Kuhn, has become the predominant model for advanced access control because it reduces this cost. A variety of IT vendors, including

IBM, Sybase, Secure Computing, and Siemens began developing products based on this model in 1994. In 2000, the Ferraiolo-Kuhn model was integrated with the framework of Sandhu et al. (1996) to create a unified model for RBAC, published as the NIST RBAC model and adopted as an ANSI/INCITS standard in 2004. Today, most information technology vendors have incorporated RBAC into their product lines, and the technology is finding applications in areas ranging from health care to defense, in addition to the mainstream commerce systems for which it was designed. As of 2010, the majority of users in enterprises of 500 or more are now using RBAC, according to the Research Triangle Institute (Ferraiolo, and Kuhn, 2000).

Some of benefits of the Access Control systems are reduced employee downtime, more efficient provisioning, and more efficient access control policy administration beyond the added security provided by RBAC and also the Access Control systems can be easily set up.

The extra security stuff inherent in Access Control is understandable. There are lots of reasons for this. However, there should be some place for exceptions -- programs that are run constantly and have been safe to run for years and years should be protected from change by Malware by the Access Control, then should be flagged somehow. The shortcomings of the Access Control systems are elaborated as that it's too intrusive. There are very little problems with it anymore (Russ, 2007).

All of the secure ones require that users somehow approve system wide changes. It is the price of security. User Access Control (UAC) is a compromise between security and compatibility for legacy applications. Microsoft could have easily made Vista secure without UAC. This would have broken almost all legacy applications because most of them were poorly programmed from a security standpoint.

2.1.2 Access Rights Administration

System devices, programs, and data are system resources. Each system resource may need to be accessed by individuals (users) in order for work to be performed. Access beyond the minimum required for work to be performed exposes the institution's systems and information to a loss of confidentiality, integrity, and availability. Accordingly, the goal of access rights administration is to identify and restrict access to any particular system resource to the minimum required for work to be performed.

Management and information system administrators should critically evaluate information system access privileges and establish access controls to prevent unwarranted access.Access rights should be based upon the needs of the applicable user to carry out legitimate and approved activities on the institution's information systems. Policies, procedures, and criteria need to be established for both the granting of appropriate access rights and for the purpose of establishing those legitimate activities.

Formal access rights administration for users consists of four processes:

- An enrolment process to add new users to the system;
- An authorization process to add, delete, or modify authorized user access to operating systems, applications, directories, files, and specific types of information;
- An authentication process to identify the user during subsequent activities; and
- A monitoring process to oversee and manage the access rights granted to each user on the system.

The enrolment process establishes the user's identity and anticipated business needs for information and systems. New employees, IT outsourcing relationships, and contractors may also be identified, and the business need for access determined during the hiring or contracting process.

During enrolment and thereafter, an authorization process determines user access rights.In certain circumstances the assignment of access rights may be performed only after the manager responsible for each accessed resource approves the assignment and documents the approval. In other circumstances, the assignment of rights may be established by the employee's role or group membership, and managed by pre-established authorizations for that group. Customers, on the other hand, may be granted access based on their relationship with the institution (Mohare, Lanjewar and Parekh, 2012).

Authorization for privileged access should be tightly controlled. Privileged access refers to the ability to override system or application controls. Good practices for controlling privileged access include:

- Identifying each privilege associated with each system component,
- Implementing a process to allocate privileges and allocating those privileges either on a need-to-use or an event-by-event basis,
- Documenting the granting and administrative limits on privileges,
- Finding alternate ways of achieving the business objectives,
- Assigning privileges to a unique user ID apart from the one used for normal business use,
- Logging and auditing the use of privileged access,
- Reviewing privileged access rights at appropriate intervals and regularly reviewing privilege access allocations, and
- Prohibiting shared privileged access by multiple users.

The access rights process programs the system to allow the users only the access rights they were granted. Since access rights do not automatically expire or update, periodic updating and review of access rights on the system is necessary. Updating should occur when an individual's business needs for system use changes. Many job changes can result in an

expansion or reduction of access rights. Job events that would trigger a removal of access rights include transfers, resignations, and terminations. When these job events occur, institutions should take particular care to promptly remove the access rights for users who have remote access privileges, access to customer information, and perform administration functions for the institution's systems.

Periodic review of user accounts is a good control to test whether the access right removal processes are functioning and whether users exist who should have their rights rescinded or reduced because updating may not always be accurate. Access rights to new software and hardware present a unique problem. Typically, hardware and software are shipped with default users, with at least one default user having full access rights. Easily obtainable lists of popular software exist that identify the default users and passwords, enabling anyone with access to the system to obtain the default user's access. Default user accounts should either be disabled, or the authentication to the account should be changed. Additionally, access to these default accounts should be monitored more closely than other accounts.

Sometimes software installs with a default account that allows anonymous access.Anonymous access is appropriate, for instance, where the general public accesses an informational Web server. Systems that allow access to or store sensitive information, including customer information, should be protected against anonymous access.The access rights process also constrains user activities through an acceptable-use policy (AUP). Users who can access internal systems typically are required to agree to an AUP before using a system. An AUP details the permitted system uses and user activities and the consequences of noncompliance. AUPs can be created for all categories of system users, from internal programmers to customers. An AUP is a key control for user awareness and administrative policing of system activities. Examples of AUP elements for internal network and stand-alone users include:

- The specific access devices that can be used to access the network;
- Hardware and software changes the user can make to their access device;
- The purpose and scope of network activity;
- Network services that can be used and those that cannot be used;
- Information that is allowable and not allowable for transmission using each allowable service;
- Bans on attempting to break into accounts, crack passwords, or disrupt service;
- Responsibilities for secure operation; and
- Consequences of noncompliance.

Depending on the risk associated with the access, authorized internal users should generally receive a copy of the policy and appropriate training, and signify their understanding and agreement with the policy before management grants access to the system. Authorized users may seek to extend their activities beyond what is allowed in the AUP, and unauthorized users may seek to gain access to the system and move within the system. Network security controls provide many of the protections necessary to guard against those threats.

2.1.3 Authentication

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized (Burrows et al, 1990).

Authentication is the verification of identity by a system based on the presentation of unique credentials to that system. The unique credentials are in the form of something the user knows, something the user has, or something the user is. Those forms exist as shared secrets, tokens, or biometrics. More than one form can be used in any authentication process.

Security-sensitive environments protect their resources against unauthorized access by enforcing access control mechanisms. Text based passwords are not secure enough for such applications. User authentication can be improved by using both text passwords and structured images. Our image based registration and authentication system is called IBRAS. The system developed displays an image or set of images to the user, who would then select one to identify them. The system uses such image based passwords and integrates image registration and notification interfaces. Image registration enables users to have their favorite image(Conklin et al, 2004).

Authentication that relies on more than one form is called multi-factor authentication and is generally stronger than any single-factor authentication method. Authentication contributes to the confidentiality of data and the accountability of actions performed on the system by verifying the unique identity of the system user. That channel does not benefit from physical security and controlled computing and communications devices like internal local area networks (LANs), and is used by people whose actions cannot be controlled by the institution. The agencies consider the use of single-factor authentication in that environment, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Telecommunication institutions should perform risk assessments of their environment and, where the risk assessments indicate the use of single factor authentication is inadequate, the institutions should implement multi-factor authentication, layered security, or other controls reasonably calculated to mitigate risk.

In many web applications, it is desirable to have users log in by giving some unique login name and a password before accessing pages, focusing on the three basic phases to the web authentication process (Wolter 1997).

Logging in: The user must be prompted for a login and password. Some program on the server must check these against a database to confirm that they are valid.

User Tracking: Normally there is no persistent connection between a user's browser and the web server. If the web-site consists of more than one page, and if you do not want the user to log in again for each new page he looks at, we need some way to preserve the login information from page to page.

Logging Off: If we have a way to remember that a user is logged on, we also need a way to destroy that information when the user logs off.

Authentication systems has numerous advantages, some of them are:

Authentication system could help enhance existing popular systems and this design can be further improved to enhance security.

The IBRAS tool of the authentication systems can be very well developed to perform role based access control. The authentication system of database can be maintained as relational database by connecting the system to the database using JDBC connectivity.

The present system was developed as a stand-alone application. It can be deployed on the Internet easily. It can be integrated with simple biometric systems to enhance the security of the system.

The shortcomings of the authentication systems were, there were no focuses on improving the database by providing the persistent storage.

The system was not suitable for small devices like cell phones and PDA's.The system was not built with complete Object Oriented design. The next step was to rebuild the system using OO methodology using the popular required design patterns.

The system does not store the images. The images are read byte wise and hashed using a secure hashing function SHA-1. Images are large files. But SHA-1algorithm produces a 20 byte output which is very secure and requires less memory (Sundar et al,2003).

2.1.3.1 Shared Secret Systems

Shared secret systems uniquely identify the user by matching knowledge on the system to knowledge that only the system and user are expected to share. Examples are passwords, pass phrases, or current transaction knowledge. A password is one string of characters. A pass phrase is typically a string of words or characters that the system may shorten to a smaller password by means of an algorithm. Current transaction knowledge could be the account balance on the last statement mailed to the user/customer. The strength of shared secret systems is related to the lack of disclosure of and about the secret, the difficulty in guessing or discovering the secret, and the length of time that the secret exists before it is changed.

A strong shared secret system only involves the user and the system in the generation of the shared secret. In the case of passwords and pass phrases, the user should select them without any assistance from any other user, such as the help desk. One exception is in the creation of new accounts, where a temporary shared secret could be given to the user for the first log-in, after which the system requires the user to create a different password. Controls should prevent any user from re-using shared secrets that may have been compromised or were recently used by them.

Passwords are the most common authentication mechanism. Passwords are generally made difficult to guess when they are composed from a large character set, contain a large number of characters, and are frequently changed. However, since hard-to-guess passwords may be difficult to remember, users may take actions that weaken security, such as writing the passwords down. Any password system must balance the password strength with the user's ability to maintain the password as a shared secret. When the balancing produces a password

that is not sufficiently strong for the application, a different authentication mechanism should be considered. Pass phrases are one alternative to consider. Due to their length, pass phrases are generally more resistant to attack than passwords. The length, character set, and time before enforced change are important controls for pass phrases as well as passwords.

Shared secret strength is typically assured through the use of automated tools that enforce the password selection policy. Authentication systems should force changes to shared secrets on a schedule commensurate with risk. Passwords that are either not changed or changed infrequently are known as static passwords. While all passwords are subject to disclosure, static passwords are significantly more vulnerable. An attacker can obtain a password through technical means and through social engineering. Static passwords are appropriate in systems whose data and connectivity is considered low risk, and in systems that employ effective compensating controls such as physical protections, device authentication, mutual authentication, host security, user awareness, and effective monitoring and rapid response. Weaknesses in static password mechanisms generally relate to the ease with which an attacker can discover the secret.

2.1.3.2 Biometrics

Biometrics can be implemented in many forms, including tokens. Biometrics verifies the identity of the user by reference to unique physical or behavioral characteristics. A physical characteristic can be a thumbprint or iris pattern. A behavioral characteristic is the unique pattern of key depression strength and pauses made on a keyboard when a user types a phrase. The strength of biometrics is related to the uniqueness of the physical characteristic selected for verification. Biometric technologies assign data values to the particular characteristics associated with a certain feature. For example, the iris typically provides many more characteristics to store and compare, making it more unique than facial characteristics.

Unlike other authentication mechanisms, a biometric authenticator does not rely on a user's memory or possession of a token to be effective. Additional strength is that biometric do not rely on people to keep their biometric secret or physically secure their biometric. Biometrics is the only authentication methodology with these advantages.

Enrolment is a critical process for the use of biometric authentication. The user's physical characteristics must be reliably recorded. Reliability may require several samples of the characteristic and a recording device free of lint, dirt, or other interference. The enrollment device must be physically secure from tampering and unauthorized use.

When enrolled, a user's biometric is stored as a template. Subsequent authentication is accomplished by comparing a submitted biometric against the template, with results based on probability and statistical confidence levels. Practical usage of biometric solutions requires consideration of how precise systems must be for positive identification and authentication. More precise solutions increase the chances a person is falsely rejected.

Conversely, less precise solutions can result in the wrong person being identified or authenticated as a valid user (i.e., false acceptance rate). The equal error rate (EER) is a composite rating that considers the false rejection and false acceptance rates. Lower EERs mean more consistent operations. However, EER is typically based upon laboratory testing and may not be indicative of actual results due to factors that can include the consistency of biometric readers to capture data over time, variations in how users presents their biometric sample (e.g., occasionally pressing harder on a finger scanner), and environmental factors.

Weaknesses in biometric systems relate to the ability of an attacker to submit false physical characteristics or to take advantage of system flaws to make the system erroneously report a match between the characteristic submitted and the one stored in the system. In the first situation, an attacker might submit to a thumbprint recognition system a copy of a valid user's thumbprint. The control against this attack involves ensuring a live thumb was used for

the submission. That can be done by physically controlling the thumb reader, for instance having a guard at the reader to make sure no tampering or fake thumbs are used. In remote entry situations, logical liveness tests can be performed to verify that the submitted data is from a live subject.

Attacks that involve making the system falsely deny or accept a request take advantage of either the low degrees of freedom in the characteristic being tested, or improper system tuning. Degrees of freedom relate to measurable differences between biometric readings, with more degrees of freedom indicating a more unique biometric. Facial recognition systems, for instance, may have only nine degrees of freedom while other biometric systems have over one hundred. Similar faces may be used to fool the system into improperly authenticating an individual. Similar irises, however, are difficult to find and even more difficult to fool a system into improperly authenticating.

Attacks against system tuning also exist. Any biometric system has rates at which it will falsely accept a reading and falsely reject a reading. The two rates are inseparable; for any given system improving one worsens the other. Systems that are tuned to maximize user convenience typically have low rates of false rejection and high rates of false acceptance. Those systems may be more open to successful attack.

2.1.4 Network Access

Network security requires effective implementation of several control mechanisms to adequately secure access to systems and data. Many institutions have increasingly complex and dynamic networks stemming from the growth of distributed computing. Security personnel and network administrators have related but distinct responsibilities for ensuring secure network access across a diverse deployment of interconnecting network servers, file servers, routers, gateways, and local and remote client workstations. Security personnel

typically lead or assist in the development of policies, standards, and procedures, and monitor compliance. They also lead or assist in incident-response efforts.

Network administrators implement the policies, standards, and procedures in their day-to-day operational role. Internally, networks can host or provide centralized access to mission-critical applications and information, making secure access an organizational priority. Externally, networks integrate institution and third-party applications that grant customers and insiders access to their financial information and Web-based services.

An effective approach to securing a large network involves dividing the network into logical security domains. A logical security domain is a distinct part of a network with security policies that differ from other domains, and perimeter controls enforcing access at a network level. The differences may be far broader than network controls, encompassing personnel, host, and other issues.

Security domains are bounded by perimeters. Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as DNS. The perimeter controls may exist on separate devices or be combined or consolidated on one or more devices. Consolidation on a single device could improve security by reducing administrative overhead. However, consolidation may increase risk through a reduced ability to perform certain functions and the existence of a single point of failure.

Additionally, devices that combine prevention and detection present unique risks. Traditionally, if a prevention device fails, the detection device may alert on any resulting malicious activity. If the detection device fails, the prevention device still may function. If both functions are on the same device, and the device fails, the otherwise protected part of the institution's network may be exposed.

2.1.4.1 Firewalls

A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).

Typically, institutions may have four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rulesets can be static or dynamic. A static ruleset is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic ruleset often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring the IP is not on a "white list", creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP. Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

2.1.4.2 Malicious Code Filtering

Perimeters may contain proxy firewalls or other servers that act as a control point for Web browsing, e-mail, P2P, and other communications. Those firewalls and servers frequently are used to enforce the institution's security policy over incoming communications. Enforcement is through anti-virus, anti-spyware, and anti-spam filtering, the blocking of downloading of executable files, and other actions. To the extent that filtering is done on a signature basis, frequent updating of the signatures may be required.

2.1.4.3 Outbound Filtering

Perimeter servers also serve to inspect outbound communications for compliance with the institution's security policy. Perimeter routers and firewalls can be configured to enforce policies that forbid the origination of outbound communications from certain computers. Additionally, proxy servers could be configured to identify and block customer data and other data that should not be transmitted outside the security domain.

2.1.4.4 Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (NIPS) are an access control mechanism that allow or disallow access based on an analysis of packet headers and packet payloads. They are similar to firewalls because they are located in the communications line, compare activity to preconfigure or pre-programmed decisions of what packets to pass or drop, and respond with pre-configured actions. The IPS units generally detect security events in a manner similar to IDS units and are subject to the same limitations. After detection, however, the IPS unit may take actions beyond simple alerting to potential malicious activity and logging of packets. For example, the IPS unit may block traffic flows from the offending host. The ability to sever communications can be useful when the activity can clearly be identified as malicious. When the activity cannot be clearly identified, for example where a false positive may exist, IDS-like alerting commonly is preferable to blocking.

Although IPS units are access control devices, many implement a security model that is different from firewalls. Firewalls typically allow only the traffic necessary for business purposes, or only "known good" traffic. IPS units typically are configured to disallow traffic that triggers signatures, or "known bad" traffic, while allowing all else. However, IPS units can be configured to more closely mimic a device that allows only "known good" traffic.

IPS units also contain a "white list" of IP addresses that should never be blocked. The list helps ensure that an attacker cannot achieve a denial of service by spoofing the IP of a critical host.

2.1.4.5 Quarantine

Quarantining a device protects the network from potentially malicious code or actions. Typically, a device connecting to a security domain is queried for conformance to the domain's security policy. If the device does not conform, it is placed in a restricted part of the network until it does conform. For example, if the patch level is not current, the device is not allowed into the security domain until the appropriate patches are downloaded and installed.

2.1.4.6 DNS Placement

Effective protection of the institution's DNS servers is critical to maintaining the security of the institution's communications. Much of the protection is provided by host security.

However, the placement of the DNS also is an important factor. The optimal placement is split DNS, where one firewalled DNS server serves public domain information to the outside and does not perform recursive queries, and a second DNS server, in an internal security domain and not the DMZ, performs recursive queries for internal users.

2.1.4.7 Wireless Issues

Wireless networks are difficult to secure because they do not have a well-defined perimeter or well-defined access points. Unlike wired networks, unauthorized monitoring and denial of service attacks can be performed without a physical wire connection. Additionally,

unauthorized devices can potentially connect to the network, perform man-in-the-middle attacks, or connect to other wireless devices. To mitigate those risks, wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications.

2.1.5 Operating System Access

Telecommunication institutions must control access to system software within the various network clients and servers as well as stand-alone systems. System software includes the operating system and system utilities. The computer operating system manages all of the other applications running on the computer. Common operating systems include IBM zOS, OS/400, AIX, LINUX, various versions of Microsoft Windows, and Sun Solaris. Security administrators and IT auditors need to understand the common vulnerabilities and appropriate mitigation strategies for their operating systems. Application programs and data files interface through the operating system. System utilities are programs that perform repetitive functions such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks such as security, system monitoring, or transaction processing.

System software can provide high-level access to data and data processing. Unauthorized access could result in significant financial and operational losses. Telecommunication institutions should restrict privileged access to sensitive operating systems. While many operating systems have integrated access control software, third-party security software also is available. In the case of many mainframe systems, these programs are essential to ensure effective access control and can often integrate the security management of both the operating system and the applications. Network security software can allow institutions to

improve the effectiveness of the administration and security policy compliance for a large number of servers often spanning multiple operating system environments.

2.1.6 Application access

Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which application functions are available to users and other applications. The most commonly referenced applications from an examination perspective support the information processing needs of the various business lines. These computer applications allow authorized users or other applications to interface with the related database. Effective application access control can enforce both segregation of duties and dual control.

Access rights to sensitive or critical applications and their databases should ensure that employees or applications have the minimum level of access required to perform their business functions. Effective application access control involves a partnership between the security administrators, the application programmers (including TSPs and vendors), and the business owners.

2.1.7 Physical and Environmental Protection

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Conceptually, those physical security risks are mitigated through zone-oriented implementations. Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone. For instance, data centers may be in the highest security zone, and branches may be in a much lower security zone. Different security zones can exist within the same structure. Routers and servers in a branch, for instance, may be protected to a greater degree than customer service terminals.

Computers and telecommunications equipment within an operations center will have a higher security zone than I/O operations, with the media used by that equipment stored at yet a higher zone. The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, the following threats: Aircraft crashes, Chemical effects, Dust, Electrical supply interference, Electromagnetic radiation, Explosives, Fire, Smoke, Theft/Destruction, Vibration/Earthquake, Water, Criminals, Terrorism, Political issues (e.g. strikes, disruptions) and any other threats applicable based on the entity's unique geographical location, building configuration, neighboring entities, etc.

2.1.8 Data Centre Security

When selecting a site for the most important information systems components, one major objective is to limit the risk of exposure from internal and external sources. The selection process should include a review of the surrounding area to determine if it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Outside intruders can be deterred through the use of guards, fences, barriers, surveillance equipment, or other similar devices. Since access to key information system hardware and software should be limited, doors and windows must be secure. Additionally, the location should not be identified or advertised by signage or other indicators.

Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. They should provide continuous coverage. Detection devices have two purposes - to alarm when a response is necessary and to support subsequent forensics. The alarm capability is useful only when a response will occur.

Some intruder detection devices available include Switches that activate an alarm when an electrical circuit is broken; light and laser beams, ultraviolet beams and sound or vibration detectors that are invisible to the intruder, and ultrasonic and radar devices that detect

movement in a room; and Closed-circuit television that allows visual observation and recording of actions.

Risks from environmental threats can be addressed through devices such as halon gas and halon replacements, smoke alarms, raised flooring, and heat sensors. Physical security devices frequently need preventive maintenance to function properly. Maintenance logs are one control the institution can use to determine whether the devices are appropriately maintained. Periodic testing of the devices provides assurance that they are operating correctly.

Security guards should be properly instructed about their duties. The employees who access secured areas should have proper identification and authorization to enter the area. All visitors should sign in and wear proper IDs so that they can be identified easily. Security guards should be trained to restrict the removal of assets from the premises and to record the identity of anyone removing assets. Consideration should be given to implementing a specific and formal authorization process for the removal of hardware and software from premises.

2.1.9 Physical Security in Distributed IT Environments

Hardware and software located in a user department are often less secure than that located in a computer room. Distributed hardware and software environments (e.g., local area networks or LANs) that offer a full range of applications for small financial institutions as well as larger organizations are commonly housed throughout the organization, without special environmental controls or raised flooring. In such situations, physical security precautions are often less sophisticated than those found in large data centers, and overall building security becomes more important. Internal control procedures are necessary for all hardware and software deployed in distributed, and less secure, environments.

The level of security surrounding any hardware and software should depend on the sensitivity of the data that can be accessed, the significance of applications processed, the cost of the

equipment, and the availability of backup equipment. Because of their portability and location in distributed environments, personal computers (PCs) often are prime targets for theft and misuse. The location of PCs and the sensitivity of the data and systems they access determine the extent of physical security required.

For PCs in unrestricted areas such as a branch lobby, a counter or divider may provide the only barrier to public access. In these cases, institutions should consider securing PCs to workstations, locking or removing disk drives and unnecessary physical ports, and using screensaver passwords or automatic timeouts. Employees also should have only the access to PCs and data they need to perform their job. The sensitivity of the data processed or accessed by the computer usually dictates the level of control required. The effectiveness of security measures depends on employee awareness and enforcement of these controls.

An advantage of PCs is that they can operate in an office environment, providing flexible and informal operations. However, as with larger systems, PCs are sensitive to environmental factors such as smoke, dust, heat, humidity, food particles, and liquids. Because they are not usually located within a secure area, policies should be adapted to provide protection from ordinary contaminants. Other environmental problems to guard against include electrical power surges and static electricity. The electrical power supply in an office environment is sufficient for a PC's requirements.

However, periodic fluctuations in power (surges) can cause equipment damage or loss of data. PCs in environments that generate static electricity are susceptible to static electrical discharges that can cause damage to PC components or memory. Physical security for distributed IT, particularly LANs that are usually PC-based, is slightly different than for mainframe platforms. With a network there is often no centralized computer room. In addition, a network often extends beyond the local premises.

There are certain components that need physical security. These include the hardware devices and the software and data that may be stored on the file servers, PCs, or removable media (tapes and disks). As with more secure IT environments, physical network security should prevent unauthorized personnel from accessing LAN devices or the transmission of data. In the case of wire-transfer clients, more extensive physical security is required.

Physical protection for networks as well as PCs includes power protection, physical locks, and secure work areas enforced by security guards and authentication technologies such as magnetic badge readers. Physical access to the network components (i.e., files, applications, communications, etc.) should be limited to those who require access to perform their jobs. Network workstations or PCs should be password protected and monitored for workstation activity.

Network wiring requires some form of protection since it does not have to be physically penetrated for the data it carries to be revealed or contaminated. Examples of controls include using a conduit to encase the wiring, avoiding routing through publicly accessible areas, and avoiding routing networking cables in close proximity to power cables. The type of wiring can also provide a degree of protection; signals over fiber, for instance, are less susceptible to interception than signals over copper cable.

Network security also can be compromised through the capture of radio frequency emissions. Frequency emissions are of two types, intentional and unintentional. Intentional emissions are those broadcast, for instance, by a wireless network. Unintentional emissions are the normally occurring radiation from monitors, keyboards, disk drives, and other devices.

Shielding is a primary control over emissions. The goal of shielding is to confine a signal to a defined area. An example of shielding is the use of foil-backed wallboard and window treatments. Once a signal is confined to a defined area, additional controls can be

implemented in that area to further minimize the risk that the signal will be intercepted or changed.

2.1.10 Encryption

Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.

Encryption can be used as a preventive control, a detective control, or both. As a prevention control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow discovery of unauthorized changes to data and to assign responsibility for data among authorized parties. When prevention and detection are joined, encryption is a key control in ensuring confidentiality, data integrity, and accountability.

Encryption can strengthen the security of an institution's systems when properly used. Encryption also has the potential, however, to weaken other security aspects. For instance, encrypted data drastically lessens the effectiveness of any security mechanism that relies on inspections of the data, such as anti-virus scanning and intrusion detection systems. When encrypted communications are used, networks may have to be reconfigured to allow for adequate detection of malicious code and system intrusions. Although necessary, encryption carries the risk of making data unavailable should anything go wrong with data handling, key management, or the actual encryption. For example, a loss of encryption keys or other failures in the encryption process can deny the institution access to the encrypted data. The products used and administrative controls should contain robust and effective controls to ensure reliability.

Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs and risks of encryption. The costs include potentially significant overhead costs on hosts and networks. Generally speaking, authenticators are encrypted whether on public networks or on the financial institution's network. Sensitive information is also encrypted when passing over a public network and also may be encrypted within the institution.

Encryption cannot guarantee data security. Even if encryption is properly implemented, for example, a security breach at one of the endpoints of the communication can be used to steal the data or allow an intruder to masquerade as a legitimate system user.

2.1.11 Malicious Code Prevention

Malicious code is any program that acts in unexpected and potentially damaging ways. Common types of malicious code are viruses, worms, Trojan horses, monitoring programs such as spyware, and cross-site scripts. The functions of each were once mutually exclusive; however, developers combined functions to create more powerful malicious code.

Malicious code can replicate itself within a computer and transmit itself between computers, change, delete, or insert data, transmit data outside the institution, and insert backdoors into institution systems, attack institutions at either the server or the client level and attack routers, switches, and other parts of the institution infrastructure. Malicious code can also monitor users in many ways, such as logging keystrokes and transmitting screenshots to the attacker. Typically malicious code is mobile, using e-mail, Instant Messenger, and other peer-to-peer (P2P) applications, or active content attached to Web pages as transmission mechanisms. The code also can be hidden in programs that are downloaded from the Internet or brought into the institution on diskette. At times, the malicious code can be created on the institution's systems either by intruders or by authorized users. The code can also be introduced to a Web server in numerous ways, such as entering the code in a response form on a Web page.

Malicious code does not have to be targeted at the institution to damage the institution's systems or steal the institution's data. Most malicious code is general in application, potentially affecting all Internet users with whatever operating system or application the code needs to function.

2.1.12 Controls to Protect against Malicious Code

Typical controls to protect against malicious code use technology, policies and procedures, and training, all applied in a layered manner from perimeters inward to hosts and data. The controls are of the preventative and detective/corrective variety. Controls are applied at the host, network, and user levels:

2.1.12.1 Host Level

- Host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.
- Host IPS, including anti-virus, anti-spyware, and anti-rootkit software. An additional technology is software that limits applications calls to the OS to the minimum necessary for the application to function.
- Integrity checking software, combined with strict change controls and configuration management.
- Application of known-good configurations at boot-up.
- Periodic auditing of host configurations, both manual and automated.

2.1.12.2 Network Level

- Limiting the transfer of executable files through the perimeter.
- IDS and IPS monitoring of incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors.

- Routing ACLs that limit incoming and outgoing connections as well as internal connections to those necessary for business purposes.
- Proxy servers that inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers.
- Filtering to protect against attacks such as cross-site scripting and SQL injection.

2.1.12.3 User Level

There should be user education in awareness, safe computing practices, indicators of malicious code, and response actions. On Monday 04 April, 2011 the leading independent newswire and information source for the worldwide financial technology community in UK, FINEXTRA, reported on their website about serious data breach (Epsilon Data Breach) affecting multiple companies including Barclays Bank of Delaware and US Bank, all in United States. The incident occurred in USA. The event was later confirmed by a report at Infosec Island (www.infosecisland.com).

The report states that Epsilon, an email marketing and service provider which contracts with some of largest retail and financial companies in the nation, has reported that their networks have been breached. The company states that their systems experienced an unauthorized access event that has exposed the names and email addresses of the customers the company's clients serve.

By regulation all institutions in a business of collecting customers' data (including financial institutions) are obliged by law to ensure security of such data, otherwise the customer must be informed of incapability of securing the data. The organization may also be required to comply with standard or requirement such as:

i. Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data

- Do not use vendor-supplied defaults for system passwords and other security parameters

ii. Protect cardholder data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

iii. Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

iv. Implement strong access control measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

v. Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

vi Maintain an information security policy

- Maintain a policy that addresses information security

In event of non-compliance, the entire network environment may be vulnerable to exploitation, unauthorized access events, illegal data excavation by crackers and hackers. This may result in the case of Epsilon Data Breach.

2.1.13 Data Encryption: Applications and Limits

Schneier (2010) discussed how the information age practice of encrypting data at rest deviates from the historical use of cryptography for protecting data while it is communicated or in transit. One of Schneider's key points is that for data in motion, encryption keys can be ephemeral, whereas for data at rest, keys must be retained for as long as the stored data is

kept encrypted. As Schneider points out, this does not reduce the number of things that must be stored secretly; it just makes those things smaller (the size of a key is far smaller than a typical data file) as Schneier states: "This whole model falls apart on the Internet.

Much of the data stored on the Internet is only peripherally intended for use by people; it is primarily intended for use by other computers and therein lays the problem. Keys can no longer be stored in people's brains. They need to be stored on the same computer, or at least the network, that the data resides on. In meeting this challenge, there has been a recent rise in the number of security appliances that are intended to address this and related security implementation issues for data in motion security. With recent news events of financial and public health data with personal identifiers being stolen or lost, cryptography and encryption has become an important issue for any organization handling sensitive data. Using cryptography and encryption can be utilized to prevent unfortunate breach of commitment to protect the confidentiality of customer, client or patient records.

2.1.13.1 Encryption

The oldest known encryption device based on the transposition principle is the Scytale, which was mentioned by Thucydides in his History, in the fifth century B.C. Encryption converts plaintext into cipher text the encrypted data or message, which has the appearance of random, unintelligible data. The transformed information, in its encrypted form, is called the ciphertext. There are two classes of encryption: a public key known to everyone and a private or secret key known only to the recipient of the message (Robinson, 1995).

2.1.13.2 Cryptography

Cryptograph includes both the practice and study of encryption and decryption that encodes data so that it can only be decoded by specific/authorized individuals. Encryption is the ability to change plaintext data so that it becomes unrecognizable to any but the intended recipient attempts to view the data, while decryption is changing the data back to its original

plaintext form. A cryptosystem is a system for encrypting and decrypting data. These usually involve an algorithm for combining the original data "plaintext" with one or more "keys" - numbers or strings of characters known only to the sender and/or recipient. The resulting output is known as “cipher text” (Robinson, 1995).

2.1.13.3 Cryptosystem

Cryptosystem is a system used for encrypting and decrypting data. A strong cryptosystem has a large range of possible keys so that it is not possible to just try all possible keys a “brute force” approach. Cryptography commonly uses mathematical algorithms as the ‘key’ and this same “key” is input on encryption to change the data and the same “key” must be used to decrypt the data. A strong cryptosystem will produce cipher text which appears random to all standard statistical tests. A strong cryptosystem will resist all known previous methods for breaking codes “cryptanalysis”. Although cryptography is very old (dates back to Ancient Egypt), the desktop-computer revolution has made it possible for cryptographic to become widely used to secure data (Robinson, 1995).

2.1.13.4 Encryption of Data in Motion

It is said that “there is nothing like absolute security of data in motion; until it is found to be broken, it is still secured”. Schneier (2010) pointed out that cryptography is singularly ill-suited to solve the major network security problems of today: denial-of-service attacks, website defacement, theft of credit card numbers, identity theft, viruses and worms, DNS attacks, network penetration, and so on. He stated:

“Computer security is much more balanced. There'll be a new attack, and a new defense, and a new attack, and a new defense. It's an arms race between attacker and defender. And it's a very fast arms race. New vulnerabilities are discovered all the time. The balance can tip from defender to attacker overnight, and back again the night after. Computer security defenses are inherently very fragile.

Unfortunately, this is the model we're stuck with. No matter how good the cryptography is, there is some other way to break into the system. Recall how the FBI read the PGP-encrypted email of a suspected Mafia boss several years ago. They did not try to break PGP; they simply installed a keyboard sniffer on the target's computer. Notice that SSL- and TLS-encrypted web communications are increasingly irrelevant in protecting credit card numbers; criminals prefer to steal them by the hundreds of thousands from back-end databases.

On the Internet, communications security is much less important than the security of the endpoints. And increasingly, we cannot rely on cryptography to solve our security problems Schneier (2010)."

Data-in-Motion technologies are not comprehensive data loss prevention solutions and continue to be circumvented. When laptops, for example, are used by employees in public environments they are at much greater risk because the data-in-motion technologies cannot extend their processing to these third party environments. Data-in-Motion technologies can only prevent exposures when those exposures occur in clear text. Hackers capable of penetrating an organization's security defences are generally sufficiently sophisticated and establish secure tunnels through which to transmit private data because they know Data-in-Motion technologies may be present. This act of encrypting data while in motion negates the effectiveness of Data-in-Motion solutions (Lee, 2010).

Data-in-Motion technologies are more complicated to implement and operate than Data-at-Rest technologies. Upfront, Data-in-Motion technologies require additional hardware and professional services expertise to deploy. They are not plug-and-play. The nature of the data transmitted is different for each organization and the exact policies desired by each organization often require special configurations. After initial deployment, Data-in-Motion

technologies also require continuous tuning to optimize their behavior. Improper configuration dramatically reduces the effectiveness of the blocking technology (Lee, 2010).

Data-in-Motion solutions also require constant monitoring and place a performance strain on the network. Unlike Data-at-Rest solutions, which can be scheduled to perform scanning during off-peak hours, Data-in-Motion technologies are always on and constantly 'sniffing' the network for data. This constant sniffing can dramatically reduce an organization's productivity or force the organization to purchase more expensive infrastructure to support the increased network demand (Lee, 2010).

Lee (2010) stressed out that there are basically two ways to use encryption when trying to protect data in motion: an encrypted connection or using file encryption.

2.1.13.5 Encrypted Connection

An encrypted connection is basically where anything that is sent over a network is automatically encrypted, regardless of the encryption status of the information to be sent. For example, if you're sending an encrypted file, it will get encrypted again while being sent. Generally, the end user doesn't have to do anything but send the information. A prime example is on-line banking, where a particular site (beginning with https://) encrypts any information being sent from your browser to a bank's servers and vice-versa. This form of encryption has a drawback: usually, it's either there or not. And, if a secure connection is not available, there is very little a person can do.

2.1.14 Using File Encryption Software for Data in Motion Security

Another method of ensuring data in motion security is to use file encryption, which is technically an encryption method for data at rest. The beauty of file encryption is that an encrypted file exists in encrypted form, so it does not matter whether it's being stored or sent as an attachment, the file will always be encrypted, and hence, protected. If an encrypted

connection is not available, but a document must be sent via network, and must also be protected, it makes sense to encrypt the file prior to sending it. In the end, it provides just as much security as a secure network (Lee, 2010).

Some commercial vendors such as Centrify Corporation as developed a software suite namely "Centrify Suite 2012" which adopts integrated approach of securing access to sensitive information within the internal network. Centrify DirectSecure is a policy-based software solution that secures sensitive information by dynamically isolating and protecting cross-platform systems and enabling optional end-to-end encryption of data in motion. By leveraging existing Active Directory infrastructure and the native IPsec support built into today's operating systems, DirectSecure seamlessly blocks entrusted systems from communicating with trusted systems, and does so without the need to change network or applications. Additionally, DirectSecure enables system administrators/users to take advantage of the new Windows 7 DirectAccess feature to secure end-to-end communications with UNIX and Linux systems running DirectSecure.

One remarkable feature is that it enables optional end-to-end encryption of data in motion to address compliance requirements and secure sensitive data. Thus traffic sent between trusted systems is cryptographically protected so that the receiving system can verify that an authenticated system sent the packet and that the packet was not tampered with and/or modified in transit. With DirectSecure groups of servers can be configured to accept specific types of traffic. In addition, some or all of the traffic between managed systems can be optionally encrypted, providing protection from malicious network users who attempt to capture and interpret network traffic. Encrypting data in motion is important to addressing audit requirements (for example, PCI requirement) or to better secure legacy applications that transport sensitive data in the clear (www.pcicomplianceguide.org).

Many other institutions concern about security of data in motion takes a step further to institute operation policies or security control measures, in addition to adopted software and hardware installations. Division of Cancer Prevention and Control, National Center for Chronic Disease Prevention and Health Promotion (USA), proposes security policy to be adopted by all National Program of Cancer Registries (NPCR). It states that all NPCR should have a security policy that is specific to the needs of the registry and the organization the registry operates. Below is section of their underlying data security policy (www.ftp.cde.gov.gov).

1. All network communications should be encrypted prior to being transmitted and decrypted when received by the intended recipient
    - Encryption of data in motion provides end to end protection as information travels across a network
    - Encryption of data in motion does not provide protection of the information being attacked on the endpoints where most attacks occur
2. Hides information as it moves across the network, between the database and the client
3. Includes traffic moving over your local network, the Internet, or even over a wireless network
4. Standards for data-in-motion encryption include SSL (Secure Sockets Layer), TLS (Transport Layer Security) and IPSEC (Internet Protocol Security)
5. Encryption of data in motion does nothing to protect data that is attacked at the end points (most attacks do not occur on data-in-motion. Most attacks occur against the end points, where data sits for long periods of time)
6. Prevents:
    - someone from intercepting sensitive information as it moves between the client and database

- session hijacking (redirecting data intended for a target)
- replay attacks where an authentication session is replayed by an attacker to fool a computer into granting access

2.1.15 Vulnerabilities in Web-based applications

Table 2.1 Steps to find Vulnerabilities in Web-based applications

	Process	Action
1	Identify applications running on ports	Use of Ports Scanner -
2	Find version information (if possible)	From vendors website or installation CD/DVD
3	Look for exploits	Review application literature from the Internet
4	Run exploits against the target application	Find exploits against the application from the internet
5	Analyze flaws on the web application	Apply open source Nikto and Paros Proxy software

According to OWASP the top ten vulnerabilities known to exist specifically within Web Applications are:

1. Cross Site Scripting
2. Injection Flaws (including SQL injections)
3. Malicious File Execution (typically involves uploading malicious and unchecked programs into a server; an example would be the "PHP remote file inclusion " vulnerabilities)
4. Insecure Direct Object Reference (similar to the Webmin Arbitrary file Disclosure vulnerability)
5. Cross Site Request Forgery (an attack that targets a victim' s browser)
6. Information Leakage and Improper Error Handling

7. Broken Authentication and Session Management (session hacking, as seen in Web Goat)
8. Insecure Cryptographic Storage (this is simply poor application design, when programmers don't use the best form of encryption or implement encryption incorrectly)
9. Insecure Communications (includes sending usernames and passwords across the network unencrypted, where anyone listening on the network segment can capture the data)
10. Failure to Restrict URL Access (more improper programming, where a malicious user can bypass log-in security measures)

2.1.16 Network mapping and OS fingerprinting

Network mapping was used to create a picture of the configuration of the branch's network. A network diagram was created which infers the logical locations and IP addresses of routers, firewalls, Web servers and other border devices. It assisted in identifying or "fingerprinting" the various operating systems in the network. Tools such as Look@Lan, LanState, Spiceworks, ping, traceroute and Nmap, help me to create a reasonably accurate network map.

An extension of network mapping was Port Scanning. This technique was aimed at identifying the type of services available on the target machine. The scan result reveals important information such as function of a computer (whether it is a Web server, mail server etc) as well as revealing ports that may be serious security risks such as telnet. Port scans should include number of individual tests, including:

- TCP (Transmission Control Protocol) scan
- Connect scan
- SYN (or half open) scan
- RST (or Xmas-tree) scan
- UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) scans. Tools such as Nmap can perform this type of scan.
- Dynamic ports used by RPC (Remote Procedure Call) should be scanned using tool such as RPCinfo.

Using NetBIOS tools help in scanning for sharing folders on targeted computers.

2.1.17 Spoofing

Spoofing involves creation of TCP/IP packets using somebody else's Internet addresses and then sending the same to the targeted computer making it believe that it came from a trusted source. It was the act of using one machine to impersonate another. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. The destination machine only uses that source IP address when it responds back to the source.This technique was used (internal and external) in my penetration testing to access computers that have been instructed or configured (firewall protected) to only reply to specific computers. This result in sensitive data released to unauthorized systems like the usernames, passwords and other important credentials was exposed to my laptop. And also, allowed accessed to some materials only from certain approved logins. IP spoofing was also an integral part of many network attacks that do not need to see responses (blind spoofing).

2.1.18 Network sniffing

Sniffing was technique used to capture data in motion (transmission) as it travels across a network. Sniffing was an important information gathering technique that enables capturing of specific information, such as passwords and also an entire conversation between specific computers, if required. This technique was performed by using the network card of a laptop which was put in promiscuous mode, so that it captures all data being sent across the network. So after the experiment, some packet information and paths on the network system were retrieved. Also, some usernames and passwords were captured as the users logged into the system. Sniffing was extensively used in internal testing where the sniffer or the computer in promiscuous mode was directly attached to the network enabling capturing of a great deal of information. Sniffing was performed by a number of commercial tools such as Ethereal, Network Associates SnifferPro and Network Instruments Observer.

2.1.19 Trojan attack

Trojans are malicious programs that are typically sent into network as e-mail attachments or transferred via IM chat rooms. These programs run in stealth mode and get installed on the client computer without the user's knowledge. A Trojan attack program was installed on a laptop which was used to open remote control channels to attackers and captured available data within the network environment. And the result shows that when Trojan program are sent into network system, any available data which was not well secured within a networked

environment would be captured. But after the experiment, all the information or data on their network environment was well secured with passwords and special codes.

2.1.20 Brute force attack

This technique involves trying a huge number of alphanumeric combinations and exhaustive trial and error methods in order find legitimate authentication credentials. The objective behind this time consuming exercisewasto gain access to the target system.

Some of the test conducted using the brute force attack techniques are as follows:

I created my own codes and tried to get access to the network system of the bank for five consecutive times. So I made some alphanumeric combinations and some trial and error methods like;

First of all, this 1052138679436 was used which was the same number of digits a customer must attained before gaining access to the system and I used this number for three times to gain access to the system.

Secondly, the code was changed and this was used 0050287491015 to get accessed to the system for two times.

Then, this alphanumeric combination "B1616492S103K" was used to also gain access to the system for several times.

Also, the name of the branch manager and the branch code was combined as "Asante00345Edward", if I could gain access to their main server; I did this for three consecutive times.

Again, the network system was overloaded using the brute force attacks so that the system would stop responding to legitimate requests.

Finally, an account lockout was used; this attack was used to close the account to legitimate users who wanted to access the system.

So out of the entire test conducted using the brute force attack, none of them proved fertile except the overloading of the system which made the links in the network system slow in transmitting data across the network environment. So it was meant that, it was not easy for intruder to penetrate to a network system using any brute force method.

2.1.21 Security Policy and Control Review

IT security breaches arise through the intentional exploitation or the unintentional triggering of vulnerabilities in the application of IT within business concerns. For example, Zero-day threats are attacks that use an unknown exploit/attack for which no patch

or antivirus definition file exists as yet. There is no method of detection for zero-day exploits that is 100%. This can trigger massive damaged and even in severe cases continue the damage until patch or fix was developed. By that time, if the exploits were to target data-in-motion, it would be realized that massive sensitive data might have been transmitted to remote system for so long a time.

2.1.21.1 Cause of application vulnerabilities

Vulnerabilities can arise through failures in:

- requirements - that is, an IT product may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;
- development - that is, an IT product does not meet its specifications and/or vulnerabilities have been introduced as a result of poor development standards or incorrect design choices;
- cooperation - that is, an IT product has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

2.1.22 Review of internal data security policies

Data in management information system is usually created from pieces of information gathered about a person or a specific subject. Each collection of data matches specific objective that can be tagged as "sensitive", or otherwise. Recent data exploits have brought us the knowledge that, data-in-motion may inherit some amount of vulnerability from;

1. the application used in creating and storing the data, entails some vulnerabilities;
2. the stored system, if it had no security at all or its security had been previously compromised;
3. Poorly managed user rights and controls.

For this reasons, presence of internal data security policy may help me to form a judgment as to security of the data-in-motion from when it was data-at-rest. The main objectives to look for in such a policy are:

1. encryption – what is the branch's standard encryption methodology, when will encryption be used and by whom.
2. digital signatures – what is the branch's standard, when will digital signatures be used

and by whom.

3. access controls – usually descriptions of logon warning screens on a computer and access lists for dedicated computer rooms, non-disclosure agreements.
4. passwords – duration, number of and what type of characters, who must use passwords, for what and when, how to create.
5. Files, folders and network resources sharing – what are regulations, users and access controls.
6. use of personal resources within the branch – allowed or not allowed, if so, under what conditions.
7. Personnel/physical security – what happens if a system containing sensitive information is moved out from a locked door.
8. System configuration change – changes that alter the security profile (risk) of the branch.
9. inventory of IS assets –who should keep an inventory of all the branch's IS assets, who should have access to that inventory, is it available to the IT/audit teams.
10. Updates, patches and fixes – how often all the computers and the network are checked for updates, patches and security vulnerabilities to be fixed.
11. Report or evidence of vulnerability tests for all applications used on the computers in the branch.
12. Finally, report of periodic security audit

2.1.23 Review of internal data security compliance

Compliance is alignment with a set of general policies, where the type of compliance required depends upon the region and currently ruling government, industry and business types, and supporting legislation. Compliance is compulsory; however, as with any other threat, a risk assessment must be made whether or not to invest in any type of compliance.

Government agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render the product insecure and place highly sensitive

information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

Generally, there are three types of compliance respected by financial institutions and organizations enforcing data security. They are:

1. Legislative

   Compliance with legislation is in accordance to the region where the legislation can be enforced. The strength and commitment to the legislation comes from previously successful legal arguments and appropriately set and just enforcement measures. Failure to comply with legislation may lead to criminal charges. Examples are Sarbanes-Oxley, HIPAA, and the various Data Protection and Privacy legislation.

2. Contractual

   Compliance to contractual requirements is in accordance to the industry or within the group that requires the contract and may take action to enforce compliance. Failure to comply with contractual requirements often leads to dismissal from the group, a loss of privileges, loss of reputation, civil charges, and in some cases where legislation exists to support the regulatory body, criminal charges. An example is the payment card industry data security standard (PCI DSS) promoted and required by VISA and MasterCard.

3. Standards based

   Compliance to standards is in accordance with the business or organization where the compliance to standards is enforced as policy. Failure to comply with standards often leads to dismissal from the organization, a loss of privileges, a loss of reputation or brand trust, civil charges, and in some cases where legislation exists to support the policy makers, criminal charges. Examples are the OSSTMM, ISO 27001/5, and ITIL.

In this context, compliance helps network architects, network administrators, security staff, technical support staff, and computer security program managers who are responsible for the technical aspects of preparing, operating, and securing their organization's networks. My final approach will be on verifying if the network security infrastructure complies with any standard, and whether it is certified by any relevant statutory organization.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter provides approach and technique for evaluating security of data-in-motion at the Adum and KNUST branches of the Barclays Bank.The approach takes reconnaissance that an attack was imminent by intruders and illegal hackers who would found means to intercept data-in-motion within the branch network perimeter in other to have sensitive information that might lead to wealth. Many attacks on financial institutions were not particularly directed to intercept sensitive data in motion (such as customer account information), but rather information that could gave the intruder right of access to assume himself as authorized administrator within the internal network which can lead to access to database of many customers and clients sensitive banking information.

3.1 Vulnerability scanning/analysis

This technique was exhaustive on examining the branch's network infrastructure aimed at determining its current state. The targets range from a single system or only critical systems (sending or receiving data) to scanning the entire network. It was performed using automated tools that test for a multitude of potential weaknesses in a system against a database of known vulnerabilities and report potential security holes. Some of the commonly used vulnerability scanners include: the open-source Nessus Project's Nessus, ISS Internet Scanner, GFI Software's GFI LanGuard Network Security Scanner, eEye Digital Security's Retina Network Security Scanner, the BindView RMS vulnerability-management solutions and Network Associates Cyber Cop.

3.2 Scenario analysis

Once a vulnerability scanning has been done and weaknesses identified, the next step was to perform Scenario testing. This testing aims at exploiting, identifying security weaknesses to perform a system penetration that would produce a measurable result, such as stolen information, stolen usernames and passwords or system alteration. After the scenario experiment, no information, usernames and passwords were retrieved from the system. This level of testing assures that no false positives are reported and makes risk assessment of vulnerabilities much more accurate. Many tools exist to assist exploit testing, although the

The approach of this study is given in Table 3.1

Table 3.1 Methodology Approach

	Approach	Reason
1	**External Testing Strategy**	
	Deployment of penetration test from the external network perimeter on the branch's wireless network	This was to ascertain whether data-in-motion is available and can be cracked by illegal intruder
	Internal Testing Strategy	
2	Apply use of most hackers' techniques commonly known to be used against target institutions in a manner to attempt to intercept data-in-motion from the wireless or wired interface of the network.	To test security of data-at-rest and the network resources
3	Test internal security on software, web-based applications, databases, access control measures, security policies, encryption and cryptographic systems in used	This was to evaluate vulnerabilities of software applications
	Security Policy and Control Review	
4	Review of internal data security policies, control and measures	to ascertain whether data is secured within the network
5	Review internal network security compliance	to find out if there is a data security measures from the source of generation to destination

3.4 External Testing Strategy

The deployment of penetration test from the external network perimeter on the branch's wireless network, according to methodology proposed in the OSSTMM (Herzog, 2003).

Some of the penetrating test I conducted on the external testing strategy are as follows:

First of all, password cracking method was used. The reason for using this method was to retrieve a user's password, username when he or she logs on to the bank system. Also, to identify weaker passwords and to examine data from a live network or from a captured file on disk. The password cracking method like the network sniffer on laptop and connected it to a legitimate wireless access point which was their database system so that when the password hashes were captured, it would retrieved a user's password when the user logs on to the system. The device which was used was a laptop, network sniffer software installed on the laptop. The laptop was connected to the database system which contains most information of the workers of the institution. This experiment was conducted for twenty-five times on the bank system and the sample of the experiment are shown below in the table. The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted five consecutive times respectively.

Table 3.2

Password cracking method using Network Sniffer	Number of user's password received
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	0

From the table 3.2, the password cracking method like the Network sniffer was used. It was to capture passwords and retrieved usernames and other credentials from the system. But it was noticed that, upon all the experiment which was conducted, none of it was successful, so the network sniffer could not be used to penetrate or have access to the system of the bank.

Also, a cracking method called hybrid attack was used with the help of dictionary attack software on a laptop. The reason for using this method was to substitute and changed some passwords and usernames of some of the workers in the bank to have accessed to the main server. Also, by modifying existing dictionary words to generate additional password attempts. Here, changes and substituted was made on some of the characters and numbers for

letters of the worker's password like a worker by name Jemima Owusu of Knust branch of the bank with the password "J146O876KN", was changed and substituted as "146JO678MB to tried and got accessed to the bank's main system. Here, the laptop on which the hybrid attacks software was connected to the server of the bank. This hybrid attack method was used for twenty times on the server to know how the results would be. And the sample results of this experiment are shown below in the table.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted four consecutive times respectively.

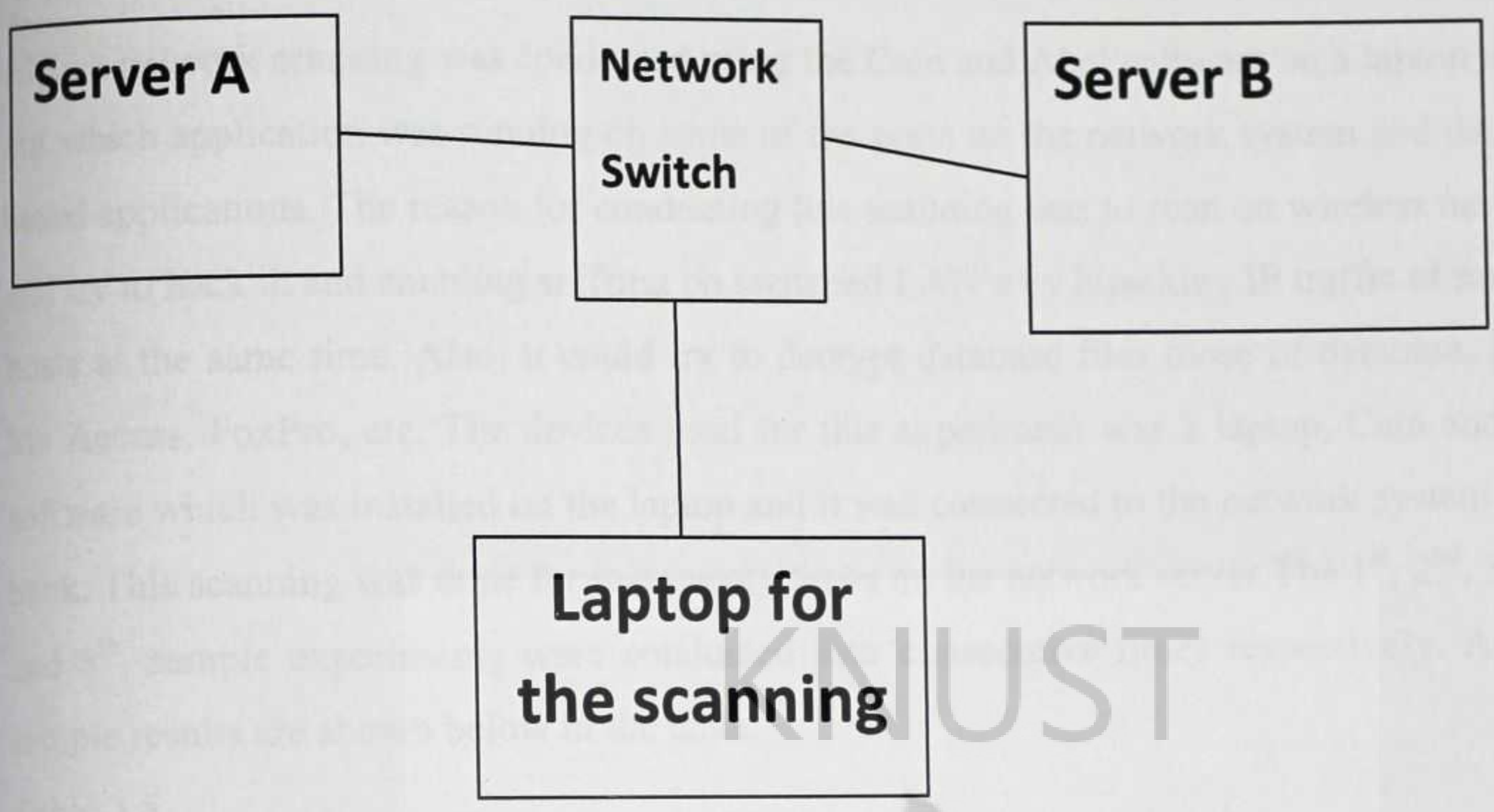
Table 3.3

Hybrid attack cracking method	Number of password and usernames changed
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	0

From table 3.3, the method of Hybrid attack was used. And it was used with the help of the dictionary attack software on a laptop. This was to check if any modifications and substitutions would be made on any username or password, so as to get accessed to the bank's main system. But after the experiment, it provides access denied, invalid codes, unknown password, etc. so this method would not be used to have accessed to the server of the bank.

Again, a network scanning was conducted using Nmap (Network Mapper) software on a laptop to find out all hosts potentially connected to the organization's network, the network services operating on those hosts and their specific applications running the identified services. Also, to determine various details about the remote computers and to gain unauthorized access to computers systems. Again, this scanning was conducted to discover computers and services on a computer network, passive services on the network despite the fact that such services are not advertising themselves with a services discovery protocols and to discover open ports which are likely to be vulnerable services, in preparation for attacking those services with another program. The devices used for this scanning was, a laptop which the Nmap was installed on it, which the laptop was connected to the bank's network server. The scanning was done for thirty rounds on the network system and the sample experiments are shown below in the table.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were scanned six consecutive times respectively.

Fig 3.1 this was how set up for Nmap scanning was:



- The laptop was my computer running Linux or UNIX operating system. It was used for scanning the network. The Nmap command was installed on the laptop connected to the network switch.
- The Server A was powered by Linux operating system. This was an unpatched server and a few services were installed on it such as web-server, file server and so on.
- The Server B was also powered by UNIX operating system. This was a fully patched server with firewall and here too, a few services were installed on it such as web-server, file server and so on.
- All the three system were connected together by the help of the network switch.

Table 3.4

Network scanning using Nmap	Devices and services detected
1st sample experiment	All active hosts and services
2nd sample experiment	Printers, switches and routes operating in the
3rd sample experiment	address space by the port scanning tool
4th sample experiment	Any device that has a network address or was
5th sample experiment	accessible was been identified.

From table 3.4, the Network scanning like the Network Mapper (Nmap) was used. This was to scan through their network system to find all potential services on the network. Because of the weaker firewall, the network Mapper was able to scan and revealed a list of all active

hosts and services, printers, switches and routes operating, and any device that has a network address or was accessible on the network was been identified.

Also, a network scanning was conducted using the Cain and Abel software on a laptop to find out which application was running on some of the ports on the network system and the web-based applications. The reason for conducting this scanning was to scan on wireless networks and try to hack in and enabling sniffing on switched LAN's by hijacking IP traffic of multiple hosts at the same time. Also, it could try to decrypt database files those of database, Excel, Ms Access, FoxPro, etc. The devices used for this experiment was a laptop, Cain and Abel software which was installed on the laptop and it was connected to the network system of the bank. This scanning was done for just twenty times on the network server.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted four consecutive times respectively. And the sample results are shown below in the table.

Table 3.5

Network scanning using Cain & Abel software	Devices and services detected
1st sample experiment	TCP port 80 was identified
2nd sample experiment	The host that was running on a web-server.
3rd sample experiment	The web server products that was installed.
4th sample experiment	The vulnerabilities of the software
5th sample experiment	application were also identified.

Again, another network scanning software was used which was the Cain and Abel software to scan the network system. This was to check how strong their firewall was. So from the table, the numerous tests that were conducted shows how the TCP port 80 was identified, the host that was running on a web-server and web-server products installed and the vulnerabilities of the software applications was identified like the Remote code execution, SQL Injection, Format String Vulnerabilities, Cross Site Scripting and Username Enumeration.

Furthermore, LanGuard software was used. The reason for using this software was to analyze the state of the network security, what the risks are, how exposed the network was and how to take action before it would compromised. Also, to get a complete picture of what applications were installed, the hardware on the network, the state of security applications, what ports were opened, any existing shares and services running on the machines. The LanGuard

software was installed on their database server and tried changing and adding some amount of money on a person account, like a customer deposited GH¢ 3,000 in his or her account and I tried to change the amount to GH¢8, 000 on the bank database system. This experiment was conducted for twenty times.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted four consecutive times respectively. And the sample results are shown below in the table.

Table 3.6

LanGuard software on Database server	Number of modifications on customers account
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	0

From the table 3.6, LanGuard software was used on the database server of the bank. This was to try and make changes on a customer's deposited accounts. But upon all the numerous tests using this software on the bank's database system, not even a single test was successful.

Finally, a 32-bit Cyclic Redundancy Check (CRC) was used. This reason for using this checker was to make changes or modify a file or account of a customer in the bank's database system, like a customer deposited GH¢3, 000 in his or her account and tried to change or modify the amount to GH¢8, 000. So the 32-bit Cyclic Redundancy Check was installed on a laptop and connected to the database system of the bank. This experiment was done for twenty times.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted four consecutive times respectively. And sample results of this experiment are shown below in the table.

Table 3.7

Using the 32-bit Cyclic Redundancy Check	Number of modifications on customers account
1 sample experiment	GH¢10,000 was changed to GH¢ 15,000.
2 sample experiment	GH¢5,000 was changed to GH¢ 8,000.
3 sample experiment	GH¢6,000 was changed to GH¢20,000.
4 sample experiment	It was successful
5 sample experiment	It was successful.

From table 3.7, the 32-bit Cyclic Redundancy Check method was used. This was used to modify a file or an account of a customer in the bank's database system. Based on the number of tests that was conducted on this method, the outcome was these, GH¢10,000 was changed to GH¢ 15,000, GH¢5000 to GH¢8000, GH¢6000 to GH¢20,000 and subsequent ones. So it was detected that although, the software on the database system was powerful, the 32-bit Cyclic Redundancy checks software was more powerful that allowed easy penetration on their database system.

3.4.1 External Testing and their End Results.

The end results of the penetrating test conducted on the external network perimeter on the bank were as follows:

Once the password hashes are obtained, an automated password cracker on a laptop rapidly generated hashes and matches a password on the database of the bank's system. This was possible due to the dictionary attack software downloaded from the internet that covers most major and minor languages, names, etc.

Although, a change and substitution was made a worker's password, it could not get accessed to the bank's system, because it could not match any password in the database system.

The scanning of the network system provided a comprehensive list of all active hosts and services, printers, switches and routes operating in the address space scanned by the port scanning tool, that was any device that has a network address or was accessible to any other device.

The Cain and Abel software identified TCP Port 80 which was opened on a host, and it was meant that the host was running on a web server and that was their web-based applications. And also identifying which web-server product was installed should be critical in identifying the vulnerabilities of their software applications.

The LanGuard software was not strong enough to penetrate to the database system of the bank, so the customer's account was not able to be changed.

Due to the strong nature of the 32-bit Cyclic Redundancy Check (CRC) the customer's deposited amount was able to change from GH¢3, 000 to GH¢8, 000 in the account

3.4.2 Summary of Tests

Based upon all the tests that were conducted under the external testing on the bank premises, it could be concluded that, the password cracking method like the Network sniffer could not be used to penetrate or have access to the bank system as shown in table 3.2.

Also, the Hybrid attack cracking method could not be used to modify or make any changes on usernames and passwords so as to have accessed to the server of the bank as indicated in table 3.3.

Again, the Network Mapper software for scanning through the network system was powerful, so the institution needs strong firewalls which would not permitted any scanning to take place or intruder unless permission is been granted which was indicated in table 3.4.

Also, the Cain and Abel software to scan the network system was powerful, so it was deduced that the firewall on the network system was not stronger enough. The bank system needs stronger and powerful firewall which would detect any intruder who invaded the banking system as indicated in table 3.5.

The LanGuard software which was used on the database server was not successful. So it shows that the software on the bank's database server to prevent intruders was so strong that no matter the number of times an intruder attempts to modify or make any changes without access permission it could not be possible as shown in the table 3.6.

Lastly, the use of 32-bit Cyclic Redundancy Check method on the bank's database system was successful. It was therefore recommended that stronger checksum such as the SHA-1should is installed on the organization's database system to ensure the integrity of data that would be stored in the checksum database of the bank system as shown in the table 3.7.

3.4.3 Tools To Implement a Sniffer on the WLAN:

Table 3.8 Tools to Implement Wireless Attack (MITM)

	Tools	Function	Download
Software			
1	Nmap		www.nmap.org
2	Cain & Abel	Sniffer tool	www.oxid.it/cain.html
3	Wire shark Network Analyzer	Network Packet Analyzer	www.wireshark.org
Operating System			
4	Backtrack 5 Linux	Hacking and penetration tools	
5	PHLAK Linux (optional)	Hacking and penetration tools	
7	Windows 7	With hacking and penetration tools	
Hardware			
4	Laptop (with Wireless Card)	Computer for the activity	
5.	Outdoor Router/Access point	As rogue access point (RAP)	
6.	Wispy	Spectrum analyzer for survey	

A Man-In-The-Middle attack, often abbreviated as MITM, was accomplished by inserting a third party into a two party communication and hiding that fact from the original two participants. The Man- In-The- Middle then gets access to the data and could secretly alter it for his own purposes.

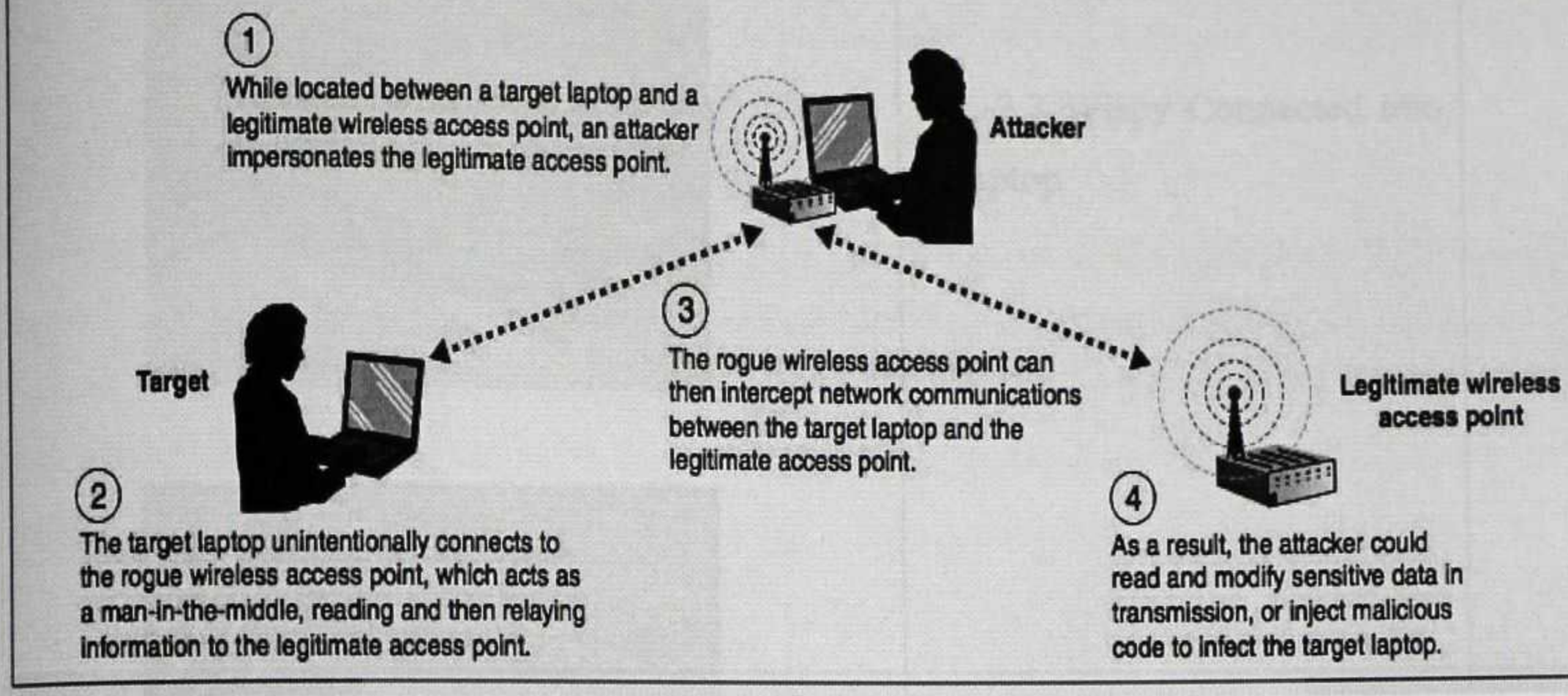


Fig 3.2 Man-In-The-Middle Attack

In wireless networking, the MITM scheme was implemented in a number of ways. One was to operate a rogue access point resembling a legitimate wireless hotspot/base station. Often the real access point was jammed or blocked while the rogue, with the same SSID, was in the clear with a strong signal. Another method was to break a target's connection and lure the target's hardware into reconnecting to the middleman. In this case the middleman has faked the access point MAC address.

These attacks are not limited to wireless networks; there have been cases of proxy faking security for SSL/HTTPS communications. It means that banking, secure email, and other sensitive connections have been compromised by man in the middle schemes. The intent was to access the branch wireless network perimeter as a test, to assess the extent of data security within the network.

3.4.4 Proposed Procedure:

The first task was to survey the entire length and breadth of the branch building in order to map out available wireless signal strength. This was done by installing the USB Wispy into the laptop and uses its accompanied software (Chanalyzer) to do wireless signal survey and scanning. After mounting signal survey for a while, directing my antennas towards direction of the branch's antenna by which it connects to another branch or regional head office, I carefully monitor for presence of signal.

Fig. 3.3 Wispy Connected into a Laptop

Fig. 3.4Chanalyzer Software showing various properties of wireless signal identified.

With presence of wireless signal I applied Aircrack (available in the Backtrack Linux OS) to intersect pre-shared keys within the target's wireless network.

There are two threats that I can demonstrate by this technique:

i. Phishing

ii. Snooping on sensitive data.

3.4.4.1 Phishing

Phishing is the act of attempting to acquire information such as username, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

In this technique, a wireless RAP was set up on a laptop computer and broadcast SSID so that wireless-enabled devices within the perimeter of the branch in the RAP's vicinity would automatically connected to my RAP instead of the branch's regular wireless service.

So my RAP was given an SSID of the branch's network in order to make it seem as genuine as possible to a casual user who might happen to glance at my RAP's SSID.

Some of the tests conducted using these phishing techniques on the branch's network were as follows:

First of all, a message was formulated containing the information "You can earned GH¢3,000 to GH¢5,000 a month as an accountant, database administrator or an employee with a financial institution background. If you want to apply for any position in this newly established financial institution, fill the form below about your personal and employers details. So I sent this as e-mail to the bank's website. The reason for sending this e-mail to bank website was to test the employee who would log in and provided his or her credentials or details easily. This message was sent for twenty times to the bank's website. The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted four consecutive times respectively. And the sample results of this experiment are shown below in the table.

Table 3.9

Formulating of false message as E-mail to bank website	Number of customers responded to E-mail
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	0

Fromthe table 3.9, e-mail message was sent to the bank's website asking the workers to apply for any position in a newly established financial institution, by filling a form that was provided alongside it, being a bank accountant, database administrator or an employee of any bank. But with the numerous e-mail messages being sent to the bank's website none of them proved futile.

Secondly, "You have won GH¢10,000 from the MTN loyal promotions" was formulated to the bank customers who are having E-banking transactions with the bank, so fill this form below and provide the accounts details in which the amount would deposited in it. This experiment was conducted to test how the customers of the bank can easily provided their information to outsiders. Also, this was done by sending text messages to the customers on E-banking transactions with the bank and provides feedback to the sender's number. The text messages were sent five times to each customer on the E-banking which were about eighty customers. The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted five consecutive times respectively. And some sample results of this experiment are been shown below in the table.

Table 3.10

MTN loyal Promotion to their Customers	Number of Customers Uploaded the Form
1st sample experiment	20
2nd sample experiment	35
3rd sample experiment	42
4th sample experiment	50
5th sample experiment	55

Again, from the table 3.10, false loyal promotions method was used and under this experiment the first sample tests shows that twenty of the customers of the bank that received the e-mail messages in their mail account filled the form and provided the full details of their credentials on the attached form with the e-mail messages. The second sample tests indicated that thirty-five customers filled the form and provided the full details of their credentials on the attached form with the e-mail messages received. The third sample tests also shown that forty-two of the customers filled the form and provided their full details of their credentials on the attached form alongside the e-mail messages received. The fourth sample tests also indicated that fifty customers of the bank provided the full details and their credentials on the attached form been sent to them. And lastly, the fifth sample tests shows that fifty-five of the branch customers provided the full details and credentials on the form been sent to in their various e-mail accounts.

Thirdly, a fake phishing website was created. The reason being that, to deceive users and exploits the poor usability of current web security technologies. Also, to trick the recipient into revealing confidential information by confirming it at the phisher's website and gather personal and financial information from recipients. So I sent e-mail messages to the

customers of the bank through their e-mail contacts, indicating, if you deposited an amount of GH¢500 within a month, you will earned multiples of interest you deposited thrice or twice of the money within the same month. If you are interested in saving with this Savings and Loan Company then visited this website for more details. This e-mail message was sent three times each to all the customers of the bank branch.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted three consecutive times respectively. And some of the sample results are shown below in the table.

Table 3.11

Creating of fake Phishing website	Number of Customers visited the website
1st sample experiment	0
2nd sample experiment	6
3rd sample experiment	16
4th sample experiment	24
5th sample experiment	40

From the table 3.11, the creation of a fake phishing website to the customers on their various e-mails accounts. Stating the earning of multiples of interest when deposited an amount of GH¢500 within a month in their accounts. So the first sample tests conducted was not successful due to network problems facing the bank, but the second sample tests conducted was successful because six customers visited the website provided alongside the e-mail messages sent to them. The third sample tests conducted under this method shows that sixteen customers visited the website provided alongside the e-mail messages. The fourth sample tests conducted also indicated that twenty-four customers visited the website attached to the e-mail messages sent to them. Lastly five sample tests under this method shows that forty customers visited the website attached to the e-mail messages sent them in their e-mail accounts respectively

Furthermore, the "Letter-head" of the bank was scanned and used it as an e-mail spoofed application. The reason for this e-mail spoofed application was, to acquire the login password and aimed at convincing the customers to give up their login or credit cards information. So I used the e-mail spoofed application and sent e-mail using the link of the phishing website I created to all the customers of that bank branch having an online banking with the bank. Stating that the bank was recruiting workers for their various networked branches so interested customers can apply by filling a form and providing their personal details, account numbers, credit card numbers and any important information that would be needed. This e-

mail was sent to all the bank branch customers. The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted five consecutive times respectively. And some of the sample results after the experiment were shown below in the table.

Table 3.12

Using E-mail spoofed application	Number of customers applied for vacancy
1st sample experiment	28
2nd sample experiment	45
3rd sample experiment	65
4th sample experiment	82
5th sample experiment	94

Moreover, from the table 3.12, an e-mail spoofed application method was used. This was to sent e-mail using the link of the phishing website to the customers, on how the bank were recruiting new workers for their various branches so interested customers should applied by filling a form attached to the e-mail messages sent to them. So the first sample tests conducted under this shows that twenty-eight customers applied for the job vacancy by provided their personal details, accounts numbers, credit card numbers and any important information about themselves. The second sample tests conducted also shows that forty-five customers applied for the job vacancy by filling the attached form alongside the e-mail messages they received. The third sample tests conducted also indicated that sixty-five of the customers applied for the job vacancy. The fourth sample tests conducted indicated that eighty-two customers applied for the job vacancy and lastly, ninety-four customers applied for the job vacancy by filling the form attached to e-mail messages sent to them.

Also, e-mail was sent to all the workers of the Adum branch of the bank through the bank e-mail account, which stated the bank needed to upgrade their system and needed all the workers of the bank to log into the provided link through which they had to fill the form provided. It was also stated that those workers that do not log in might not be able to access any information from the bank system. The reason why this experiment was conducted was to know how the workers would react to any e-mail they receive and how they could reveal their identity to the general public. The e-mail messages were sent to all the workers e-mail account.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted five consecutive times respectively. And the sample results are shown below in the table.

Table 3.13

E-mail message upgrading bank system	Number of workers that filled the form
1st sample experiment	5
2nd sample experiment	15
3rd sample experiment	18
4th sample experiment	23
5th sample experiment	28

Again, from the table 3.13, e-mail messages were sent to various workers e-mail accounts respectively. Stating the needed to upgrade the bank system, so all the workers should provide all their details on the attached form provided alongside. So the first sample tests conducted shows that, five workers filled the attached form for upgrading. The second sample tests conducted shows that, fifteen workers filled the attached form for upgrading. The third sample tests conducted indicated that eighteen of the workers filled the form for the upgrading whiles the fourth sample tests conducted shows twenty-three workers filled the attached form for the upgrading. And lastly, the fifth sample tests conducted shows that twenty- eight workers filled the form for the upgrading of the bank's system.

Moreover, online purchases of goods like cars, phones and accessories, second-hand clothes and other items at moderate price tags on them was created using the bank's website. Then ordered that, any customer of the bank could purchased any of the items by using their credit cards and stating how the payment terms could be, either by visa cards or cheques. The reason for this experiment was to have access to vital information about customer's details and their credentials.

Table 3.14

Online Purchases of Goods and Services	Number of customers that applied
1st sample experiment	31
2nd sample experiment	45
3rd sample experiment	65
4th sample experiment	80
5th sample experiment	85

Also, from the table 3.14, an Online purchases of goods and services method was used. Under this method some goods were listed with their price tags attached to them for customers to purchase them using the credit cards or cheques. And if it were a credit card, the

numbers should be provided on a form provided. So the first sample tests conducted saw thirty-one customers stating their interest in the purchasing of the goods, the second sample conducted also shows that, forty-five customers stated their interests in the purchasing of the goods, whiles the third sample tests conducted shows that, sixty-five customers showing their interests in the purchasing of the goods. The fourth sample tests conducted indicated that, eighty customers stated their interest in the purchasing of the goods. And lastly, the fifth sample tests conducted revealed that, eighty-five customers stated their interest in the purchasing of the goods

Again, an e-mail message was sent to the customers who were having online bank transactions with the bank. Stating that, the bank was upgrading their systems for effective services to them, so they should fill a form and added any additional information that needed to be added to their old credentials on the form being sent to them, using the fake "Letterhead" of the bank. This was done by sending e-mail message to all the customers e-mail account and also to trick the recipient into revealing confidential information by confirming it on the fake "Letterhead" form. This e-mail message was sent to all the customers of the bank branch.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted on three consecutive times respectively. Some of the sample results of this test were shown in the table below.

Table 3.15

E-mail message to customers on Online banking transactions	Number of customers that filled the form for upgrading
1st sample experiment	23
2nd sample experiment	48
3rd sample experiment	64
4th sample experiment	73
5th sample experiment	89

Again, from the table 3.15, e-mail messages were sent to customers concerning their Online banking transactions with the bank. Stating that the bank was updating their system for effective services for their customers. So the first sample tests were successful, the second sample tests conducted saw that one-third of the customers filled the upgrading form that was attached to the e-mail messages which were sent the customers. The third sample tests

indicated that two-thirds of the customer's population filled the upgrading form. Then, lastly all most all the customers filled the upgrading form.

Also, a message as "I LOVE YOU" was created on the bank's website for all the employees to read, indicating a man in my mid-thirty's and wanted a nice lady to marry, so the lucky lady should sent her pictures and credentials of place of work to this e-mail account kdb95@yahoo.com. The reason for this experiment was to take advantage of people to obtain information with or without the use of technology. This test was conducted for twenty rounds on the bank's website.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted four consecutive times respectively. And some sample results of the experiment are shown in the table below.

Table 3.16

"I Love U" message on bank's website	Number of ladies visited the website
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	2
4th sample experiment	5
5th sample experiment	7

Furthermore, from the table 3.16, a message was posted on the walls of the bank's website, which reads "I Love U", indicating a man looking for a lady to marry, so the lady should sent her credentials and pictures to provided e-mail account. The first and second sample tests were not successful the reason being that, most of the ladies thought that it was authentic and relevant but when the messages kept on sending to the bank's website then they started responding to the messages that was why the third, fourth and fifth sample tests proved some results where two, five and seven ladies of the bank sent their pictures and provided their credentials as a reply to the messages respectively.

A fake version of the branch's wireless login page was created. The reason for conducting this experiment was to deceive users and exploits the poor usability of current web security and acquired the login passwords and usernames. Using a freely available tool known as AirSnarf, which was installed on laptop and connected to the bank's database system and a link were created from the laptop and the database system, such that, if a user attempts to log in at that page by typing his/her username and password, I would be able to capture

those details in a file and directed the user to another web-page that would display the text " The Page cannot be displayed" on the laptop. This experiment was done for three consecutive days on the bank's database system.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted three consecutive days respectively. And some of the sample results of this test are shown in the table below.

Table 3.17

Fake version of bank's wireless login page	Number of users that logged in
1st sample experiment	3
2nd sample experiment	6
3rd sample experiment	10
4th sample experiment	12
5th sample experiment	14

Again, from the table 3.17, a fake version of the bank's branch wireless login page was created. So when a user attempts to login at that page those details are captured in a file and directed the user to another web page that would display the text "The Page cannot be displayed". So the first sample tests were successful. And the second sample tests shows that, six usernames and passwords were captured when some of the workers were logging into the system. The third sample conducted also shows that ten usernames and passwords were captured when some of the workers were logging into the system. Then, the fourth sample tests conducted indicated that, twelve usernames and passwords were captured when users were logging into the system. And the lastly sample tests also revealed that fourteen usernames and passwords were captured when users were logging into the system.

Also,using another freely available tool known as TreeWalk downloaded from the internet and installed on to the laptop. The reason why this experiment was conducted, was to by-pass the bank's ISP's and DNS server in the business environment and also to mail a recipient which has been doctored to look as though it has come from a particular sender, when in reality it has come from someone completely different. I poisoned the cache of the rogue laptop so that all attempts to navigate to any web site loaded up my fake web-page. However, attempts to navigate to other URLs would work normally as intended, making it difficult for the victim to suspect any malicious activity. This software was used for five consecutive days on the laptop with a connected link to the main server of the bank.The 1st, 2nd, 3rd, 4th, and 5th, sample experiments were conducted five consecutive days respectively. Some of the sample results of this experiment are shown in the table below.

Table 3.18

The use of TreeWalk software	Number of users that logged in
1st sample experiment	3
2nd sample experiment	6
3rd sample experiment	10
4th sample experiment	12
5th sample experiment	14

The last method used under this phishing experiment was the use of TreeWalk software. So under this experiment all the tests conducted was successful the reason being that, with the help of the fake web page created, all attempts to navigate to any website will automatically loaded the fake web-page which made it difficult for any victim to suspect any malicious activity.

3.4.4.2Phishing Testing and the End Result

The end results of the tests conducted at the bank concerning the phishing attack on the network perimeter, out of the ten only six of them were successful. The test was more successful since it was a spoofed e-mail sent by using the "Letterhead" of the bank. From the post-testing survey, about70% of the victims indicated that they trusted the content of the e-mail because it was sent from the bank through the use of the "Letterhead".

Also, most of the workers of the bank believed that the e-mail was actually sent from the bank and they did not suspect any phishing activity. Few of them reported that they saw the wrong URL but still submitted their ID and password because they did not think the website was a fake.

Again, the customers believed that due to the numerous promotional sales and activities from their network providers MTN, the messages being sent to them was from the right sources, that was why they provided the information in a form of reply to the messages they received.

Lastly, the customers believed that with this numerous financial institutions advertisement about depositing GH100 in your account and within a month or two you would earned twice as the money you deposited, that was why they logged on to this unknown website.

3.4.4.3 Summary of the tests

Based upon all the phishing tests and experiment conducted, it was indicated that, it was not easy for the workers to be convinced by any money for them to move from one working place to the other as shown in the table 3.9 above.

Also, from all indications it was detected that, customers would provide any information about themselves and full details of their bank accounts, whenever a false promotional messages are sent to their various e-mail account and whether it would be coming from the right source or not as indicated in table 3.10.

Again, it was detected that, customers could provide any information about themselves and full details of their bank accounts, whenever a false messages are sent to their various e-mail account and whether it would be coming from the right source or not. So seminars and workshops should be organized for the customer of the bank to make enquires about any messages received from the bank concerning their personal information as shown in the table 3.11 above.

Furthermore, it was revealed that, because the "Letter head" was the same as the one from the bank, that was why most of the customers of the bank applied for the job vacancy by the filling the form and provided all their needed credentials on the form without been bothered to check for the originality of the application form been sent to their e-mail accounts respectively. Advice should be given to the customers concerning how their personnel information and credentials should be secret and confidential to them alone. And also, they should not expose their personal details to unknown sources as indicated in the table 3.12.

Moreover, it was realized that, not all the workers of that branch filled the form for the upgrading of the system, because they thought that their information were been provided to the bank's already whiles those who filled the form taught that it was a new development in the bank premises which was indicated in the table 3.13.

Also, it was revealed that, customers are easily convinced to provide their credentials when it comes to any monetary matters and which they could earned enough profit from it without checking the right source from which the information were coming from as indicated in the table 3.14.

Again, it was revealed that, almost all the customers of the bank branch provided their necessary information on the form given to them through their e-mail messages. And the customers usually do not check the source of the e-mail messages received in their e-mail accounts before providing any relevant information or filling any form, otherwise, their relevant information would be in the hands of intruders and hackers as it was shown in the table 3.15.

Also, it was indicated that, when ladies are pushed a bit they could revealed some information about themselves and the bank to a third party or an intruder as it was indicated in the table 3.16.

Lastly, it was revealed that, workers do not like complaining whenever there was any fault when logging in to the system that was why most of the usernames and passwords were captured as shown in the table 3.17 above.

3.4.4.4 Snooping on sensitive data

A freely available Ethernet sniffer application was run on the rogue laptop computer, which Iobserved all the network traffic of the laptop that was connected to the wireless network of the bank through my RAP. Then I profile the victim's network usage and activities, decrypt sensitive data or information.

Then, the Backtrack Linux was used which was still running on my laptop,and issued commands to instruct the kernel on the operating system to enable IP forwarding on the RAP laptop. This allowed me to intercept data that was intended for other clients, inspected it, and then passed it to the destination. Basically, I tricked the wireless router/access point into showing the packets first, and then passed them to their intended destination.

Next step, a Spoof was used to some ARP requests to trick other clients that may be connected to the RAP access point, then divulging their data. This was accomplished by using the "arpspoof" tool that comes with the dsniff toolkit to accomplish this. The spoofed ARP requests were set to constantly broadcasted.

3.5Internal testing Strategies

Securing data in any organization, especially financial institution, is a delicate balance of operational integration, cost and reason. Depending on the particular institution, financial institutions may have many different data exchange needs and requirements. A review of any data exchange initiative may uncover the need to encrypt data as it rests within storage, as well as encrypting data as it is in motion. Within these requirements may be several types of transactions, key management needs, encryption standards, compliance mandates and many other components that require consideration. Understanding the needs and the requirements was critical to matching them with the right solution.

Some of the internal testing strategies that were deployed on the organization are as follows: First of all, internal testing was conducted using a symbolic links which was a file that points to another file and changes the permissions granted to a file. The reason for this experiment was that, some programs that need to handle symbolic links specially may identify and manipulated them directly. And also, to read or write to files named by a symbolic link which behaves as if operating directly on the target file. So the used "Man-in-the-Middle" attack method was used where my rogue access point laptop was set up between the Adum branch and Knust branch of the bank. This was to intercept a transmitted data from a customer's account on one branch of the bank to another customer's account of another branch in the database system in the bank's network system. This test was conducted for twenty times and some of the sample results of this test were shown in the table below.

Table 3.19

Using symbolic links	Permissions granted to Files
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	1

From the table 3.19, the Symbolic links method was used, with the help of the Man-in-the-Middle attack method. Based on the numerous tests under this method, only a few were able to be successful, the reason being that, at first the legitimate access point was not able to detect by the target laptop till the link were able to get through.

Then again, posed as one of the tellers in the bank's counter or desk, and experiencing difficulty in logging to the main server. So a call was made to the organization's help desk to fix the problem. So I asked for the reset password and login ID and other credentials in order to gain information on the bank's server, network or host. So as to obtain a login ID and credentials, or a password to reset. The reason for test was to convince the IT department to give up their login codes and gather personal and vital information from the department. This test was done for twenty times using different names of the tellers of both branches of the bank and some of the sample results are shown in the table below. This was easily done by using the intranet connections between the network branches of the bank.

Table 3.20

False teller in the counter	Number of Tellers credentials revealed
1st sample experiment	Information about the main server was retrieved.
2nd sample experiment	3 teller's login ID was exposed.
3rd sample experiment	4 teller's password was also exposed.
4th sample experiment	Some codes to reset the machine were also reviewed.
5th sample experiment	4 teller's credentials on tellers were exposed.

From the table 3.20, a false impersonation teller in the counter was created. Based on the various tests under this method, it was revealed that any time a call goes to organization's help desk or the server room, information was exposed to the caller without asking the identity of the caller.

Also, posed as IT staff of the bank, and called a teller at the counter to provide her user ID and password to solve a problem being countered at the server room. The reason for this experiment was to verify if the employees of the bank would voice out their credentials or personal details in the bank anyhow and also acquire their login passwords and usernames so that the intruder could took over their account. This test was easily done by using the telephone lines internally to call the tellers frequently and on several occasions which lasted for one week. Some of the sample results of this experiment were shown in the table below.

Table 3.21

Posing as IT staff of the bank	Number of Tellers' Information exposed
1st sample experiment	1 teller provides her username.
2nd sample experiment	3tellers provided their usernames and passwords.
3rd sample experiment	4tellers provided their username, ID, and passwords.
4th sample experiment	7tellers provided their username, ID, and passwords.
5th sample experiment	10 tellers provided their username, ID, and passwords.

From the table 3.21, a false impersonation was created as an IT staff or employee of the bank. So based on the various tests conducted under this method, it was indicated that any time a call comes from the server room to any teller in the counter or a staff in any office, the person humbly revealed his or her identity and credentials to the caller without asking whom the caller was and if truly the caller was an employee of the bank or not.

Again a conversation was conducted as a member of the IT staff and some of the workers of the bank on how they transmitted data from their end to the other branches of the bank. This conversation were conducted among the workers so as to detect how they could revealed or exposed secret and confidential report or information about the bank to a third party or a close friend of his or her. Also, to find out how they could abide by the rules and regulations or the code and ethics of the banking institution even when they were attempted by a third party in a bribery form. So a question of this sort were asked, for instance, if you wanted to send this amount of money GH¢20, 000 to another branch account, how would you do it? These conversations were conducted thirty times with different workers of the two branches of the bank and some of the sample results of this test were laid in the table below.

Table 3.22

Conversations with IT staff and some workers.	Responses from number of workers
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	2

From table 3.22, some conversations were held with the IT department staff and some workers of the bank branch. It was revealed that, most of the workers do not know how data or information were been transmitted from one branch of the bank to the other, but a few which was two of them knew how the transmission were been done between network branches based on the numerous conversations held with the workers. So it was revealed that through conversations with some of the workers of the bank, important and confidential information could be in the hands of an intruder or a third party outside the bank premises.

Also had a face-to-face interaction with all the members of the IT department, which was a one-on-one interaction on how they encrypted their data or information and also decrypted their data from their networked branches.This interaction were conducted among all the members in the IT department of the Adum branch of the bank, so as to detect how they could revealed or exposed secret and confidential report or information about the bank to a third party or a close friend of his or her. Also, to find out how they could abide by the rules and regulations or the code and ethics of the banking institution even when they were attempted by a third party in a bribery form. This interaction experiment was done four times with each worker of the department and some of the sample results were as shown in the table below.

Table 3.23

Face-to-Face interaction with IT department	Responses from IT department workers.
1st sample experiment	0
2nd sample experiment	0
3rd sample experiment	0
4th sample experiment	0
5th sample experiment	1

Again, from table 3.23, Face-to-Face interactions were held with the staff of the IT department. Upon all numerous the interactions and discussions with the IT staff, it was indicated that, none of them were ready to reveal any information concerning how data were encrypted before sending and how data were decrypted when received. But only one of the staff reveals how data were been encrypted and decrypted before and after transmission. This was achieved due to the closeness of me to the worker. So based on the closeness of a worker with a third person outside the bank could also leaks some salient information about the bank to the hands of an intruder.

Furthermore, a Trojan Access Point method was conducted between the Adum branch and Knust branch of the bank networked branches. The reason was attempting to gain unauthorized access to the computer system and manipulate data been transmitted across and was done in addition with the Man-in-the-Middle attack method which was set up early for other experiment. So the Adum branch which was the targeted station receives a stronger signal from my Trojan Access Point than it received from the Knust branch. So the Adum branch worker selected my Trojan Access Point because of the stronger signal, and then authenticates and associates with it. This test was conducted for just three days and some of the sample results of it were shown below in the table.

Table 3.24

Using the Trojan Access Point Method	Outcome of the experiment
1st sample experiment 2nd sample experiment 3rd sample experiment 4th sample experiment 5th sample experiment	Due to the connection of TAP to the system that collects the IP traffic for analyses, it then transmitted all the frames to the Adum branch, so the Knust branch does not recognized the attack that has taken place. So user's password, network access that compromises the user's system which gave my access point system was denied.

Again, some observations was conducted on some of the workers when they were typing their usernames and passwords, this test was done easily by intentionally chatting with these workers when they were turning on their computers and logging into the main server of the bank and by going through their personal objects, diaries and also reading all small pieces of paper or sticky notes attached to their monitors. The reason for this test was to ascertain why people got accessed to other employee's accounts without their notification or approvals. And these tests were conducted five consecutive times on each of the workers selected and some sample outcomes were laid in the table below.

Table 3.25

Observation from the bank workers.	Responses from number of bank workers.
1st sample experiment	5 of the workers wrote their passwords on sticky notes.
2nd sample experiment	3workers wrote their passwords and usernames on their diaries.
3rd sample experiment	3 workers were noticed when typing their passwords.
4th sample experiment	6 workers used their nicknames as their passwords.
5th sample experiment	8workers used their own names as passwords.

From the table 3.25, an observation was made on the bank workers. It was observed that, five out of twenty of the workers had written their passwords on sticky notes behind their computers which they were using. Three out of twenty of them also wrote their passwords and usernames on their diaries which they have been using. And a little care been paid, three out of twenty workers passwords were noticed when they were typing them. Six out of twenty of the workers also used their nicknames as their passwords, and eight out of twenty workers used their own names as passwords.

The Kevin Mitnick technique was also one of the methods used. The reason for using this method was to use social engineering to obtain the name of the target computer system and the commands used by agency employees to obtain protected taxpayer information and also to take advantage of people to obtain information with or without the use of technology. So I called the secretary to the branch manager and said" Hi, this is Mr. Kwaku Duah from IT department, we were having problems within the network system and they appeared to be coming from your machine. Can you please give me your password and user' name?"So that we can rectified the problem. This test was conducted twenty times with the secretary and other departmental secretary and personnel and some of the sample results were shown below in the table provided.

Table 3.26

Using Kevin Mitnick technique Method	Number of Workers' credentials revealed.
1st sample experiment	1 teller provided his credentials.
2nd sample experiment	2 tellers provided their credentials.
3rd sample experiment	4 workers also provided their credentials.
4th sample experiment	Customer's service personal also provided his credentials.
5th sample experiment	The Accountant also provided his credentials.

From the table 3.26, a method called Kevin Mitnick technique was used. So based on the various tests conducted, two of the tellers provided their credentials to the call that comes from the IT department, four of the workers also provided their credentials to the call that comes from the IT department. Also, the Accountant and the Customers' Service Personal also provided their credentials to the calls that come to their various offices. So after the conducting of the experiment, it was revealed that, some of the employees of the bank could just voice out any salient and confidential information to any intruder or a hacker by just a call to their intranet or internal communication system on their various offices within the banking premises.

Finally, I removed a hard disk from the system unit in one of the machine of the workers at the IT department and connected it to my laptop to retrieve information from it. The reason for experiment was to check whether vital information about the bank was kept on the computers within the IT department or on the remote back-up server of the bank. So five hard disk were removed from the computers within the IT department and some of the information found on them was listed in the table below.

Table 3.27

Removal of Hard disk from the system unit	Outcome of the experiment
1st sample experiment	Salient information was retrieved from the hard disk like the various employees in the bank, their usernames, passwords and names of the bank workers.
2nd sample experiment	
3rd sample experiment	Also, how to solve the network problem when the links and system were slow in transmission.
4th sample experiment	
5th sample experiment	

Lastly, from the table 3.27, was the removal of the Hard disk from the system unit in the IT department. Based on this, some salient information was retrieved from the hard disk like the various employees in the bank, their usernames, passwords and names of other workers from the bank. And also, how to solve the network problem in the bank when the links and systems were slow in transmission. So based on this, it was advisable to save all salient and confidential information on their back-up system then leaving them on personal computers at their various offices. And also, deletion of important information from the computers at the IT department should be done always or any time a worker finished working with it.

3.5.1 Internal Testing and the End Result

The end results of the internal testing I conducted on the network perimeter of the bank institution were as follows respectfully:

A customer's accounts which were supposed to be credited were diverted to another customer's accounts through the help of the symbolic links program on my laptop through the use of the Man-in-the-middle attack.

The information on the main server was reviewed that was, the teller's login ID, password and credentials and also the codes for the reset of the machine.

The teller at the counter provided all her User name, ID and password for the problem to be solved without any second taught it.

About ten workers of the bank that was engaged , only two tellers were able to tell how they does their transmission, but the rest of the workers does not have any idea on how an amount were transferred from the bank to its sister branch.

Only one of the members out of the fifteen staffs on the IT department shown me how to decrypted and encrypt their before and after transmission has taken place, this was due to the fact that I was so closed to him, that was why he reveals the information to me.

Due to the connection of Trojan Access Point to the system that collects the IP traffic for analyses, it then transmitted all the frames to the Adum branch, so the Knust branch does not recognized the attack that has taken place. Because of that I got the user's password, network access and compromise the user's system and gave my access point system root access.

Out of the fifteen workers I observed, I got five of them written their passwords on sticky notes attacked to their monitors. And three out of them, I was able to notice their passwords when typing them.

The secretary to the manager happily supplied me with her user name and password without thinking twice.

Some salient information were retrieved from the hard disk like the various employees in the bank, their names, usernames and passwords, and how to solve the network problems when their links and systems were down and slow in transmitting.

Furthermore, I reviewed encryption solutions specifically for data in motion by which a mimic an attack on the internal network by a disgruntled employee or an authorized visitor having standard access privileges. The focused was to understand what could happen to the data in motion, if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific data or resources within the branch's network.

3.5.2 Summary of the tests

Based upon all the numerous tests conducted under the internal testing, it was revealed that, using the symbolic links methods and with weaker firewall, an intruder could penetrate into the database system of an organization as it was indicated in the table 3.19.

Also, using a false teller method in the counter, it was revealed that, any time a call goes to organization's help desk or the server room, information was exposed to the caller without asking the identity of the caller as shown in the table 3.20 above.

Again, impersonating as IT staff of the bank, it was indicated that, any time a call comes from the server room to any teller in the counter or a staff in any office, the person humbly revealed his or her identity and credentials to the caller without asking whom the caller was and if truly the caller was an employee of the bank or not as shown in the table 3.21.

Furthermore, using discussion and conversation methods, it was indicated that, through conversations with some of the workers of the bank, important and confidential information could be in the hands of an intruder or a third party outside the bank premises as shown in the table 3.22.

Again, using Face-to-Face interactions method, the closeness of a worker to a third person outside the bank premises could also leak some salient information about the bank to the hands of an intruder as it was indicated in the table 3.23.

Also, using the observation method, it was revealed that, most of the workers do not know how to formulate a good and strong passwords and usernames for their various computers been used, which allows for easy guessing and accessed by an intruder into the computer system as shown in the table 3.25 above.

Moreover, using Kevin Mitnick technique method, it was revealed that, some of the employees of the bank could just voice out any salient and confidential information to any intruder, or a hacker by just a call to their intranet or internal communication system on their various offices within the banking premises which was indicated in the table 3.26.

Lastly, it was advisable to save all salient and confidential information on their back-up system, then leaving them on personal computers at their various offices. And also, deletion of important information from the computers at the IT department should be done always or any time a worker finished working with it as shown in the table 3.27.

I also specifically focused on products that help to secure end-to-end file transfers using common encryption standards. There were many point-to-point security products, such as Virtual Private Network or email security gateways. I reviewed the solutions that offered application-to-application types of secure file transactions which included secure EDI-based transactions, FTP, SSH, HTTPS and other means of end-to-end delivery.

In some form or another, these products allow workstations, servers or even web servers to provide a secure channel, and support common file transfer protocols in either a batch processing type of mode or by allowing users to perform self-service, on-demand transactions. They also control recipients via pushing and file-retrieval mechanisms. It was common that the data at rest within these transaction servers was encrypted as well, but my focused was on how the products help secured the remote file transfers. All installed applications might have come with manuals, brochures or some other form of literature. These were subjected to security review, to find out whether adequate security (or data encryption standard) has been insured in operation.

CHAPTER FOUR

4.0 FINDINGS FROM SOFTWARE TESTING

The above techniques and approaches could expose presence of any vulnerability, if it exists. However, should the system be highly secured, no data can be intersected, thereby concluding that the combined security measures were capable of providing adequate security for data in motion.

4.1 Encrypting Data for Network Transmission

Sensitive information that travels over an intranet or the Internet can be protected by encryption. Encryption was the mutation of information into a form readable only with a decryption key. Encryption was a powerful security mechanism because it could made decryption mathematically infeasible if one does not possess the decryption key. The secrecy of encrypted data depends on the existence of a secret key shared between the communicating parties. Providing and maintaining such secret key was known as key management. In a multiuser environment, secure key distribution may be difficult; public key cryptography was invented to solve this problem. The best encryption must address all communications with the database, including transmissions from clients and transmissions from middle tiers. It must also secure all protocols into the database.

Industry Standard Encryption Algorithms

Table 4.1 List of Industry Standard Encryption Algorithms

Algorithm	Characteristics
RSA Data Security RC4	Allows high-speed encryption for data privacy. By using a secret, randomly generated key unique to each session, all network traffic was fully safeguarded--including all data values, SQL statements, and stored procedure calls and results. The client, server, or both, could request or require the use of the encryption module to guarantee that data is protected.
Data Encryption Standard (DES)	Uses symmetric key cryptography to safeguard network communications. DES was required for financial institutions and many other institutions.
Triple DES (3DES)	Encrypts message data with three passes of the DES algorithm. 3DES provides a high degree of message security. However, it entails a performance penalty, the magnitude of which is dependent upon on the speed of the processor performing the encryption. 3DES typically takes three times as long to encrypt a data block as compared with the standard DES algorithm.

4.2 Secure Sockets Layer (SSL) Protocol

The Secure Sockets Layer (SSL) protocol was an industry-accepted standard for network transport layer security. SSL was supported by all currently available Web servers and Web browsers. It was also gaining acceptance for other protocols, including Lightweight Directory Access Protocol(LDAP) and Internet Message Access Protocol(IMAP). The SSL protocol provides authentication, data encryption, and data integrity, in a public key infrastructure (PKI).

SSL addresses the problem of protecting user data exchanged between tiers in a three-tier system. By providing strong, standards-based encryption and integrity algorithms, SSL provides system developers and users with confidence that data will not be compromised in the Internet. Unlike password-based authentication, which authenticates client to server only, SSL can authenticate server to client as well as client to server. This was a useful feature when building a Web-based three-tier system, since users often insists on authenticating the identity of an application Web server before they provide the server with sensitive information, such as credit card numbers. Technically, data in motion within network environment might be secured from unauthorized access if certain combinations of security measures have been instituted in place. Encrypting data for transmission with Secure Sockets Layer (SSL) Protocol was one of the best means of ensuring security of data in motion. This project attempts to use all tools available to intersect and decrypt data in motion to ascertain possibility of vulnerability.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.0 Conclusion

Data in motion means sensitive data traveling over private networks or the Internet, whether wired or wireless. There are multiple threats of disclosure of sensitive information on computer networks. The combination of increasingly complex laws and a dramatic increase in data losses makes data security compliance an urgent matter for corporate counsel. Breaches have resulted in the exposure of more than 250 million records and have caused businesses to incur substantial expense: by some estimates, the average breach costs more than $6.5 million. Aside from cost, breaches have also led to negative press and high profile investigations and lawsuits by federal and state enforcement officials and the plaintiffs' bar, and could irreversibly tarnish a company's image. There was an important lesson about security management in all this. The challenge for us lies in selecting the right tools for the job at hand and then not letting them get dull and rusty over time. Data was vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it. With the steady drumbeat of data breaches making headlines almost daily, it might seem reasonable to regard data breaches as an inevitable by-product of our connected world. Odds are its happening right now. The confidential data that runs your business washemorrhaging outside your organization and could be just minutes away from getting into the wrong hands.

Data leakage happens every day when confidential business information – customer or patient data, source code or design specifications, price lists, intellectual property and trade secrets, and forecasts and budgets in spreadsheets – leaves our company unprotected and goes outside the jurisdiction of our corporation. This uncontrolled data leakage puts your business in a vulnerable position. Once this data was no longer within your domain, your company

would be at serious risk. When cybercriminals "cash out" or sell this data for profit it costs your organization money, damages your competitive advantage, brand, reputation and destroys customer trust.

5.1 Recommendations

It was recommended that:

Financial institutions should implement an ongoing security process and institute appropriate governance for the security function, assigning clear and appropriate roles and responsibilities to the board of directors, management, and employees.

Financial institutions must maintain an ongoing information security risk assessment program that effectively:

- Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;
- Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and
- Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

Financial institutions should develop a strategy that defines control objectives and establishes an implementation plan. The security strategy should include:

- Appropriate consideration of prevention, detection, and response mechanisms,
- Implementation of the least permissions and least privileges concepts,
- Layered controls that establish multiple control points between threats and organization assets, and

- Policies that guide officers and employees in implementing the security program.

Financial institutions should have an effective process to administer access rights. The process should include:

- Assigning users and devices only the access required to perform their required functions,
- Updating access rights based on personnel or system changes,
- Reviewing periodically users' access rights at an appropriate frequency based on the risk to the application or system, and
- Designing appropriate acceptable-use policies and require users to agree to them in writing.

Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access. Institutions should:

- Group network servers, applications, data, and users into security domains (e.g., untrusted external networks, external service providers, or various internal user systems);
- Establish appropriate access requirements within and between each security domain;
- Implement appropriate technological controls to meet those access requirements consistently; and
- Monitor cross-domain access for security policy violations and anomalous activity.

Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should then use that information to update the risk assessment, strategy, and implemented controls.

Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should then use that information to update the risk assessment, strategy, and implemented controls.

Management should establish a few policies around the information they want to protect. Once the policy is created, employees should be notified and educated. Management should outline what data is to be protected, specifically where the data should not go and what will happen to them if the policy is violated. Employees should also be informed on why not following policies subjects the organization to unnecessary risks. They should be made aware and understand the negative publicity of data breaches.

Companies must be aware of this patchwork of laws and regulations and understand how it applies to their business operations.As the data security legal landscape changes rapidly, companies must stay on top of new and proposed laws that may affect their businesses. Many new laws have wide ranging impact and require significant advance preparation in order for a company to be in compliance with them when they become effective.

Companies must consider international data protection and security laws. A growing number of countries have substantive data protection requirements, and in some cases, breach notification requirements. Further, companies transferring data between countries must understand and comply with the growing number of laws regulating data transfers. For example, the European Commission (EC) Directive on Data Protection prohibits the transfer of personal data from the European Union (EU) to other nations unless certain privacy protection standards are met.

Intrusions caused by hackings and malware (software designed to infiltrate or damage a computer system without the owner's consent) can result in unauthorized access to private

information. Firewalls, virus protection software, and anti-spyware programs have been effective in thwarting many of these intrusions. Because cybercriminals constantly employ new techniques to circumvent protections and steal information, companies must stay vigilant by monitoring computer systems, updating anti-virus and anti-spyware software programs, and diagnosing and addressing potential vulnerabilities.

It is important for companies to periodically assess and update their data security policiesbecause technology is rapidly evolving, laws are changing, and business practices are frequently modified. Companies should review the adequacy of data security measures at least once a year, or whenever there is a material change in business practices that could implicate the security of personal information. Yet policies themselves are not sufficient if they are not enforced. Therefore, a company should conduct compulsory employee trainings on company policies and procedures, and should measure employees' meaningful compliance with them.

Many companies incorrectly believe that if a third-party contractor loses sensitive data belonging to the company, there are few or no implications for the company. In actuality, most of the burden of handling the breach will fall on the company. When dealing with contractors, therefore, there are a number of steps a company should take to ensure the protection of data. Security audits and contractual provisions requiring third parties to protect sensitive information are essential. Companies should also limit the personal information collected by contractors and limit the time contractors are permitted to retain such information. Further, businesses operating as third-party contractors should themselves assess their security procedures and make sure they are aware of their legal and contractual obligations.

Despite a company's best efforts to enact state-of-the-art privacy policies and procedures, data losses can and do occur. These incidents are often complicated and require time to investigate the circumstances of the breach, assess the nature of the risk, and determine what was exposed and whether notifications may be required. To avoid loss of valuable time, having a dedicated internal team in place and strong relationships with forensics firms and outside counsel are important measures. A well-conceived incident response plan can make the difference between a company making timely notifications, versus opening itself up to investigation or potential lawsuit.

By encoding information so that it is rendered unusable, encryption technology ensures that sensitive information cannot be misused. Encryption is a powerful data protection tool that is useful particularly for portable electronic devices (e.g., laptops, Blackberries) and sensitive data that is transferred electronically. The average breach is estimated to cost millions of cedis, so investing in encryption technology can be a cost-effective prophylactic measure.

REFERENCES

Bace, R. and Mell, P. (2006).NIST Special Publication on Intrusion Detection Systems. National Institute of Standards and Technology. California: Infidel, Inc.

Baker, W. et. al., (2011). Data Breach Investigations Report United States Secret Service.

Bonnette, C. A. (2003). Assessing threats to information security in financial institutions. GSEC Certification Practical Assignment, Version 1.4b - Option 1

Brunette, G., Nagappan R. and Weise J. (2012). Best Practices for Securely Deploying the SPARC SuperCluster T4-4

Burrows, M., Abadi, M., and Needham, R. (1990).A logic of authentication, ACM transactions on computer systems (TOCS), vol. 8, issue 1, pp. 18-36

Conklin, A., Dietrich, G., and Walz, D. (2004). Password-based authentication: a system perspective. Proceedings of the 37th Hawaii International Conference on System Sciences

Dhupar, V. (2010). Building a comprehensive IT security strategy, targeted attacks on intellectual property. India

Dynamically Segment and Isolate Cross-Platform Systems. Available at [http://www.centrify.com/directsecure/server-and-domain-isolation.asp]

Hodell, I. I. (1998). Privacy Act, Security, Data Networks and communications. Virginia: ABBE Publishers.

Ferraiolo, D. F. and Kuhn, D. R. (1992). Role based Access Control. 15th National Computer Security Conference, pp. 554-563.

Festa, P. (2011). Microsoft computer network hacked; FBI steps in, CNET News. Available at http://news.cnet.com/2100-1001-247716.html. (Accessed January 2011)

FFIEC (2006).Information Security Booklet. Virginia

Fletcher, J. (2012). Data Privacy Regulatory, Protection and Mitigation Considerations: Risk Control Technology Specialist.

Gelbstein, E. and Kamal, A. (2002) Information Insecurity, A survival guide to the uncharted territories of cyber-threats and cyber-security (2nd ed.)United Nations ICT Task Force and the United Nations Institute for Training and Research, United Nations United Nations.

Hack Wireless LAN Network and Grab the Passwords – Man in Middle Attack. Available at http://solvater.com/2010/06/hack-wireless-lan-network-and-grab-the-passwords-man-in-middle-attack/ (Accessed January 2011).

Herzog, P. (2003). OSSTMM WIRELESS 2.1. Wireless Security Testing Section Open-Source Security Testing Methodology Manual. Institute for Security and Open Methodologies. Available at http://www.isecom.org, http://www.osstmm.org.(Accessed January 2011).

Kapoor, S. (2006) Session Hijacking Exploiting TCP, UDP and HTTP Sessions, United States.

Kraemer, S., Carayon, P. and Clem, J. (2006). An adversarial viewpoint of human and organizational factors in computer and information security. University of Wisconsin

Lee, S. (2010) "What Is Data In Motion Encryption?" Available at http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/07/12/what-is-data-in-motion-encryption.aspx.(Accessed January 2011).

Mell, P. and Grance T. (2011).The NIST Definition of Cloud Computing: NIST Special Publication 800-145.

Mitchell, C. (2009). New ISO/IEC standard.

Mockli, D. (2012). Strategic trends, new developments in global affairs. Zurich: Center for Security Studies.

Mohare, R., Lanjewar, U. A. and Parekh, K. (2012). Design and Analysis of Strategic Business Information Security Control Mode Zenith International Journal of Multidisciplinary Research Vol. 2 Issue 6, June.DattaMeghe Institute of Management Studies, RTM Nagpur University.

Moteff, J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Congressional Research Service

NPCR Data Security Overview. Available at ftp://ftp.cdc.gov/pub/Software/RegistryPlus/Security/Security_Index.htm. (Accessed January 2011).

Payment Card Industry (PCI) Compliance Guide. Available at http://www.pcicomplianceguide.org/aboutpcicompliance.php (Accessed January 2011).

Ponemon, L. (2009). Fourth Annual US Cost of Data Breach Study, Benchmark Study of Companies.Ponemon Institute LLC, Research Department

Robinson, A. (1995). The story of writing.Thames& Hudson.

Schneier, B. (2010). "Data at Rest vs. Data in Motion.[Online]. Available at http://www.schneier.com/blog/archives/2010/06/data_at_rest_vs.html (Accessed January 2011).

Shi, J. et. al., (2012).Computer security, research reports.

Sundar, M., Pering, T., Light, J., and Want, R. (2003). Photographic authentication through untrusted terminals, IEEE Pervasive Computing, pp. 30-36

Tatanarg Banking Trojan Steals Zeus Data and More. Infosec Island Available at http://www.infosecisland.com/blogview/12252-Tatanarg-Banking-Trojan-Steals-Zeus-Data-and-More.html (Accessed January 2011).

Thomas, G. (2011). DGI Center of Information about Security Breaches.

Tomko, G. J., Borrett, D. S., Kwan, C and Steffan, G. (2009) SmartData: Make the data "think" for itself Data protection for the 21st century.

Turnbull, N. (2003). 'Foreword' in Calder, Alan and Watkins, Steve, *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* (2nd edn), Kogan Page

APPENDIX

LIST OF ABBREVIATIONS, ACRONYMS AND TERMS USED IN THE STUDY

DATA: Data consist of raw facts and figures - it does not have any meaning until it is processed and turned into something useful. Data comes in many forms, the main ones being letters, numbers and symbols.

INFORMATION: Information is data that has been processed in such a way as to be meaningful to the person who receives it.

LAN: Local Area Network is a collection of computers that share hardware, software, and data typically within an office or building.

WAN: Wide Area Network is a collection of computers that span the world or link computers across town.

MAC ADDRESS: A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model.

WI-FI: Wi-Fi is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN."

WDS: A wireless distribution system is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.

The notable advantage of WDS over other solutions is it preserves the MAC addresses of client frames across links between access points.

WEP: Wired Equivalent Privacy is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

WAP: Wireless Application Protocol is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones or cellular phones that uses the protocol.

STANDARD: A standard is a document. It is a set of rules that control how people develop and manage materials, products, services, technologies, tasks, processes, and systems. ISO IEC standards are agreements. ISO IEC refers to them as agreements because its members must agree on content and give formal approval before they are published. ISO IEC standards are developed by technical committees. Members of these committees come from many different countries. Therefore, ISO standards tend to have very broad support.

CONTROL: A control is any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

DOCUMENT: The term document refers to information and the medium that is used to bring it into existence. Documents can take any form or use any type of medium. The extent of your ISMS documentation will depend on the scope of your ISMS, the complexity of your security requirements, the size of your organization, and the type of activities it carries out.

INFORMATION SECURITY: Information security is all about protecting and preserving information. It is all about protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information.

INFORMATION SECURITY INCIDENT: An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of your information and weaken or impair your business operations.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS): An information security management system (ISMS) includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organizations use to manage and control their information security risks. An ISMS is part of a larger management system.

POLICY: A policy statement defines a general commitment, direction or intention. An information security policy statement expresses management's commitment to the implementation, maintenance, and improvement of its information security management system.

RISK: The concept of risk combines three ideas: it selects an event, and then combines its probability with its potential impact. The concept of risk is always future oriented: it worries about the impact events could have in the future.

RISK ANALYSIS: Risk analysis uses information to identify possible sources of risk. It uses information to identify threats or events that could have a harmful impact.

RISK MANAGEMENT: Risk management is a process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. Risk management includes all of the activities that an organization carries out in order to manage and control risk.

RISK TREATMENT: It is a decision making process. For each risk, risk treatment involves choosing amongst at least four options: accept the risk, avoid the risk, transfer the risk, or

reduce the risk. In general, risks are treated by selecting and implementing measures designed to modify risk.

THREAT: It is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system.

VULNERABILITY: Vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats

INFORMATION SECURITY EVENT: It indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.

ENVIRONMENT: The interactive, co-dependent state of the network in operation.

ETHICAL HACKING: A form of penetration testing originally used as a marketing ploy but has come to mean a pen test of all systems – where there is more than one goal, generally, everything is a goal

FIREWALL: The software or hardware tool for imposing an Access Control List (ACL) on a system or network

INTRUSION DETECTION SYSTEM (IDS): This tool is designed to monitor and sometimes stop attacks in action either passive or active, host-based or network based.

REMOTE ACCESS: This is defined as access from outside the location

ROUTER: A software or hardware device for routing packets

SOCIAL ENGINEERING: An active attack against processes

DATA-IN-MOTION: This term refers to data transmitted across a network. This data can be regarded as secure if both hosts are capable of protecting the data and a third party cannot eavesdrop on the communication

DATA-AT-REST: This term refers to data stored on computers, stored on storage devices, or being used by the data owner. It excludes data traversing a network. Examples include files or e-mails saved on a hard drive or server.

NIST: The National Institute of Standards and Technology is an agency of the US Department of Commerce.

IPSEC: Internet Protocol Security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

HACKER: A clever person, who has a natural curiosity, likes to know how things work and is interested in circumvention techniques or exploiting processes to see what happens.

PENETRATION TEST: A security test with a defined goal which ends when the goal is achieved or time runs out.

VULNERABILITY TEST: A test for services, open ports and known vulnerabilities.