EFFECTIVE INFORMATION SECURITY STRATEGY TO PREVENT NETWORK INTRUSION IN NIGERIAN BANKS

By

ZECHARIAH OLULEKE AKINPELU

A Project submitted in partial fulfilment of the requirements for

DUAL DEGREE IN (DBA AND MASTER IN CYBERSECURITY)

At

EC Council University

TABLE OF CONTENTS

ABSTRACT

The purpose of this project was to implement an effective strategy to prevent network intrusion in Nigerian bank. The research applied three theoretical frameworks - the NIST Cybersecurity, COBIT 5 for Information Security and PCI DSS. Following literature reviews on the subject matter, the study used a survey design that involved qualitative techniques. The methods used were a group strategy discussion session involving some management staff of FirstBank in Nigeria, and, interviews team leads of staff whose jobs' functions are related to the management of information security in the bank. The discussions and the interviews were guided by scripts that the researcher developed. The scripts were based on the research questions and literature reviews. The information obtained from the surveys were analysed and used in answering the research questions. Nine senior staff - team leads of units whose functions were related to management of information security were interviewed. Six management staff were also engaged in group discussion to examine the current information security management strategy in FirstBank with comparison to best practice and establish security gaps in the bank, establish the consequence of those gaps on the bank's information asset and provided solutions on how to prevent intrusion. The result of the researched revealed that ineffective information security management strategy in the bank resulted in escalating intrusion in the bank. The research also recommended the adoption of NIST Cybersecurity framework to make the bank's information security strategy effective and be able to combat intrusion.

Keywords: *Cybersecurity, COBIT 5, Preventive Control, Corrective Control, Deterrent Control, Detective Control, Compensating Control, Confidentiality, Integrity, Availability, ISO 27001*

CHAPTER ONE

INTRODUCTION

1.1 Backround Of Study

A financial organisation with effective information security strategy is less prone to data leakages and consequences of not implementing the strategy such as phishing attack, hacking, social engineering etc. Information Security management strategy is very crucial towards the protection of organisational and customers' data. COBIT 5 frameworks for information security is one of the model used to establish the effectiveness of information security strategy in an organisation. COBIT 5 provides a comprehensive ways of ensuring reasonable and appropriate security control for information resources (ISACA, 2012). National Institute of Standard and Technology (NIST) (2014) established cybersecurity framework. The framework helps organisations to apply principles and best practices of risk management to improving the security and resilience of critical infrastructure which include organisational and customer data and preventing network intrusion.

The Central Bank of Nigeria (CBN) established Nigerian Financial Services IT Standards Blueprint. The standards contain different IT/Information Security framework to be adopted by Nigerian financial institution which include the objectives and intention, description, minimum acceptable maturity level, derivable benefits, requirements for compliance, consequences for deviation and timelines for compliance. The figure below shows the CBN IT roadmap for all banks and timelines. It is expected for all banks to achieve a minimum maturity of 3 out of 5 on or before deadlines as show in the figure below.

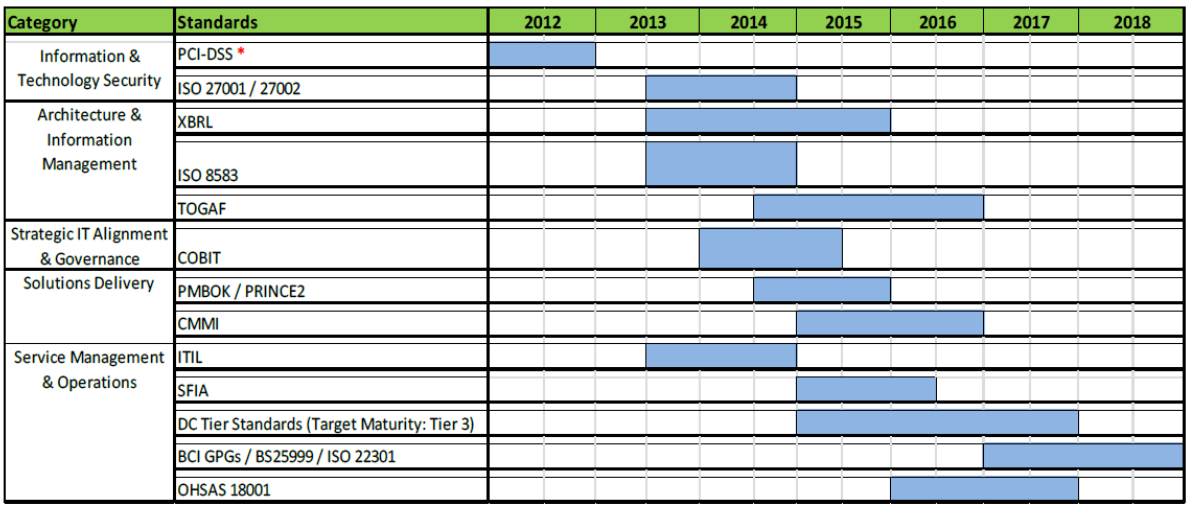

Figure 1.1: CBN IT Roadmap and Timelines

Source: CBN IT Standards and Blueprints, 2013

Retrieved from http://www.cenbank.org/ITStandards/IT_Standards_Blueprint_Final_revised%204%20website.pdf . The following are the maturity level of the CBN information security standards of three financial institutions based on the audit conducted by the apex banks examiners.

S/N	Banks	PCI DSS Maturity	ISO 27001 Maturity	COBIT 5 Maturity
1	FirstBank	4	3	4
2	Guaranted Trust Bank (GTB)	3	2	2
3	Wema Bank	2	2	1

TABLE 1.1: CBN Assessment of Bank's Information Security Standards

First Bank of Nigeria, sometimes referred to as FirstBank, is a Nigerian multinational bank and financial services company headquartered in Lagos. It is the biggest bank in Nigeria by total deposits and gross earnings. It operates a network of over 750 business locations across Africa, the United Kingdom and representative offices in Abu Dhabi, Beijing and Johannesburg set up to capture trade-related business between geographies. The bank specialises in retail banking and has the largest retail client base in Nigeria. In 2015, The Asian Banker awarded FirstBank the Best Retail Bank in Nigeria award for the fifth consecutive year.

The Nigerian banking business operates nationally, with an active customer base of over 10 million, and employs over 12,000 staff. FirstBank operates along four key Strategic Business Units (SBUs) – Retail Banking, Corporate Banking, Commercial Banking and Public Sector Banking. It was previously structured as an operating holding company before the implementation of a non-operating Holding Company structure (FBN Holdings) in 2011/2012 The researcher is a Manager in Information Security Operations in the bank. He manages teams of Security Engineers, Forensic Investigators and Threat Hunting Professionals in the group. FirstBank bank being the largest bank in Nigeria will be fair representatives of what is happening in the entire banking sectors in Nigeria. The researcher has have the opportunity to work in couples of the banks and also privilege to work in the bank that has the biggest Information Security Professionals in Nigeria.

In most Nigerian Banks, strategy towards information security to safeguard against network intrusion is not effective which poses serious financial and reputational threat to the bank. This

was revealed by the data the CBN capability maturity level as shown in the table 1.1. From the table this reveals that the strategy for most banks in Nigeria are not matured

1.2 Statement Of Problem

Information security strategy towards prevention of network intrusions for most banks in Nigeria are of great concerns due to the CBN assessment.

1.3 Purpose Of Study

The purpose of this study was to develop an effective information security strategy to prevent network intrusion in most banks.

1.4 Research Objectives

Arising from the purpose of study, the following research objectives was determined:

1. To understand and examine the current information security strategy in Nigerian Banks with comparison to best practice
2. To establish information security gaps in Nigerian Banks
3. To establish the consequence of those gaps on the banks and its information asset
4. To recommend effective ways by which network intrusion can be prevented as informed by best practice.

1.5 Research Questions

1. How information security is practiced in Nigerian Banks?
2. What are the gaps of information security t strategy in Nigerians' Banks?
3. What are the consequence of these gaps on the banks and its information asset?
4. How can the banks prevent Network Intrusion?

1.6 Definition Of Terms

Access Control: To control access to information or data

Availability: It is a term in information security that ensures reliability and timely access to data and resources to authorised users

Compensating controls: provide an alternative measure of control

Confidentiality: It is term term in information security to ensure that information is not disclosed to unauthorised individuals, processes or systems

Control Objective for Information and Related Technology (COBIT): A set of objectives for Information Technology Governance

Cryptography: Is the science of hiding information or data from the adversory or unintended persons

Cybersecurity: Is the process of protecting information/data by preventing, detecting, and responding to attacks

Detective Control: It helpts to identify malicious activities on the IT asset

Deterrent Control: It is a control in place to discourage malicious person from attacking an IT asset.

Intrusion: Fraud related to the use of technology

Effective Information Security Management Strategy: A roadmap for establishing information security practices that can be used to meet future challenges

Nigerians' Banks : The researcher's organisation

Hacking: Is the wrong use of computer/technology to carry out malicious activities like electronic fraud

Intrusion Dection Systems (IDS): A systems that detects attacks on systems or information assets

Intrusion Prevention Systems (IPS): A systems that detects and blocks attacks systems or IT assets

Integrity: It is term term in information security that ensures the accuracy and reliability of information and systems.

ISO 27001: This is a set of requirements for the management and governance of information security

NIST: A federal institute that work with government to develop standard and apply standards

PCI DSS: A set of standards for the protection of cardholder information

Preventing Control: Prevent the occurrence of security event

Security Information and Event Monitoring (SIEM): Is a systems that aggregate all computer security logs of an organisation in order to use the information obtained to respond to any incidences arise from the use of IT

1.7 Conclusion

This chapter provided a background to this study. It highlighted the objectives and significance of the study. It also provided a summary of the research plan.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This chapter focused on the intensive review of literature conducted on the research topic. For a better understanding of the research topic, extensive work was done on the findings. Theories and write-ups from several articles and journals which were from information security source materials, textbooks, search engines and other relevant sources, which helped form an extensive understanding of information security management strategy to prevent network intrusion in Nigerian Banks.

Intrusion-detection systems (IDS) and intrusion-prevention systems (IPS) are two defensive mechanisms used by most of the organizations to secure their networks. Both rely on similar technologies, but each fills a different function, maintains different placement in the network, and defends against different kinds of attacks. Understand this relationship, and outline the differences between IDS and IPS systems.

Intrusion is a set of actions that compromise the basic security goals which are confidentiality, integrity, availability (CIA) of a computing/networking resource. Intrusion detection systems (IDS) has the capability to identify threats, attacks and any malicious activities on the network which are logged in form of alerts. An IDS cannot block the attacks, attacks are passed. These logs assist the security administrator to have a visibility of the attacks profile in the network.

Intrusion prevention system (IPS) has the capability to detect intrusion activities and proactively block the activities before resulting in exploitation of the network. An IPS are monitoring real time packet traffic with malicious activities or which match specific profiles and will trigger the generation of alerts and it can drop, block that traffic in real time pass through in network. The mainly IPS counter measures is to stop an attack in progress.

An IDS is best used for network attack monitoring and for alerting security administrators of emerging threats. An IDS is passive while and an IPS is proactive. IDS and IPS both increase the security posture of an enterprise networks, monitoring traffic and inspecting and scanning packets for intrusion. Both systems are based on known signatures. Both are a preventative technical control whose purpose is to guarantee that incoming network traffic or packet is legitimate.

An IDS is designed to detect the attack and also to store new signature into the systems log files as applicable. An IPS will be required to drop malicious traffics. Implementing an IPS can be risky because it has the potential to slow down network traffic or to set up a self-imposed denial of service attack by blocking legitimate traffic. IPS system presents additional performance challenges because it has to be configured in an in-line mode while and IDS is configured in a promiscuous mode. Both configuration based on misuse detection and anomaly detection have advantages and drawbacks. Major drawback of any IPS or IDS is after installing the IDS and IPS is the low performance issues on the network, however the benefits outweigh the drawback. Both systems requires continuous fine tuning and update on their signatures to ensure their efficiency.

2.2 Theoretical Framework

This study was inspired by three framework which are Cybersecurity framework, COBIT 5 framework for information security and PCI DSS Framework

2.3 Cybersecurity Framework

This study was inspired by framework for improving critical infrastructure (National Institute of Standards and Technology, 2014). The framework focused on how to use business drivers to guide security activities considering risk as part of the organisation's risk management process. The framework helped organisations to apply principles and best practices of risk management to improving the security and resilience of critical infrastructure/data which include organisational and customer data. The Framework Core comprises four elements which were functions, categories, subcategories and informative references. The five concurrent and continuous functions are Identify, Protect, and Detect, Respond, and Recover which together provided a high-level, strategic view of the lifecycle of an organisation's management of cybersecurity risk as shown in figure below.

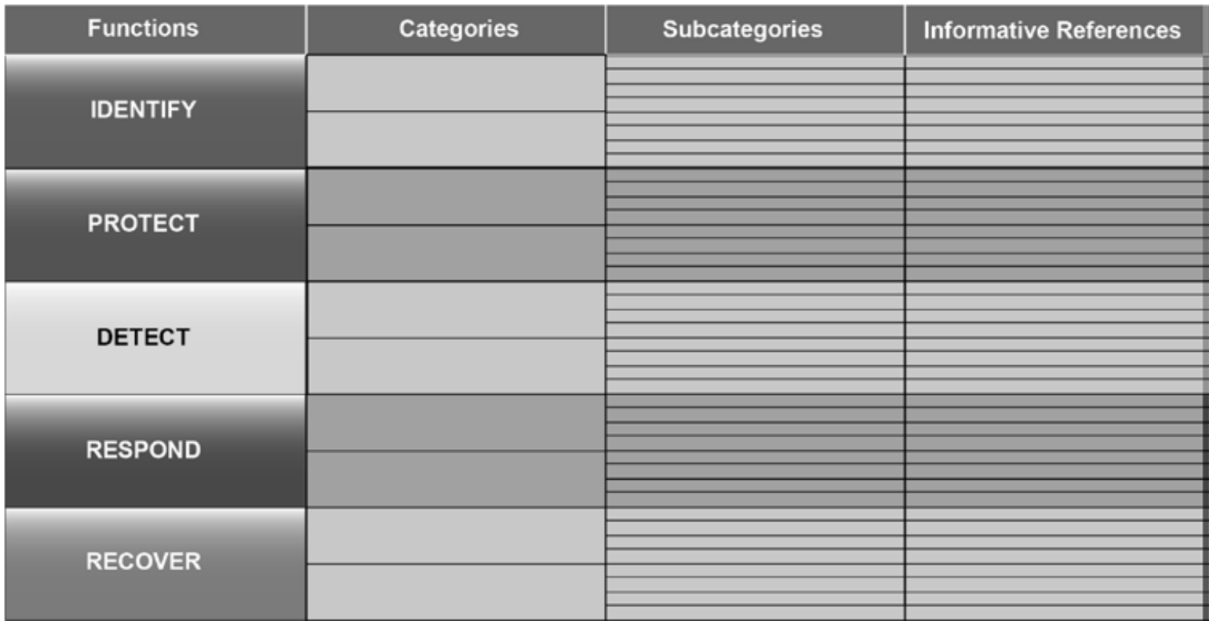

Figure 2.2: Cybersecurity Core Framework

Source: Framework for Improving Critical Infrastructure Cybersecurity, NIST, USA, 2014

2.4 COBIT 5 for Information Security Framework

COBIT 5 for Information Security an ISACA publication (2012) highlighted the major drivers for the development of Information Security and benefit of COBIT 5. The framework provided a comprehensive ways of ensuring reasonable and appropriate control for information resources. It was based on five guiding principle as illustrated in the figure below:

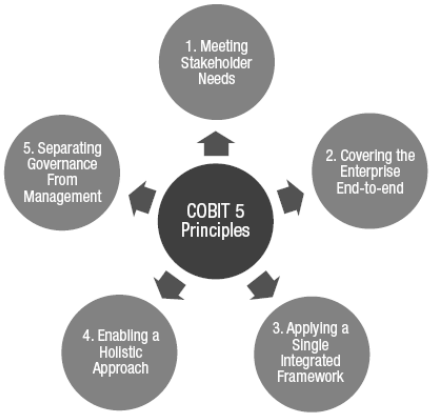

Figure 2.3: COBIT 5 Framework for Information Security Principle (ISACA, 2012)

2.5 PCI DSS Framework

PCI DSS provided a baseline of technical and operational requirements to protect cardholder data information data. The standard specified twelve requirements for compliance. This compliance was organised into six control objectives as shown in table 2 below. Retrieved December 17, 2015 from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

2.6 Conclusion

This chapter reviewed relevant literature on information management, information security, information security management strategy, intrusion, cybersecurity as well as the theoretical framework guiding the study. The next chapter describes the research method and process used in this study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The objective of this chapter is to report and present the methodology of the study that was conducted. The chapter looks at the research design that was used in addressing the research questions, a description of the sample group the research instruments used and the method of analysis.

3.2 Research Design

The research design is qualitative. It used a qualitative approach that comprised of a group discussion session (much similar to a focus group) of the head of units whose functions are related to the management of information security and interview sections with team heads. The discussion session and the interviews were conducted based on scripts that was prepared by the researcher. The researcher made use of stratified sampling because the research is aimed at the subgroups of the entire departments in the bank. These departments are : information technology group; information systems control; IT audit and enterprise risk management.

3.3 Population Of Study

The target population of the study was 15 in the following division: information technology group; information systems control; IT audit and enterprise risk management out of total management staff of 28 in the bank. The population was targeted to these categories of staff because their functions are related to the management of information security in the bank. Interviews were conducted to nine senior staff who are the various team leads of different units in the targeted departments. A group discussion was conducted to six senior management of the researcher's organisation because of their roles in the management of information security management in the bank.

3.4 Sample And Sample Size

3.4.1 Discussion Group

As a result of the research type conducted by the researcher, it was imperative to ensure a careful selection of participants, only very senior management of the researcher's organisation were invited to participate in the session. The total population of management staff are 28. Six management staff whose functions are related to the management of information security in the bank as given in Table 3.1 below were selected for the discussion:

S/N	Title/Designation
1	Chief Information Officer
2	Chief Risk Officer
3	Chief Compliance Officer
4	Chief Internal Auditor
5	Chief Information Security Officer
6	Group Head, E-Business

Table 3.1: Profile of Participants

3.4.2 Interviews

The population of the study is made up of nine team leads (senior staff) whose jobs' responsibility were related to the management of information security in the bank out of total management staff of 28 in the bank.

3.5 Research Instrument

3.5.1 Instrument Used For The Discussion Group

The researcher prepared a list of questions – based on the research questions and the recommended approaches in the literature review, to serve as a script for the discussions.

In addition to the question guide, the researcher encouraged the participants to ask follow-up questions similar to the pattern of questions recommended for action learning sets. The script contained 12 questions

1. Question 1-6 relate to research objective 1
2. Question 7 relate to research objective 2
3. Questions 8 – 10 relate to research objectives 3
4. Questions 11-12 relate to research objective 4

3.5.2 Instrument Used For The Interviews

The researcher prepared an interview guide to act a script for discussion with the management staff to be interviewed. The questions were related to all the objectives. An in-depth interview is an open-ended, discovery-oriented method to obtain detailed information about a topic from a stakeholder. According to Wallace Foundation (2015), in-depth interviews are a qualitative research method; their goal is to explore in depth a respondent's point of view, experiences, feelings, and perspective on the subject matter. By means of a thorough composed interview

guide, the interviewer ensures that the conversation encompasses the topics that are crucial to ask for the sake of the purpose and the issue of the survey (Megafon, 2015). In addition, the in-depth interviews were done using the question guide in Appendix I. The in-depth interview helped to throw more insight into the research objectives as questions were allowed to flow naturally based on information provided by the respondent. The script contained 18 questions.

1. Questions 1 – 3 relate to research objective 1
2. Question 4 - 12 relate to research objective 2
3. Questions 13 – 16 relate to research objective 3
4. Question 17 - 18 relate to research objective 4

The interviews were conducted during lunch hour and scheduled meetings with some of the respondents.

3.8 Data Administration And Collection

3.8.1 Data From Group Discussion

The researcher obtained the required data through the group discussion session. Prior to the session, the researcher took time to explain the purpose of the research to the participants. The researcher also spent time getting their buy-in and cooperation.

Respondents were assured them that their comments would be considered as their professional opinions. They were also assured that they would be allowed sufficient time to make useful contributions to help the business.

The researcher invited the participants verbally, meeting each of them in the office individually. After their acceptance of the invitation, all participants agreed on a venue for the group discussion. The meeting room in the head office was to be used. The researcher liaised with the corporate services department and made other preparations required to ensure that the meeting would be conducted successfully.

All six invited participants attended the meeting on the agreed date and the discussions were held at the designated venue. The participants were allowed to share their views and discuss opinions or points raised during the meeting. The meeting was originally scheduled to last for four hours, but eventually ran for an extra 12 minutes.

3.8.2 Data From Interviews

The means of data collection was gathered information from interviews and document review. The researcher used his phone to record the interviews with the interviewees. The researcher had earlier informed the sample size and intended interviewees informally during conversations with them physically via chats and emails. This enabled a better reception during the interviews. A total of nine people were interviewed; though the researcher tried to interview one more person. The researcher also has a rapport with most of the interviewees and this elicited more responses from them as they were comfortable with the researcher. The researcher's role was primarily that of a listener. Each interview was scheduled to hold for about 40 to 45 minutes due to the busy nature of each staff on their respective desks, but some of the interviews lasted for about 50 minutes.

3.9 Analysis Of Data

The researcher chose to analyse the data obtained from the group discussion and interviews using a qualitative approach because it allowed the researcher to participate in the research setting. The researcher gathered information from interviews and documentary evidences (internal reports from financial control department), analysed the data from these sources, observed and studied certain patterns and was able to draw the researcher's conclusions based on the findings therein. In addition, he was able to present gathered information in a qualitative format. The details of the analyses and a summary of the discussions are presented in chapter four.

3.11 Conclusion

This chapter described the research design and methodology in detail. It described the target population and sample size for the survey. It also discussed the methods used in collecting and analysing the researcher's findings.

The next chapter presents the results of the analysis of the data obtained from the discussions and the researcher's findings.

CHAPTER FOUR

RESULTS PROJECT FINDINGS

4.1 Introduction

This chapter presents the data collected through the process outlined in chapter three. It also contains the interpretation of the data as well as supporting information of the findings.

4.2 Sample Profile

As earlier discussed in chapter 3, a group discussion and in-depth interview questions were developed. A total number of fifteen (15) members of senior staff made up the sample size. Six management staff were engaged in the group discussion and nine team leads were interviewed. A sample of the In-depth interview questions and group discussion question are presented in the appendix.

4.3 Presentation Of Results

4.3.1 Research Objective 1

The objective is to understand and examine the current information security management strategy in Nigerian Banks with comparison to best practice. In providing answers to research question one, discussion question 1-6 and interview question 1-3 provide answers to this.

4.3.1.1 Discussion Group

Discussion 1: What is the current practice like in the Planning of Information Security in the bank?

Discussant	Response
Discussant 1	IT Group and information security group are responsible for the planning of information security in the bank as against involving the management and the board to ensure their oversight
Discussant 2	I agreed with the CIO. IT and Information security plan the information security for the Bank
Discussant 3	The IT compliance of compliance group ensure that the bank's various policies and standards are being adhered to. My group also benchmark the current practice with the regulatory standards such as CBN
Discussant 4	On a yearly basis, the audit group comes up with the audit program with the scope and objectives of audit. Information Security Audit is also

	included in the plan to ensure the assurance that the bank's IT assets are protected
Discussant 5	We work with IT group to come up with policies and standards that governs IT activities and how the bank can be protected from IT related risk

Table 4.1: Discussion on Research Question 1

Discussion 2: How is the current Monitoring and Reviewing Process of Information Security like in the bank?

Discussant	**Response**
Discussant 1	The process not clearly defined but the information security group follows up with various gaps identified by internal auditor, external examiners and compiance group to ensure adequate and timely remediation of gaps discovered
Discussant 2	There is no structure monitoring and review process in the bank as far as information security is concerned
Discussant 3	The current monitoring and reviewing processes are runned in Silos, this is part of the information security group processes. These processes need to be reviewed and all stakeholders and managements need to be involved
Discussant 4	There is no proper monitoring and reviewing process is place. Currently, there is no security incidence and event monitoring solution in place. Audits are not enable on all our critical systems talk less of monitoring or reviewing. This makes it difficult to detect or review any security incidence.
Discussant 5	There is no defined Monitoring and Reviewing Process, even the technology and man power to run the process does not exist

Table 4.2: Outcome of Discussion 2

Discussion 3: How is the current Maintenance and improvement of Information Security like in the bank?

Discussant	Response
Discussant 1	The information security group is responsible for the maintenance and improvement of information Security
Discussant 2	The current maintenance and improvement of information security is maturity level 1. The maintenance and improvement of information security is defined in the information security policy but the resources and technology that is required is not available
Discussant 5	The man power for the maintenance and improvement of Information Security in the bank is yet to be fully built and the also lack the required tools to keep this running.

Table 4.3: Outcome of Discussion 3

Discussion 4: What are the available information security related Documents and records in the bank?

Discussant	Response
Discussant 1	The following documents and standards exist: (i) information security policy (ii) IT Policies (iii) IT Procedures
Discussant 2	I am only aware of the information security policy even though not sign off by any members of the senior management
Discussant 3	Information Security Policy
Discussant 4	(i) Information Security Policy (ii) IT audit programme
Discussant 5	These are the available information security related document and records in custody of information security group (i) information security policy (ii) Application Security Standard (iii) Server Hardening Standard (iv) Database Security Standard (v) Anti-Virus Procedure
Discussant 6	I am aware of information security policy

Table 4.4: Outcome of Discussion 4

Discussion 5: How do the management view information security management in the bank?

Discussant	Response
Discussant 1	Information Security is seen as IT business
Discussant 2	Top management sees information security management as IT and information security group responsibility
Discussant 3	As an integral part of IT functions
Discussant 4	Information security is perceived as show stopper to business activities
Discussant 5	Information security is seen as part of IT and the management find it difficult to invest in it as they believe they have already invested heavily in IT
Discussant 6	Information security is perceived as a sub-function of IT

Table 4.5: Outcome of Discussion 5

Discussion 6: Is the Top Management committed to the practice of information security?

Discussant	Response
Discussant 1	Not at all, we are trying to let them be committed to the practice of information security
Discussant 2	No, we are yet to receive their commitment
Discussant 3	As at now, management is yet to be committed to the practice of information security
Discussant 4	Absolutely, No
Discussant 5	Top management commitment is a critical success factor for information security but it is unfortunate that we are yet to get their buy in
Discussant 6	No, because they are yet to be convinced about the needs for information security

Table 4.6: Outcome of Discussion 6

4.3.1.2 Interview Question

Question 1: How is access control to systems, application and network in Nigerian Banks handled based on each staff job's functions?

Interviewee	Response
Respondent 1	Access control to systems, application and network is not adequate. Some staff of Information Technology hasve excessive access to systems
Respondent 2	Privilege account are not managed properly as some IT staff have access to this account. Some of the accounts are used to carry out routine IT admin functions
Respondent 3	Some members of staff access control are in line with their jobs' function while some members of staff access to systems are not in conformity with their job's function.
Respondent 4	Least Privilege Principle is not defined for some IT staff as some programmers have access to production environment.
Respondent 5	There is no defined policy for access control in the bank.
Respondent 6	Access to systems application and database are based on job's functions but some staff of network administration access are not properly defined
Respondent 7	Access to the bank's systems, application and network in Nigerian Banks is in conformity with the bank information security policy
Respondent 8	The bank's access control to IT infrastructure is not full proof. There is always room for improvement
Respondent 9	All access to systems are handled properly but there are some exceptions to this based on the job's demand.

Table 4.7: Outcome of Interview Question 1

Question 2: What is the management perception of Information Security Management?

Interviewee	Response
Respondent 1	Management does not see the reasons for reviewing the activities of information management

Respondent 2	Executives management do not put in place control to ensure good practice for information management
Respondent 3	Management disposition to information security is indifferent
Respondent 4	Management is not driving information security management
Respondent 5	There is no management buy in to information security management. They need to drive it to ensure its effectiveness
Respondent 6	There is no financial support from management for the management of information security as they feel that there is no financial benefit
Respondent 7	Management sees information security management as part of IT and believe lots of money has already been allocated to IT and there is no need to spend more on information security
Respondent 8	Management disposition to information security is changing as there is now provision for it in the budget.
Respondent 9	Management has negative disposition to information security as they believe that their main responsility is to ensure profitability not knowing the security posture can as well impact on the profitability of the bank

Table 4.8: Outcome of Interview Question 2

Question 3: How is the information security perceived by staff of Nigerian Banks?

Interviewee	**Response**
Respondent 1	Staff sees information security as a show stopper for them in delivering their day to day work.
Respondent 2	Staff sees information security activities such as password complexities, segregation of duties among other as waste of time.
Respondent 3	Staff are not comfortable with compliance when it comes to adhering to the bank's information security policy
Respondent 4	Some staff sees it as a must to have especially staff in information technology group and some do not understand what it entails
Respondent 5	Staff has negative culture towards information security as they has little level of awareness towards the subject matter.

Respondent 6	The awareness level of staff whose jobs are related to information systems or technology is ok while non-technical staff seems to be nonchalant about information security
Respondent 7	IT staff sees it as a means to protect the bank IT assets from attackers while the general staff seems not to understand it
Respondent 8	Quite number of staff has little knowledge about information security while the technical staff especially the IT staff sees it as very necessary
Respondent 9	Staff sees it as a means to ensure that customers' data are protected even though they are not ready to practice it because they see it as a burden

Table 4.9: Outcome of Interview Question 3

4.3.2 Research Objective 2

The objective is to establish information security gaps in Nigerian Banks. In providing answers to research question two, discussion question 7 and interview question 4-12 provide answers to this.

4.3.2.1 Discussion Group

Discussion 7: What are the gaps in the planning of Information Security in the bank?

Discussant	**Response**
Discussant 1	Lack of management involvement in the planning of information security in the bank
Discussant 2	Lack of management support in the planning of information security in the bank
Discussant 3	The planning of information security is supposed to be driven by top management and the executives to ensure that information security align with the business objectives. Currently, information security objectives do not align with business objectives
Discussant 4	The planning of information security is carried out without taking the stakeholders along

Discussant 5	The planning of Information Security in the bank is managed by information security group. For ISMS to be effective top management leadership is required to easily integrate information security into business

Table 4.10: Outcome of Discussion 7

4.3.2.2 Interview Questions

Question 4: Is there standard procedures or approvals before an IT change is made that will impact the bank information system?

Interviewee	**Response**
Respondent 1	The IT change management process is run in Silos by IT department, all stakeholders are not involved in the process and senior management approval is not required.
Respondent 2	There is an IT Change management procedures and approval is not required for change that will impact on the bank information system.
Respondent 3	The IT change management procedure is inadequate and there is no provision for management approval before a change is deployed to production
Respondent 4	There is a standard procedures for IT change but not sure whether it adequate
Respondent 5	The current IT procedures do not address change that has major impact on the bank's information systems as critical stakeholders are not carried along in the process, management is not also aware of IT changes
Respondent 6	Yes, there is standard procedures for IT changes, also Head, IT operations sign off all changes before implementation
Respondent 7	There is standard procedures for IT changes and IT senior staff approves all changes that will impact the bank information system before go live
Respondent 8	There is change management process even though the process is yet to be mature, we are working on how to improve the process to ensure that all stakeholders are carried along and get senior management or representative approval before deployment

Respondent 9	There is a standard procedures for IT changes and supervisor and head of IT operations approvals are gotten before implementation

Table 4.11: Outcome of Interview Question 4

Question 5: Is the network, host, and application(s) vulnerable to attacks from the internet or intranet which result in financial/reputational loss?

Interviewee	**Response**
Respondent 1	Yes, there are few cases of incidence of financial loss due to lack of adequate control from the network and application layers.
Respondent 2	The bank's network is vulnerable to attacks, the bank losses huge amount of money due to the attack in the last one year
Respondent 3	The bank has suffered from reputational damage due to financial loss cause by the bank's vulnerable network and application.
Respondent 4	Electronic fraud ranked first based on the bank's fraud statistic and this was as a result of inadequate countermeasure in the bank network, systems and application.
Respondent 5	The lack of adequate control to mitigate risk of financial loss and reputational damage has exposed the bank immensely
Respondent 6	The bank's network, systems and application are protected to a reasonable extent. However, 100% protection cannot be guaranteed as there are new vulnerabilities every day in cyber word. The bad guys exploit on this and take advantage of the systems for their financial gains.
Respondent 7	There is no full proof controls against attacks from malicious people. Even though there is a measure of controls against attacks, the bank still suffer attacks from hackers some of these resulted in financial loss and image damage to the bank.
Respondent 8	IT department try as much as they can to protect attacks by making sure that adequate controls within the provided resources are implemented. However, these controls are not enough as the management need to invest more on information security to mitigate the risk of financial losses due to hacking of the bank's systems

Respondent 9	Some applications and operating systems are vulnerable to attack from the internet and even the bank's intranet.

Table 4.12: Outcome of Interview Question 5

Question 6: Can malicious user easily access, modify, or destroy data or services within the system due to the current information security practices?

Interviewee	**Response**
Respondent 1	Yes, malicous user can easily carry out unauthorised access or modification on the bank network due to the present configuration.
Respondent 2	Malicious users can gain access to the bank systems to carry out fictitious activities due the insufficient security practices in the bank
Respondent 3	It is possible for a malicious user to gain access to carry out un-approved activities because of the current information security practices. The bank is not complying to all the documented standards and policies
Respondent 4	Yes, malicious user can access, modify or destroy data or services within the system as revealed by the bank's fraud statistic. There are more incidences of computer related fraud
Respondent 5	There likelihood for a malicious user to gain access, modify and destroy data or services is high because the current information practices in the bank is not good enough.
Respondent 6	It is possible for a malicious user easily access, modify, or destroy data or services within the system as it is impossible to achieve 100% protection in information security
Respondent 7	Yes, depending on the skill set of a malicious users
Respondent 8	Based on lack of management commitment to information security and the bank lacks intrusion and prevention system (IPS) that will detect/prevent any intrusion to the bank's systems. Management is yet to approve the purchase of this tool
Respondent 9	Yes it is possible.

Table 4.13: Outcome of Interview Question 6

Question 7: Is there adequate technical control in place to protect the bank's network to prevent financial loss?

Interviewee	Response
Respondent 1	No, the technical control in place is not sufficient.
Respondent 2	No, as it is very obvious
Respondent 3	The technical control in place is not adequate
Respondent 4	Just like I mentioned earlier if we have adequate technical control in place to prevent financial loss, computer related fraud will not rank first in the bank's fraud statistic
Respondent 5	If the technical control is adequate, the bank would not have been so exposed to financial losses in our electronic platforms
Respondent 6	No, there is no technical control that is adequate that is the reason for defence in depth approach to information security
Respondent 7	Yes, but the bank still need to invest more on various technical tools to prevent financial loss
Respondent 8	Investment need in information security is required for the bank to have full assurance in the technical control in place. Hence, the bank lack tools to adequately protect the bank's network against financial loss
Respondent 9	Not adequate, there are lots of technological control not in place as these requires money for the acquisition

Table 4.14: Outcome of Interview Question 7

Question 8: Is Security Review and assurance part of business process and IT operational activities?

Interviewee	Response
Respondent 1	Yes, it is as the internal audit group carry out the review of IT activities on a periodic basis(every quarter). This audit programs are being reviewed on a yearly basis

Respondent 2	Yes, routine security review of IT operations is part of key performance indicators (KPIs) for all staff of IT control
Respondent 3	Yes, security review and assurance is part of business process and IT operational activities of the bank as my unit conduct compliance assessment from time to time to ensure that we are doing the right thing.
Respondent 4	I do not believe that we practice what we say because if the required units are doing their job as required they would have let the management know our lapses of IT operations activities in order to make informed decision.
Respondent 5	Yes, there is from various compliance units such as IT Control, IT audit, IT risk and IT security. The question should be if there is management review and oversight of the various reviews conducted?
Respondent 6	Yes, as my unit is doing its part and the reports are sent to IT management
Respondent 7	Yes, Security Review and assurance is part of business process and IT operational activities
Respondent 8	Yes there is but there is no active action plans to remediate all the security lapses identified. Though, IT is doing its part but management support will be required to remediate the major issues.
Respondent 9	Yes security review and assurance is part of business process and IT operational activities though the manner at which this is conducted may not be adequate.

Table 4.15: Outcome of Interview Question 8

Question 9: Is there a strategy for Enforcement of Information Security in Nigerian Banks?

Interviewee	**Response**
Respondent 1	No such strategy exist
Respondent 2	I am not aware of such
Respondent 3	Yes, partly IT compliance ensure enforcement of the agreed information security policies and procedures
Respondent 4	Not at all

Respondent 5	There is no clearly defined strategy for enforcement of information security in the bank
Respondent 6	I am not sure if such strategy exist
Respondent 7	No, there is no strategy for Enforcement of Information Security in Nigerian Banks
Respondent 8	No. Such strategy needs to be driven by senior management.
Respondent 9	No. It doesn't exist

Table 4.16: Outcome of Interview Question 9

Question 10: Is there frameworks that cover all aspect of Information Security Management.in Nigerian Banks?

Interviewee	**Response**
Respondent 1	No, the current information security policy is not comprehensive
Respondent 2	Even though we have various security policies and standards they do not cover all aspect of information security management
Respondent 3	Yes, partly IT compliance ensure enforcement of the agreed information security policies and procedures
Respondent 4	Partly yes and partly no because what is currently on ground does not cover all aspect of Information Security Management.in Nigerian Banks
Respondent 5	The bank's information security policy is not robut enough, there is need for proper review to ensure that all aspect of information security management is covered and in line with business objectives
Respondent 6	Yes, there is frameworks that cover some aspect of Information Security Management.in Nigerian Banks. This need to be reviewed to ensure it completeness
Respondent 7	No, the current framework does not cover all aspect of Information Security Management.in Nigerian Banks

Respondent 8	The current framework need to be reviewed to ensure it covers all aspect of Information Security Management.in Nigerian Banks
Respondent 9	No, the current framework need to be revamped

Table 4.17: Outcome of Interview Question 10

Question 11 Nigerian Banks culture, ethics and behaviours reflect a secure IT environment?

Interviewee	**Response**
Respondent 1	No, there is need for cultural change to information security
Respondent 2	Nigerian Banks organisational structure does not reflect a secure IT environment
Respondent 3	Members of staff are still struggling security culture in the organisation
Respondent 4	No, the manner at which staff and management carry out IT activities does not reflect a secure IT environment
Respondent 5	No, Nigerian Banks culture, ethics and behaviours reflect a secure IT environment
Respondent 6	The bank has poor information security culture, ethics and behaviours
Respondent 7	Most staff especially those whose job roles do not relate with information security has bad security culture
Respondent 8	No, as there is no driver to information security culture, ethics and behaviours. It is easy for staff to develop the culture if it is embedded into organisational culture by the management
Respondent 9	To some extent, the Nigerian Banks culture, ethics and behaviours do not reflect a secure IT environment

Table 4.18: Outcome of Interview Question 11

Question 12: Are you adequately trained on Information Security Management principle as it relates to protection of bank's information asset?

Interviewee	Response
Respondent 1	I have not gone for any training on information security management trainig for the past three years
Respondent 2	Not at all
Respondent 3	Since the time I became the Head, IT Compliance, the bank is yet to send me to any formal training on Information Security Management principle
Respondent 4	No, I am yet to go for any technical training on IT forensic as it relates to my job functions
Respondent 5	No, there is no training plan for such and I have not gone for any bank's sponsored training except for the one I enrolled
Respondent 6	No, I have always been training myself as the bank makes no provision for such training
Respondent 7	No, I am not adequately trained on Information Security Management principle as it relates to protection of bank's information asset
Respondent 8	IT is working with the management to ensure that all technical training on Information Security Management are being planned for with the management to ensure that bank's information assets are well protected
Respondent 9	No, I have not gone for any bank's sponsored training on Systems and Unix security

Table 4.19: Outcome of Interview Question 12

4.3.3 Research Objective 3

The objective is to establish consequence of information security gaps on the bank and its asset. In providing answers to research question two, discussion question 8-10 and interview question 13-16 provide answers to this.

4.3.3.1 Discussion Group

Discussion 8: Has the bank's network, application and systems been infiltrated with Virus or Malware?

Discussant	Response

Discussant 1	Virus and Malware are continous threats faced by the bank.
Discussant 2	Yes, we have recurring infiltration of virus and malware on our network, application and systems
Discussant 3	Yes, almost everyday
Discussant 4	Yes, this is a growing concerns
Discussant 5	Though most of our critical servers are not directly facing the internet, however the workstations are vulnerable as we receive daily alert of virus and malware via the workstation. Though the risk infiltration is low as no users of workstation has admin right which is the type of right required by most malware to carry out malicious activities.
Discussant 6	There are several cases of infiltration especially for staff handling sensitive data

Table 4.19: Outcome of Discussion 8

Discussion 9: Has the bank been exposed to Hacking that lead to financial in the past two year?

Discussant	**Response**
Discussant 1	It is unfortunate that the bank is exposed to hacking which has resulted in great financial loss to the bank.
Discussant 2	Yes
Discussant 3	Yes
Discussant 4	Yes
Discussant 5	Yes
Discussant 6	Yes

Table 4.20: Outcome of Discussion 9

Discussion 10: What are the customer's (internal or external) complaints like on the unauthorized access or modification on their accounts?

Discussant	**Response**

Discussant 1	We always have different complaints ranges from password compromise to unauthorise transactions from our external customers. We seldom have complain from internal customes on this except for the major breach that happens in which on of the administrators account were compromised to carry out unauthorised activities which resulted in great financial loss to the bank.
Discussant 2	We receive dozens of report from the customers service department on unauthorised access or modification on customers' accounts
Discussant 5	The complaints from customers ranging from phishing attack, social engineering, password compromise
Discussant 6	We had several complaints from customers on most of our e-payment platforms that their passwords were compromised and unauthorised transactions were carried out on their accounts.

Table 4.21: Outcome of Discussion 10

4.3.3.2 Interview Questions

Question 13: What is the rate of major breaches involving sensitive or confidential information for the past one year?

Interviewee	**Response**
Respondent 1	The rate at which breaches such as phishing, social engineering and identity theft occur have been on the increase for the past one year
Respondent 2	There are more incidences of electronic fraud for the past one year.
Respondent 3	There has been several complaints from the customers that some transactions occur on their electronic platforms which they do not initiate. Some complaints that their account details were revealed to an outsider and they were wondering how it happened
Respondent 4	The fraud on the electronic platform such as mobile banking, online banking has been on the increase as revealed by the bank's fraud statistic. I will be willing to share the statistic with you. Based on the statistic alone, 88% of the fraud are as a result of ineffective information security strategy. Refer to appendix IV for details.

Respondent 5	Based on our yearly risk loss index, the rate of major breaches involving sensitive or confidential information for the past one year has increased by 30% which is very alarming
Respondent 6	We have more incidents reported this year as a result of breaches involving sensitive or confidential information.
Respondent 7	There are more complaints from the customers' end that their accounts details such as password, balance have been compromised
Respondent 8	Based on the yearly report of IT, there is 28% increase in reported incidence as a result of breaches involving sensitive or confidential information last year ending (2015) compare to 2014.
Respondent 9	The rate of breaches involving sensitive or confidential information has been on the increase for the past one year

Table 4.22: Outcome of Interview Question 13

Question 14: What is the rate of stealing customers' data at rest or in motion for the past 3 months?

Interviewee	**Response**
Respondent 1	In the last three months we investigated about 30 cases of customers whose PIN, password and other cardholder data information were compromised.
Respondent 2	Quite numbers of compromised cases were recorded in the last three months
Respondent 3	There are about five legal cases due to stolen customers' data either at rest or in motion
Respondent 4	IT audit and my unit always collaborate to investigate cases of stolen data, based on the report there are about 30 cases
Respondent 5	Based on report collated from various risk champions, there are more cases of such incidence in the last three months
Respondent 6	The rate of occurrence of incidence due to stolen data has been increasing in the past three months.

Respondent 7	I may not be able to say the exact rate but I know that we have more incidence of customers' stolen data in the past three months
Respondent 8	There are more incidences of such in this quarter than the previous quarter.
Respondent 9	There are lots of reported cases for the past three months

Table 4.23: Outcome of Interview Question 14

Question 15: What is the rate of malware and virus infection of sensitive data for the past one month?

Interviewee	**Response**
Respondent 1	It is evident that there is presence of malware and virus infection on the network but cannot really determine the effect on sensitive data in the last one month.
Respondent 2	About eight of the systems of staff especially the IS control systems that have some sensitive data were corrupted with malware and virus, those systems were formatted before restoring the data back.
Respondent 3	About 30% of the banks' workstations were infected at one point or the other, among the workstations some of them have sensitive data
Respondent 4	Some of the banks' workstation have sensitive data and large numbers of the banks' workstation have been infected with malware
Respondent 5	More than 25% of the systems in our networked were infected with malware. Some of the systems have sensitive data on it.
Respondent 6	We monitor the spread of malware and virus on a daily basis and take active measure to ensure that all systems in our network have antivirus install, up to date. We centrally push antivirus, scan any infected systems and push update. Last month ending about 29% of the systems on our network were infected due to outdated antivirus as at that particular day. However, we were able to carry out fixes on those systems in last than three days.

Respondent 7	There has been increase in the rate of malware/virus infections on our network but we were able clean the network of virus infections
Respondent 8	The occurrence of malware and virus have been on the increase for the past one month but we have a robust antivirus program to manage this as we were able to contain this
Respondent 9	There has always been malware and virus threat through our windows platforms and the last one month is not an exception but the good news is that we were able to monitor and manage this.

Table 4.24: Outcome of Interview Question 15

Question 16: Has the bank suffered financial loss and reputational damage due to inefficient information security strategy?

Interviewee	**Response**
Respondent 1	The bank has suffered greatly as a result of ineffective information security strategy
Respondent 2	Yes, the bank has suffered from both financial loss and reputational damage as a result of ineffective strategy to prevent this
Respondent 3	It is unfortunate that the bank image has been dragged in the mud due to compliance with the CBN roadmap on IT security. The bank has lost several millions of naira as a result of this.
Respondent 4	Yes, the bank has always been losing financial as a result of inefficient information security strategy. This is not good for our reputation as a bank.
Respondent 5	Lately, the bank has been exposed to financial and reputational risk due inefficient information security strategy
Respondent 6	The bank has lost some money due to inefficient information security strategy
Respondent 7	There has been escalating intrusion which leads to financial and reputational loss as a result of inefficient information security strategy

Respondent 8	Yes, the bank profitability has been greatly impaired as the bank has lost huge amount of money as a result of lack of management commitment to information security.
Respondent 9	Yes of course, this need to be addressed immediately else the bank might lose the market to competitors.

Table 4.25: Outcome of Interview Question 16

4.3.4 Research Objective 4

The objective is recommend effective ways by which bank's intrusion can be prevented as informed by best practice. In providing answers to research question two, discussion question 11-12 and interview question 17-18 provide answers to this.

4.3.4.1 Discussion Group

Discussion 11: What can be done to improve the existing information security strategy?

Discussant	**Response**
Discussant 1	The information security objectives need to be derived from the business objectives to ensure alignment.
Discussant 2	Senior management oversight is required to revamp the existing strategy. Need for gap assessment of the existing information security strategy compare with the industry standard and then the bank need to develop a strategy to close the identified gaps
Discussant 3	Aligning of existing strategy with industry standard such as COBIT 5, NIST, PCI DSS or ISO 27001 because such standards are proven and tested over period of time to be effective
Discussant 4	Continuous independent review of information security strategy with all the stated controls and audit reports of findings should be sent to senior management.
Discussant 5	Network revamp to ensure secure network, follow a secure practice for the bank's application and systems, implementation of file integrity monitoring to detect any unauthorised change, implementation of SIEMs

	to proactively monitor users activity and act before security events crystalize to fraud.
Discussant 6	Bank-wide information security awareness, creating a roadmap for the desired state and get management buying in order to improve our existing strategy

Table 4.26: Outcome of Discussion 11

Discussion 12: What are the controls to be implemented to prevent intrusion?

Discussant	**Response**
Discussant 1	In order to prevent intrusion in the bank a combination of administrative, technical and physical control would be required
Discussant 2	To prevent intrusion in the bank, there should be a robust IT risk management in place and top – bottom approach need to be considered to be effective
Discussant 3	Complying the regulatory standards on the requirements for electronic systems such implementation of two factor authentication, maker-checker for all transfer, keeping of audit trail will serve as deterrent practice to prevent intrusion
Discussant 4	Implementation of fraud monitoring systems to monitor transactions on all our electronic platforms, flag any suspicious pattern in order and stop any discovered fraudulent activities.
Discussant 5	Implementation on Intrusion Prevention Systems. This system can proactively detect any malicious packet or hacking attempts on the bank's network, systems or applications. This solution can be integrated with SIEM as earlier discussed for optimised utilisation

Table 4.27: Outcome of Discussion 12

4.3.4.2 Interview Questions

Question 17: What can be done to ensure that managements are accountable for Information Security Management Strategy?

Interviewee	**Response**

Respondent 1	Managements need to be made aware of all the security assessment conducted by internal audit group, not just having the report but drive the action plans for remediation.
Respondent 2	Managements need to ensure that information security is an integral part of the business not just seeing it in silos
Respondent 3	Compliance to information security standards need to be part of job's functions of the management. Management drive is required to ensure compliance to the bank information security strategy
Respondent 4	Management oversight of all information security activities will make management to be accountable for security strategy
Respondent 5	To ensure that managements are accountable for information security management strategy, there will be a need for gap assessment to determine our current state, analyse and plan how to get to the desired state and come up with traction. Throughout this phase, management need to be engaged, this can be achieved by instituting information security steering committee comprising different management stakeholders.
Respondent 6	Managements should be made responsible for any security breaches as a result of their lack of support.
Respondent 7	Effective information security management strategy need to be driven from the top, management need to be aware of the various information security initiatives before they can be accountable for it.
Respondent 8	Boards and senior management need an awareness for them to be able to understand their role/accountability in information security management. This can better be achieved by engaging a consultant on formal boards and senior managements' education on information security.
Respondent 9	In order to ensure that management are accountable for Information Security Management Strategy, they will need to understand the implication of lack of good strategy and how it can affect the business. I believe information security awareness is very critical to achieve this.

Table 4.28: Outcome of Interview Question 17

Question 18: What measures can be put in place to prevent the recurring intrusion in the bank?

Interviewee	**Response**
Respondent 1	In order to prevent intrusion in the bank, defence in depth mechanism which is a layer security need to be put in place. We will to combine different controls both technical and administratie at different layes such as network, systems and application to achieve this.
Respondent 2	From my point of view, the bank need to ensure that all our public facing application/systems such as email and online banking are well protected by following industry standard on information security. Some of the practices to be adopted are: good authentication and authorisation practice; placing all public facing application behind a firewall and implementation of intrusion prevention system.
Respondent 3	The bank need to ensure strict compliance with information security best practice such as ISO 27001 and COBIT 5 to prevent the recurring intrusion in the bank
Respondent 4	To prevent the recurring intrusion in the bank, there will be needs: for investment in solution that can monitor and detect intrusion before it happens; to improve on the bank's information security practice and for information security awareness campaign for staff and customers
Respondent 5	As I mentioned earlier, there will be a need for gap assessment to be based on industry standard such as PCI DSS, ISO 27001 and COBIT 5, the bank need to come up with a strategy of the bank's desired maturity level and set out action plans in achieving the sets objectives.
Respondent 6	The bank need to invest in IT security by ensuring that various tools to ensure that the technical controls are achieved are in place.
Respondent 7	To prevent the recurring intrusion in the bank, the bank needs to tighten up the information security practice by ensuring that it aligns with IT security best practices, there will be need for adequate technical controls such as segmentation of the bank network, implementation of intrusion prevention systems (IPS) and Security Incidence and Event Monitoring (SIEM).

Respondent 8	To prevent the recurring intrusion in the bank, we will need to look at this from people, process and technology. First and foremost people need to do what they are supposed to do to ensure adequate protection of the bank's IT asset, our customers, staff and management need to be informed that information security is everybody responsibilities. Our processes need to be revamped to ensure a secure environment and the bank need to invest on security tools.
Respondent 9	Implementation of various controls across our network, systems and application. Some of this control can be implementation of 2 factor authentication and implementation of SIEM

Table 4.29: Outcome of Interview Question 18

4.4 Summary Of Findings

From the research question 1 (How information security management is practiced in Nigerian Banks?) the findings are as below:

1. Management is not involve in the planning of information security management. The planning is carried out in silos without carrying all the stakeholders along
2. There is no management buy in the current information security strategy
3. The current monitoring/reviewing and maintenance process of information security management is ineffective as the bank lack the resources such as man power and technical tools to make this functional
4. Access control to application, network and systems is not adequate
5. Poor awareness by members of staff and management to information security

From the research question 2 (What are the gaps of information security management strategy in Nigerian Banks?) the findings are as below:

1. Information security objectives do not align with business objectives because of lack of management buy and support
2. Inefficient IT change management process as stakeholders and managements are not included in the process
3. The bank's network, systems and application are vulnerable to attacks from malicious people
4. The technical control in place to protect the bank's against attack or electronic fraud is insufficient

5. The current policies and standards that governs the management of information security in the bank is not sufficient as its enforcement is not clearly defined in the documents
6. IT security personnel are not adequately trained on the management of information security and members of staff are not aware of the need for information security

From the research question 3 (What are the consequences of these gaps on the bank and its information asset?) the findings are as below:

1. Ineffective information security strategy has exposed the bank to malware and virus attack
2. The bank has suffered greatly from financial loss as a result of hacking through the attack vector such malware, social engineering and malicious user through our electronic platform
3. Customers confidence in the bank has been eroded due to intrusion on their accounts which results in reputational damage/financial losses for the bank
4. Intrusion is prevalent in Nigerians' Banks and has resulted in huge financial loss to the bank due to ineffective information security strategy

From the research question 4 (How can the bank prevent intrusion?) the findings are as below:

1. Management commitment and buy in is required in the bank's information security strategy to ensure its alignment with business objectives
2. Implementation of robust risk management process is required
3. Benchmarking the existing practice with best practice to identify the gaps and comes up with strategy to close those gaps will be required
4. Implementation of technical controls for the prevention of intrusion such as SIEM, IPS, fraud management systems

4.5 Recomendation

The researcher's findings corroborates the notion in the literature review on the need for information security management in order to mitigate risk against confidentiality, integrity and availability of information assets in the bank as informed by COBIT (2012), NIST (2014), and ISO 27001 (2013) as explained in section 2.2.

Nigerian Banks need to build effective information security strategy with the objectives of balancing the need to secure information assets against the need to enable business, ensuring compliance and maintaining cultural fit as informed by NIST (2014), PCI and ISO. There is

also need to carry out intensive gap assessment in order to determine the current state of data security strategies and the desired state in order to improve on the security posture. This is necessary to know whether the bank derives the benefit of effective information security strategy or faces the consequences of ineffective information security strategy.

To prevent the recurring intrusion in the bank as established in the findings strategy to prevent this need to be informed by NIST (2014), ISACA (2012), De Haes (2013) and PCI (2015) and proper technical control such as deployment of intrusion detection and prevention systems.

4.6 Conclusion

This chapter presented the analysis of the findings from the surveys used in this research that is group discussion conducted with management staff and interviews team leads of staff whose jobs' functions are related to the management of information security.

5.0 BIBLIOGRAPHY

Calder, A. and Williams, G., 2014, 'PCI DSS: A Pocket Guide', IT Governance Publishing.

Drum, R.: IDS & IPS Placement for network protection. CISSP (March 26, 2006)

Final version of NIST cybersecurity framework draws mixed reviews. Retrieved from http://searchsecurity.techtarget.com/news/2240214505/Final-version-of-NIST-cybersecurity-framework-draws-mixed-reviews

Flick, T., 2009, 'Hacking the smart grid', Black Hat USA Conf., Las Vegas, NV.

Freeman, EH 2007, 'Holistic Information Security: ISO 27001 and Due Care', Information Systems Security, 16, 5, pp. 291-294, Business Source Premier, EBSCOhost, viewed 9 March 2016

The Nigerian Cybercrimes (Prohibition, Prevention,Etc) Act, 2015

IPS vs. IDS: Similar on the Surface, Polar Opposites Underneath white paper by Tipping point

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISACA Publication COBIT 5. *Frameworks for Information Security*, 2012

International Organisation of Standards ISO 27001.*The ISO27001 Framework*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en2010

Jabbusch, J.: IDS vs. IPS: How to know when you need the technology (November 22, 2010)

Leonard Klie. CRM Magazine, 'Data Security Should Be in Everyone's Job *Description',* May 2015, Vol. 19 Issue 5, p32-36

Lindstrom, P., Director, R.: Intrusion prevention systems (IPS): Next generation firewalls, A Spire Research Report – by Spire Security (March 2004)

Megafon, 2015, In-depth Interview. Available at http://uk.megafon.dk/331/in-depth-interview

NEFF 2014 Annual Report. Retrieved from http://cbn.gov.ng/Out/2016/CCD/NEFF%202014%20Annual%20Report%20.pdf

NIST Cybersecurity Framework is Good and Bad. Retrieved from http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST.GOV available at http://www.nist.gov/cyberframework/upload/cybersecurityframework-021214.pdf

Payment Card Industry (PCI) Data Security Standard, v3.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Ricky M. & Monique L. Magalhaes , 'Developing an Information Security and Risk Management Strategy (Part 1)', viewed February 21, 2016, http://www.windowsecurity.com/articles-tutorials/intrusion_detection/developing-information-security-and-risk-management-strategy-part1.html

Retrieved from https://security.stackexchange.com/questions/44931/difference-between-ids-and-ips-and-firewall

Retrieved from https://www.pandasecurity.com/usa/support/card?id=31463

Shaw n Conaway ,"Using an Intrusion Prevention System as Part of a Layered Security Approach", Network Support , Technical Enterprises ,October-2006.

Sushma Mishra and Robert Morris (2011), 'Information Security Effectiveness: A Research Framework', *Issues in Information Systems*, Vol. XII No. 1, pp 246-255

The Cybersecurity Risk. Communications of the ACM. Jun 2012, Vol. 55 Issue 6, p29-32

Tom Olzak, 'COBIT 5 For Information Security: The Underlying Principles', Retrieved February 25, 2016 from http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/

Trochim, W.M. (2002). *Research Methods Knowledge Base*, 1-34.

Thomson, K.L., von Solms, R. and Louw, L., 2006, 'Cultivating an organisational information security culture', Computer Fraud & Security, 2006(10), pp.7-11.

Wallace Foundation, 2015, 'Workbook E: Conducting In-Depth Interviews', Available at http://www.wallacefoundation.org/knowledge-center/after-school/collecting-and-using-data/Documents/Workbook-E-Indepth-Interviews.pdf (Assessed on 28 December 2015)

Whitman, M. and Mattord, H., 2011, 'Principles Of Information Security', Cengage Learning.

Whitman, ME 2003, 'ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY', Communications Of The ACM, 46, 8, pp. 91-95, Business Source Premier, EBSCOhost, viewed 4 February 2016

Zhang, S. and Le, F.H., 2013, 'An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model', Journal of Economics, 1, p.5.

APPENDIX

1.0 Research Tool – Interview Script

Interview Design Document

To be used for interview sessions with staff whose job's functions are related to the management of information security in the bank
Nigerians' Banks

Designed for use as part of the dissertation
Implementation of Effective Information Security Management Strategy to Prevent Intrusion in Nigerian Bank

By
Zechariah Oluleke Akinpelu.

S/N	Interviewee	Designation	Date	Location
1	Respondent 1	Team Lead IT Audit	10-Dec-18	Head Office
2	Respondent 2	Team Lead, IS Control	14-Dec-18	Head Office
3	Respondent 3	Team lead, IT Compliance	15-Dec-18	Head Office
4	Respondent 4	Team lead, eFraud	16-Dec-18	Head Office
5	Respondent 5	Head, IT Risk	17-Dec-18	Head Office
6	Respondent 6	Team lead, Application & Database Security	18-Dec-18	Head Office
7	Respondent 7	Team lead, Network Security	21-Dec-18	Head Office
8	Respondent 8	Head, IT Operation	21-Dec-18	Head Office
9	Respondent 9	Team lead, Systems and Unix Security	21-Dec-18	Head Office

Schedules (i.e Date and Time) is subjected to change following appointment bookings with the interviewee

S/N	Activity	Time Allotted (Minutes)	Remarks
1	Opening	2	The researcher introduces the objective of the meeting which is to implement effective strategy to prevent intrusion in the bank
2	Question 1	3	This include follow up questions
3	Question 2	3	
4	Question 3	3	
5	Question 4	3	
6	Question 5	3	
7	Question 6	3	
8	Question 7	3	
9	Question 8	3	
10	Question 9	3	
11	Question 10	3	
12	Question 11	3	
13	Question 12	3	
14	Question 13	3	
15	Question 14	3	
16	Question 15	3	
17	Question 16	3	
18	Question 17	3	
19	Question 18	3	
20	Other Comments or Questions	5	
21	Total Time	61	

Requirements

Item	Remarks
Notepad and Pen	Researcher will bring his own
Recording Device	Researcher uses his smarphone
Interview Script	Prepared by researcher
Refreshment	Not Required

INTERVIEW Questions

Question 1: How is access control to systems, application and network in Nigerian Banks handled based on each staff job's functions?

Question 2.What is the management perception of Information Security Management?

Question 3. How is the information security perceived by staff of Nigerian Banks?

Question 4: Is there standard procedures or approvals before an IT change is made that will impact the bank information system?

Question 5: Is the network, host, and application(s) vulnerable to attacks from the internet or intranet which result in financial/reputational loss?

Question 6: Can malicious user easily access, modify, or destroy data or services within the system due to the current information security practices?

Question 7: Is there adequate technical control in place to protect the bank's network to prevent financial loss?

Question 8: Is Security Review and assurance part of business process and IT operational activities?

Question 9: Is there a strategy for Enforcement of Information Security in Nigerian Banks?

Question 10: Is there frameworks that cover all aspect of Information Security Management.in Nigerian Banks?

Question 11: Is Nigerian Banks culture, ethics and behaviours reflect a secure IT environment?

Question 12: Are you adequately trained on Information Security Management principle as it relates to protection of bank's information asset?

Question 13: What is the rate of major breaches involving sensitive or confidential information for the past one year?

Question 14: What is the rate of stealing customers' data at rest or in motion for the past 3 months?

Question 15: What is the rate of malware and virus infection of sensitive data for the past one month?

Question 16: Has the bank suffered financial loss and reputational damage due to inefficient information security strategy?

Question 17: What can be done to ensure that management are accountable for Information Security Management Strategy?

Question 18: What measure can be put in place to prevent the recurring intrusion in the bank?

9.2 Dissertation Group Discussion Script

Group Discussion Design Document

To be used for group discussion for the management staff whose job's functions are related to the management of information security in the bank

Meeting Logistics

Target Meeting Date: Saturday, 22 December 2018

Target Start Time: 9.00am

Target End Time: 1.00pm

Proposed Location: Head Officer 8th Floor Meeting Room Nigerians' Banks Ltd,

Marina, Lagos

Facilitator/Moderator: Zechariah Oluleke Akinpelu

Asst. Moderator/Time Keeper: Belove Momoh

Strategy Session			
S/N	Participant	Designation	Location
1	Discussant 1	Chief Information Officer	Head Office
2	Discussant 2	Chief Risk Officer	Head Office
3	Discussant 3	Chief Compliance Officer	Head Office
4	Discussant 4	Chief Internal Auditor	Head Office
5	Discussant 5	Chief Information Security Officer	Head Office
6	Discussant 6	Group Head, Ebusiness	Head Office

Requirements

Item	**Remarks**
Notepad and Pen	Participants
Flip Chart	Available
White Baord	Available

Projector	Available
Business Model Canvas Paper	Available
Post-it Notes	Available
Laptop	Facilitator to bring his laptop
Focus Group Script	Prepared by Facilitator
Sound Recorder	Researcher's Samsung Smartphone (S5)
Markers	Available
Refreshment	Snack, Coffee, Tea:To be made available in the room and self serve

1. Call to order

After thanking the participants for coming, Zechariah called to order the Strategy Session 9am on Saturday 21st , 2018 at the meeting room, 8th Floor, FirstBank, Marina, Lagos, Nigeria.

2. Meeting Proper

2.1 The researcher welcomed the participants and introduced the objective of the meeting – to discuss how to implement of Effective Information Security Management Strategy to Prevent Intrusion in Nigerian Banks

2.2 He explained that the session was important, because if not well articulated, the objective of preventing intrusion in Nigerians' Banks will not be achieved. He also noted that during the course of the session, all questions, comments, suggestions would be considered relevant, as all ideas are welcome.

2.3 The researcher urged the participants to switch off their phones or put it in silence so as to have little or no interruptions.

2.4 The Chief Information Security Officer thanked everyone for attending the meeting. He stressed the need to curb the escalating intrusion in the bank by implementing effective information security management. In addition, he reiterated that this strategy session was an important one.

DISCUSSION GROUP QUESTIONS

1. What is the current practice like in the Planning of Information Security in the bank?

2. How is the current Monitoring and Reviewing Process of Information Security like in the bank?

3. How is the current Maintenance and improvement of Information Security like in the bank?

4. What are the available information security related Documents and records in the bank?

5. How do the management view information security management in the bank?

6. Is the Top Management committed to the practice of information security?

7. What are the gaps in the planning of Information Security in the bank?

8. Has the bank's network, application and systems been infiltrated with Virus or Malware?

9. Has the bank been exposed to Hacking that lead to financial in the past two year?

10. What are the customer's (internal or external) complaints like on the unauthorized access or modification on their accounts?

11. What can be done to improve the existing information security strategy?

12. What are the controls to be implemented to prevent intrusion?