

**THE DETERMINANT OF INFORMATION SECURITY
PRACTICES TOWARDS ORGANIZATIONAL PERFORMANCE
IN THE BANKING SECTOR: EVIDENCE FROM NIGERIA**

BABATUNDE DORCAS ADEBOLA

**DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
March 2014**

**THE DETERMINANT OF INFORMATION SECURITY PRACTICES
TOWARDS ORGANIZATIONAL PERFORMANCE IN THE BANKING
SECTOR: EVIDENCE FROM NIGERIA**

By

BABATUNDE DORCAS ADEBOLA

**Thesis submitted to the
Othman Yeop Abdullah Graduate School of Business,
Universiti Utara Malaysia,
In Fulfillment of the Requirement for the Degree of Doctor of Philosophy**



Kolej Perniagaan
(College of Business)
Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

BABATUNDE DORCAS ADEBOLA

calon untuk Ijazah **DOCTOR OF PHILOSOPHY**
(candidate for the degree of)

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

THE DETERMINANT OF INFORMATION SECURITY PRACTICES TOWARDS ORGANIZATIONAL PERFORMANCE IN THE BANKING SECTOR : EVIDENCE FROM NIGERIA

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada:

29 Disember 2013.

(That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:

29 December 2013).

Pengerusi Viva : **Assoc. Prof. Dr. Azhar bin Abd. Rahman**
(Chairman for Viva)

Tandatangan
(Signature)

Pemeriksa Luar : **Assoc. Prof. Dr. Omar bin Zakaria**
(External Examiner)

Tandatangan
(Signature)

Pemeriksa Dalam : **Assoc. Prof. Dr. Chek bin Derashid**
(Internal Examiner)

Tandatangan
(Signature)

Tarikh: **26 Disember 2013**
(Date)

Nama Pelajar
(Name of Student)

: Babatunde Dorcas Adebola

Tajuk Tesis / Disertasi
(Title of the Thesis / Dissertation)

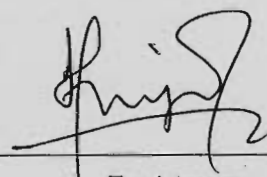
: The Determinant of Information Security Practices towards
Organizational Performance in the Banking Sector : Evidence
from Nigeria

Program Pengajian
(Programme of Study)

: Doctor of Philosophy

Nama Penyelia/Penyelia-penyelia
(Name of Supervisor/Supervisors)

: Dr. Mohamad Hisyam bin Selamat



Tandatangan

PERMISSION TO USE

In presenting this thesis in fulfillment of the requirements for the degree of Doctor of Philosophy (PhD) in University Utara Malaysia. I hereby agree that the University Library may have free access to this thesis for academic use. I also agree that permission to copy the thesis in any form, whole or in part for scholarly purpose, may be granted by my supervisor or, in the absence by the dean of Othman Yeop Abdullah Graduate School of Business.

It is understood that any copying or publication of this thesis or part of it is therefore for the purpose of financial gains shall not be allowed without the prior knowledge shall be given to me and the Universiti Utara Malaysia for any scholarly use which may made of any of the material from this thesis.

Request for permission to copy or make other use of materials in this thesis in whole or in part should be addressed to:

Dean of Othman Yeop Abdullah Graduate School of Business,

Universiti Utara Malaysia,

06010 Sintok,

Kedah Darul Aman, Malaysia.

ABSTRACT

This study examines the determinant factors of information security practices towards organizational performance among Nigerian banks. To achieve this, a framework that consists of technological, organizational, and environmental (TOE) factors is proposed using information security culture as a mediator of TOE factors. The framework identifies the factors influencing information security practices among Nigerian bankers. Findings using TOE will eventually lead to the improvement of organizational performance through the establishment of information security culture among Nigerian banks. Thus, the use of information security practices will assist in reducing human factors such as errors, failures, internal incidents and social engineering attacks. A questionnaire survey was designed to obtain data on information security culture, organizational performance, organizational, environmental and technological factors. Multiple regression was used to test for the relationship between organizational performance, information security culture, TOE factors and the reliability and validity of the data. The findings indicated that perceived technology advancement, information security policy and procedure, international security standard, information security awareness, perceived training programs, motivation of employee and perceived job roles and responsibilities significantly influence the organizational performance. The remaining variables have no statistically significant influence on organizational performance. Also, this study found that information security culture significantly mediates the relationship between organizational performance and TOE factors. Thus, the result of this study shows that the objectives of this study were achieved.

Key words: organizational performance, information security practices, TOE factors, information security culture

ABSTRAK

Kajian ini mengkaji penentu amalan sekuriti maklumat terhadap prestasi organisasi di kalangan bank-bank di Nigeria. Untuk mencapai matlamat ini, satu rangka kerja yang terdiri daripada faktor-faktor teknologi, organisasi, dan alam sekitar (TOE) dicadangkan menggunakan budaya sekuriti maklumat sebagai faktor pengantara TOE . Rangka kerja ini mengenal pasti faktor-faktor yang mempengaruhi amalan sekuriti maklumat di kalangan bank-bank di Nigeria. Ini boleh membawa kepada peningkatan prestasi organisasi melalui pembentukan budaya sekuriti maklumat antara bank-bank di Nigeria. Dengan ini, ia membantu mengurangkan faktor-faktor kemanusiaan seperti kesilapan manusia, kejadian dalaman dan serangan kejuruteraan sosial. Satu soal selidik telah digunakan untuk mendapatkan data mengenai budaya sekuriti maklumat, prestasi organisasi, faktor-faktor teknologi, organisasi dan alam sekitar. Regresi berganda telah digunakan untuk menguji hubungan antara prestasi organisasi, budaya sekuriti maklumat, faktor-faktor TOE dan kebolehpercayaan dan kesahihan data. Dapatan kajian menunjukkan bahawa kemajuan teknologi, dasar sekuriti maklumat dan prosedur, tahap sekuriti antarabangsa, kesedaran orang ramai terhadap sekuriti maklumat , program-program latihan, motivasi pekerja dan peranan kerja dan tanggungjawab dengan nyata dapat mempengaruhi prestasi organisasi. Pembolehubah berikutnya tidak mempunyai pengaruh yang besar ke atas statistik prestasi organisasi. Selain itu, kajian ini mendapati bahawa budaya sekuriti maklumat mengurangkan dengan ketara hubungan di antara prestasi organisasi dan faktor-faktor TOE. Oleh itu, dapatan daripada kajian ini menunjukkan objektif kajian ini telah tercapai.

Kata kunci: prestasi organisasi, amalan sekuriti maklumat, faktor-faktor TOE, budaya sekuriti maklumat

ACKNOWLEDGEMENT

With gratitude in my heart to the almighty God, the giver of wisdom who has bestowed His love and mercy on me in achieving my PhD dreams. Unto Him be all adoration forever and ever. I am indeed indebted to several people, Nigerian Banks, friends and family. Most especially I am grateful to my supervisor Associate Prof. Dr Mohamad Hisyam Selamat for his immensely guidance, support and encouragement throughout my program. I also want to appreciate Professor Dr. Mohamad Tayib the former Vice Chancellor of the College of Business, Professor Dr. Azizi Ismail, the dean of Othman Yeop Abdullah Graduate School of Business (OYAGSB) and all the staff of OYAGSB for making my stay in Universiti Utara Malaysia an unforgettable experience.

My most appreciation goes to my hubby, Prince Daniel M. Babatunde; and my loving children, Prince Daniel Adedamola Babatunde, Princess Daniella Damiloia Babatunde and Prince Jesse Toluwanimi Adewale Babatunde for their invaluable support, prayers, encouragement and endurance during my program cannot be quantified. The appreciation will not be complete without special thanks to Associate Professor Omar Zakaria, Associate Professor Chek Derashid for their comments and invaluable suggestions during my PhD proposal defense and viva in making the thesis a better one. Also, my sincere appreciation goes to Mr Popoola, O.M. J, Dr Saliu Abdulwahaab Adelabu, for their moral supports and encouragement at the very crucial time when the going seems so tough, knowing for sure that a friend in need is a friend indeed. Lastly, to all my extended families, I pray that God in His infinite mercy will bless you all. Appreciate a lot.

TABLE OF CONTENT

| Title | Page |
|-----------------------------------|------|
| TITLE PAGE | i |
| CERTIFICATE OF THESIS WORK | ii |
| PERMISSION TO USE | iv |
| ABSTRACT | v |
| ABSRAK | vi |
| AKNOWLEDGMENT | vii |
| TABLE OF CONTENT | viii |
| LIST OF TABLES | ix |
| LIST OF FIGURES | xx |
| LIST OF ABBREVIATIONS | xxi |
| CHAPTER ONE-INTRODUCTION | 1 |
| 1.1 Research Background | 1 |
| 1.2 Problem Statement | 6 |
| 1.3 Research Questions | 12 |
| 1.4 Research Objectives | 12 |
| 1.5 Scope of Study | 13 |
| 1.6 Significant of the Study | 13 |
| 1.7 Organization of the Thesis | 14 |
| 1.8 Definitions of Crucial Terms | 15 |
| 1.9 Summary | 18 |

| | |
|--|----|
| CHAPTER TWO-LITERATURE REVIEW | 20 |
| 2.1 Introduction | 20 |
| 2.2 Overview of the Nigerian Banking Sector | 21 |
| 2.3 Information Security | 21 |
| 2.3.1 Information Security Governance | 22 |
| 2.3.2 Information Security Management | 24 |
| 2.3.3 Information Technology Governance | 25 |
| 2.3.4 Information Security Culture | 28 |
| 2.4 The Importance of Information Security Culture | 31 |
| 2.5 The Relationship between Information Security Culture and OP | 32 |
| 2.6 Establishment of Information Security Culture | 33 |
| 2.6.1 Technological Factors | 34 |
| 2.6.1.1 Perceived Technology Advancement | 35 |
| 2.6.1.2 Information Security In-sourcing | 36 |
| 2.6.2 Environmental Factors | 37 |
| 2.6.2.1 International Security Standard | 38 |
| 2.6.2.2 Perceived Government Rules and Regulations | 40 |
| 2.6.3 Organizational Factors | 41 |
| 2.6.3.1 Size of the Organization | 42 |
| 2.6.3.2 Information Security Development | 43 |
| 2.6.3.2.1 Information Security Awareness | 44 |
| 2.6.3.2.2 Information Security Policy and Procedure | 46 |

| | |
|--|----|
| 2.6.3.2.3 Perceived Training Programs | 48 |
| 2.6.3.3 Perceived Information Security, Threat and Vulnerabilities | 50 |
| 2.6.3.4 Motivation of Employees | 55 |
| 2.6.3.5 Perceived Top Management Support and Commitment | 58 |
| 2.6.3.6 Perceived Job Roles and Responsibilities | 59 |
| 2.7 Information Security Culture as a Mediating Variable | 60 |
| 2.8 Organizational Performance as a Dependent Variable | 64 |
| 2.9 Underpinning Theory | 66 |
| 2.10 The Proposed Theoretical Framework | 68 |
| 2.11 Summary | 70 |
| CHAPTER THREE- RESEARCH METHODOLOGY | 72 |
| 3.1 Introduction | 72 |
| 3.2 Hypothesis Development | 72 |
| 3.2.1 The Direct Effect | 72 |
| 3.2.1.1 Perceived Technology Advancement | 73 |
| 3.2.1.2 Information Security In-sourcing | 73 |
| 3.2.1.3 International Security Standard | 74 |
| 3.2.1.4 Perceived Government Rules and Regulations | 74 |
| 3.2.1.5 Size of the organization | 75 |
| 3.2.1.6 Information Security Awareness | 76 |
| 3.2.1.7 Information Security Policy and Procedure | 77 |
| 3.2.1.8 Perceived Training Programs | 78 |

| | |
|---|-----|
| 3.2.1.9 Perceived Information Security Threat, Risks and Vulnerabilit | 80 |
| 3.2.1.10 Motivation of Employee | 81 |
| 3.2.1.11 Perceived Top Management Support and Commitment | 82 |
| 3.2.1.12 Perceived Job Roles and Responsibilities | 83 |
| 3.3 The Indirect Effect | 86 |
| 3.3.1 Information Security Culture as a Mediating Variable | 86 |
| 3.3.1.1 Test of a Casual Steps | 87 |
| 3.3.1.2 Product of Coefficient Test | 89 |
| 3.4 Research Design | 91 |
| 3.5 Research Equation | 92 |
| 3.5.1 Simple Regression Analysis | 94 |
| 3.5.2 Multiple Regression Analysis | 94 |
| 3.5.2.1 Direct Relationship Equation 1 and 2 | 95 |
| 3.5.2.2 Indirect Relationship Equation 2 | 95 |
| 3.6 POPULATION AND SAMPLE | 97 |
| 3.6.1 Population | 97 |
| 3.6.2 Sample of the Study | 97 |
| 3.6.3 Sampling Framework | 100 |
| 3.7 Research Activities | 102 |
| 3.7.1 Research Instrument Development | 102 |
| 3.7.2 Data Collection | 103 |
| 3.7.3 Data Analysis Technique | 104 |

| | | |
|------------|--|------------|
| 3.7.3.1 | Test for Difference | 104 |
| 3.7.3.2 | Descriptive Statistics | 105 |
| 3.7.3.3 | Factor Analysis | 105 |
| 3.7.3.4 | Correlation Analysis | 106 |
| 3.7.3.5 | Multiple Regression Analysis | 107 |
| 3.8 | OPERATION OF VARIABLES | 109 |
| 3.8.1 | Organizational Performance | 110 |
| 3.8.2 | Perceived Technology Advancement | 110 |
| 3.8.3 | Information Security In-sourcing | 110 |
| 3.8.4 | International Security Standard | 111 |
| 3.8.5 | Perceived Government Rules and Regulations | 111 |
| 3.8.6 | Size of the organization | 111 |
| 3.8.7 | Information Security Awareness | 112 |
| 3.8.8 | Information Security Policy and Procedure | 112 |
| 3.8.9 | Perceived Training Programs | 113 |
| 3.8.10 | Perceived Information Security Threat, Risks & Vulnerabilities | 114 |
| 3.8.11 | Motivation of Employee | 114 |
| 3.8.12 | Perceived Top Management Support and Commitment | 114 |
| 3.8.13 | Perceived Job Roles and Responsibilities | 115 |
| 3.8.14 | Perceived Technology Advancement | 115 |
| 3.9 | Summary | 116 |

| | |
|---|-----|
| CHAPTER FOUR-RESEARCH INSTRUMENT DEVELOPMENT | 117 |
| 4.1 Introduction | 117 |
| 4.2 Questionnaire Development | 117 |
| 4.2.1 The Organization of the Questionnaire | 118 |
| 4.2.2 Organizational Performance | 119 |
| 4.2.3 Technological Factors | 119 |
| 4.2.4 Organizational Factors | 120 |
| 4.2.5 Environmental Factors | 121 |
| 4.2.6 Information Security culture | 121 |
| 4.3 Refinement of Questionnaire | 123 |
| 4.3.1 Validity Test | 123 |
| 4.3.2 Pilot Test | 124 |
| 4.4 Reliability | 125 |
| 4.5 Reliability Test on Pilot Test | 125 |
| 4.6 Summary | 126 |
| CHAPTER FIVE-DATA ANALYSIS AND FINDINGS | 127 |
| 5.1 Introduction | 127 |
| 5.2 Respondents Rate | 128 |
| 5.2 Non-Respondents Rate | 131 |
| 5.3 Information Security | 131 |
| 5.4 Data Cleaning | 131 |
| 5.4.1 Treatment of Outliers among Cases | 131 |

| | | |
|---------|---|-----|
| 5.4.2 | Normality Test | 131 |
| 5.4.3 | Multicollinearity Test | 133 |
| 5.4.4 | Homoscedasticity | 134 |
| 5.5 | Demographic Information of the Respondents | 135 |
| 5.5.1 | Position of the Respondents | 135 |
| 5.5.2 | Gender of the Respondents | 136 |
| 5.5.3 | Age of the Respondents | 137 |
| 5.5.4 | Marital Status of the Respondents | 138 |
| 5.5.5 | Level of Education of the Respondents | 138 |
| 5.5.6 | Experience of the Respondents | 139 |
| 5.5.7 | Number of Employees in the Respondents' Bank | 140 |
| 5.5.8 | Overall Employees in the Respondents' Bank | 141 |
| 5.5.9 | Establishment of Information Security Culture | 142 |
| 5.6 | Goodness of Measure | 144 |
| 5.6.1 | Validity Test After FA | 145 |
| 5.6.2 | Reliability Test After FA | 146 |
| 5.6.3 | Construct Validity | 146 |
| 5.6.3.1 | Factor Analysis of Organizational Performance | 147 |
| 5.6.3.2 | Factor Analysis of Technological Factors | 150 |
| 5.6.3.3 | Factor Analysis of Organizational Factors | 153 |
| 5.6.3.4 | Factor Analysis of Environmental Factors | 161 |
| 5.6.3.5 | Factor Analysis of Information Security Culture | 163 |

| | | |
|-------|---|-----|
| 5.7 | The Restatement of Hypothesis | 168 |
| 5.8 | Descriptive Statistics of All Variables | 170 |
| 5.8.1 | Descriptive Statistics of Technological Factors | 171 |
| 5.8.2 | Descriptive Statistics Organizational Factors | 172 |
| 5.8.3 | Descriptive Statistics of Environmental Factors | 173 |
| 5.8.4 | Descriptive Statistics of Information Security Factors | 174 |
| 5.8.5 | Descriptive Statistics of Organizational Performance | 174 |
| 5.9 | Correlation Analysis | 175 |
| 5.10 | Multiple Regression Analysis | 177 |
| 5.11 | Testing for Model Using Multiple Regression | 178 |
| 5.12 | Hierarchical Multiple Regression | 182 |
| 5.13 | Research Hypothesis: Test Result | 184 |
| 5.14 | Refining of Framework | 184 |
| 5.15 | Summary | 188 |
| | CHAPTER SIX-DISCUSSION OF FINDINGS | 190 |
| 6.1 | Introduction | 190 |
| 6.2 | Implication to the Practical Setting | 190 |
| 6.2 | Research Question 1: How Element of TOE Factors Influence Organizational Performance | 190 |
| 6.3 | Research Question 2: What is the Relationship between IS Practices and Information Security Culture | 191 |
| 6.4 | Research Question 3: To Examine Whether ISC Mediate the Relationship between TOE Factors and Organizational Performance | 197 |

| | | |
|-----|--|-----|
| 6.5 | Research Question 1: How Element of TOE Factors Influence Organizational Performance | 198 |
| 6.6 | Summary | 205 |
| | CHAPTER SEVEN- SUMMARY AND CONCLUSION | 206 |
| 7.1 | Introduction | 206 |
| 7.2 | Summary | 208 |
| 7.3 | Research Contribution | 208 |
| | 7.3.1 Academia Contribution | 208 |
| | 7.3.2 Managerial Contribution | 210 |
| | 7.3.3 Practical Contribution | 211 |
| 7.4 | Limitation of the Study | 212 |
| 7.5 | Suggestions for Future Study | 213 |
| 7.6 | Conclusion | 214 |
| | REFERENCES | 216 |
| | APPENDIXES | 253 |
| | Appendix A Number of Consolidated Nigerian Banks | 254 |
| | Appendix B-1 Map of Nigeria | 255 |
| | Appendix B-2 Data Collection Letter | 256 |
| | Appendix B-3 Sample of Determination for a Given Population | 257 |
| | Appendix B-4 Determination of Sample Size | 259 |
| | Appendix B-5 Determination of Appropriate Sample in Survey Research | 261 |
| | Appendix C-1 Survey Questionnaire | 263 |
| | Appendix D-1 Factor Solution and Reliability of OP | 272 |

| | |
|--|-----|
| Appendix D-2 Factor Solution and Reliability of ISC | 276 |
| Appendix D-3 Factor Solution and Reliability of Technological Factors | 279 |
| Appendix D-4 Factor Solution and Reliability of Organizational Factors | 284 |
| Appendix D-5 Factor Solution and Reliability of Environmental Factors | 288 |
| Appendix E-1 Multiple Regression Analysis on OP and TOE Factors | 310 |
| Appendix E-2 Multiple Regression Analysis on ISC and TOE Factors | 314 |
| Appendix E-3 Hierarchical Multiple Regression Analysis | 315 |
| Appendix G List of Journal Publications from the Thesis | 317 |

LIST OF TABLES

| Table | | Page |
|-----------|---|------|
| Table 1.1 | The Fraud and Forgeries Cases Reported to the NDIC | 8 |
| Table 2.1 | Summary of Literature Review | 71 |
| Table 3.1 | Summary of the Hypothesis on TOE Factors and Organizational Performance | 84 |
| Table 3.2 | Summary of the Hypothesis on TOE Factors and ISC | 85 |
| Table 3.3 | Summary of Mediating Effect of ISC on ISP and Op | 90 |
| Table 3.4 | Numbers of Nigerian Consolidated Banks | 97 |
| Table 3.5 | Distribution of Questionnaire among Banks | 101 |
| Table 4.1 | The Items and the Sources Related to Organizational Performance | 119 |
| Table 4.2 | The Items and the Sources Related to Technological Factors | 119 |
| Table 4.3 | The Items and the Sources Related to Organizational Factors | 120 |
| Table 4.4 | The Items and the Sources Related to Environmental Factors | 121 |
| Table 4.5 | The Items and the Sources Related to Information Security Culture | 122 |
| Table 4.6 | Summary of Organization of the Question on ISC | 122 |
| Table 4.7 | Reliability Analysis of Pilot Test | 126 |
| Table 5.1 | Respondent Rate of the Questionnaire | 128 |
| Table 5.2 | Test of Non- Respondents Bias using Independent Sample Test | 130 |
| Table 5.3 | Respondents' Position | 136 |
| Table 5.4 | Respondents' Gender | 137 |
| Table 5.5 | Respondents' Age | 137 |
| Table 5.6 | Respondents' Marital Status | 138 |
| Table 5.7 | Respondents' Level of Education | 139 |
| Table 5.8 | Respondents' Experience | 140 |
| Table 5.9 | Respondents' Number of Branches | 141 |

| | | |
|-------------|--|-----|
| Table 5.10 | Respondents' Overall Number of Branches | 142 |
| Table 5.11 | Respondents Rate on Establishment of ISC | 142 |
| Table 5.12 | The Summary of Respondents' Profile | 143 |
| Table 5.13 | KMO,MSA,BTS and Significant Factor of OP | 147 |
| Table 5.14 | The Extracted Component of OP | 148 |
| Table 5.15 | Factor Loading for OP Using Varimax Rotation | 149 |
| Table 5.16 | Summary of Cronbach's Alpha of Op | 150 |
| Table5.17a | KMO,MSA,BTS and Significant for PTA Factor | 151 |
| Table 5.17b | Extraction of Component for PTA | 151 |
| Table 5.18a | Total Variance Explained of PTA | 152 |
| Table 5.18b | Total Variance Explained of ISI | 152 |
| Table 5.19 | Summary of Reliability Test of Technological Factor | 153 |
| Table 5.20 | Summary of Reliability Test of Organizational Factor | 160 |
| Table 5.21 | KMO,MSA,BTS and Significant of ISS | 161 |
| Table 5.22 | Total Variance Explained of ISS | 161 |
| Table 5.23 | Factor Loading of ISS | 162 |
| Table 5.24a | KMO,MSA,BTS on PGRR | 162 |
| Table 5.24b | Total Variance Explained of PGRR | 163 |
| Table 5.25 | Summary of Reliability Test of Environmental Factor | 163 |
| Table 5.26 | The KMO,MSA,BTS on ISC | 164 |
| Table 5.27 | Extraction Component of ISC | 164 |
| Table 5.28 | Factor Loading Reliability Test of ISC | 165 |
| Table 5.29 | Summary of Reliability Test of ISC | 165 |
| Table 5.30 | Summary of Validity and Reliability Result | 166 |
| Table 5.31 | Final Variables for Further Analysis | 167 |
| Table 5.32 | Restatement of Hypothesis | 169 |

| | | |
|------------|--|-----|
| Table 5.33 | Descriptive Statistics of Technological Factors | 172 |
| Table 5.34 | Descriptive Statistics of Environmental Factors | 173 |
| Table 5.35 | Descriptive Statistics of Information Security Culture | 174 |
| Table 5.36 | Descriptive Statistics of Organizational Performance | 175 |
| Table 5.37 | Guilford Rule of Thumb | 176 |
| Table 5.38 | Correlation Analysis | 177 |
| Table 5.39 | Anova Result on TOE Factors and OP | 180 |
| Table 5.40 | Coefficient Value of TOE Factors and OP | 180 |
| Table 5.41 | Anova Result on TOE Factors and ISC | 181 |
| Table 5.42 | Coefficient Value of TOE Factors and ISC | 182 |
| Table 5.43 | Anova Result on TOE Factors ISC and OP | 183 |
| Table 5.44 | Coefficient Value of TOE Factors , ISC and OP | 184 |
| Table 5.45 | Summary of Hypothesis Testing | 185 |

LIST OF FIGURES

| Figure | | Page |
|------------|--|------|
| Figure 1.1 | Information Transformation within the Organization | 4 |
| Figure1.2 | Improved Organizational Performance Through ISC | 11 |
| Figure 2.1 | Information Security Transformation | 22 |
| Figure 2.2 | Adjusted Risk Data Repository | 53 |
| Figure 2.3 | The Proposed Theoretical Framework | 70 |
| Figure 5.1 | Normal P-Plot of Regression Standardized Residual | 133 |
| Figure 5.4 | The Revised Theoretical Framework | 187 |

LIST OF ABBREVIATION

| | |
|--------|--|
| NDIC | Nigeria Deposit Insurance Corporation |
| OP | Organizational Performance |
| ISC | Information Security Culture |
| ISM | Information Security Management |
| IS | Information System |
| ISS | International Security Standard |
| CBN | Central Bank of Nigeria |
| NSE | Nigeria Stock Exchange |
| ISMS | Information Security Management System |
| IT | Information Technology |
| ICT | Information Communication Technology |
| CPA | Certified Public Accountant |
| ISO | International Organization for Standardization |
| EDPD | European Data Privacy Directive |
| GLBA | Gramm-Leach-Bliley Act |
| SOX | Sarbanes-Oxley-Act |
| BSI | British Standard Institute |
| IMF | International Monetary Fund |
| SEC | Security Exchange Commission |
| FFIEC | Federal Financial Institute Examinations Council |
| NSTISS | National security Telecommunication and Information System |

CHAPTER ONE

INTRODUCTION

1.1 Research Background

The global era of technology advancement brought about changes in the operational perspectives of the organization in order to improve the performance of business activities (Wang & Zhao, 2011; Parsons, McCormac, Butavicious & Feguson, 2010). This increases the volume of sales on one hand and the profit growth on the other. These changes affect performance within an organization either positively or negatively. Information and communication technology (ICT) through the use of the internet reduces the world to the global village. The effective use of ICT has been the concern of organizations on sharing information through the internet (Wang & Zhao, 2011; Parsons et al., 2010). It is postulated by Parsons et al. (2010) that organizations are on the verge of losing information to social engineering attack, knowing for sure that human is the greatest target of social engineering attack.

The attack on information defeats the objectives of confidentiality, integrity and availability (Akinsuyi, 2009; Qingxiong, Schmidt, Herberger, & Parsons, 2009). Many organizations consider the information to be the basis of knowledge because it is the business “actionable” and any organization that loose information, lack competitive advantage and cannot survive because of performance deterioration (Brotby, 2009; Drucker, 1993). Thus, it calls for information security culture that provide a platform for

relevant and reliable information processing for decision making through responsible staff members. Information security therefore becomes inevitable in the organization.

The Information Security Audit and Control Association (ISACA, 2012) defines information security as the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction ensuring that objectives are delivered ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. In lieu of the ISACA definition on information security governance, Organization for Economic Cooperation and Development (OECD) argues that information security should include the "structure through which the objectives of the enterprises are set and the means of sustaining those objectives and monitoring performance are determined" (Parsons et al., 2010; ISO 27001: 2005; OECD Guidelines, 2005). In tandem with the above definitions, this study defines information security culture as the ability of the management to protect information through proper information security practices in order to enhance better performance in the organization.

The aim of information security is to protect information from uncalled and unauthorized act which could lead to threat with the use of computer (Elchagar, Bouladour, Makoudi & Regragui, 2012; Huang, Rau & Salvendy 2007; Hong, Chi, Chao & Tang, 2003). Thus, the purpose of information security is to ensure confidentiality, availability and integrity of information within the organization (Huang, et al., 2007; Brown & Heywood, 2005). Securing and protecting information asset brings structure and governance to the

information security function within an organization (Elchagar et al., 2012; Pivonti, 2005). Also, it allows business continuity; to keep pace with legal compliance and achieving competitive advantage organization. Therefore, practising information security is secondary to the need to make a profit (Kruger & Kearney, 2006). Scholars are of the opinion that organizations will continue to depend on information system for strategic and operational advantages and therefore the implementation of information security becomes inevitable in the organization. The need therefore arises for the organization to establish information security culture to avert information risk and threats which can hinder organizational competitive advantage (Parsons et al., 2010; Kankanhalli, Teo, Tan & Wei, 2003).

From the above discussion, it can be seen that the first and foremost thing in the process of establishing information security is responsible staff members. Thus, understanding factors that can motivate staff members to diligently and sincerely implement information security activities is critical. Zakaria (2013) stated that information securities activities lead to information routines and in turn information security norms and ultimately information security culture. This continuum is illustrated in Figure 1.1. In other words, when discussing about responsible staff members in information security implementation, it is closely related to the establishment of information security culture. Thus the focus of this study is factors or activities influencing the establishment of information security culture in the organizations.

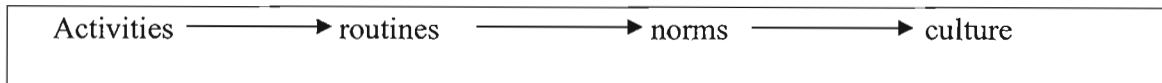


Figure 1.1
Information Security Transformation within the Organization (Zakaria, 2013)

As information security is related to the establishment of business investment, value and continuity, linking it to organizational performance is evitable (Von Solms, 2005; Andress, 2002; 1999). Its absence could lead to financial loss, negative publicity, lawsuits and permanent damage to the business. Major components of information security culture are about the availability of human, technology and process. If these components are not provided, e-fraud, cybercrime committed by the fraudsters through social engineering attack, hacking and phishing could occur (Parsons et al., 2010; Isiavwe, 2010; Anderson, 2008; Aiello, 2008; Workman, 2008; Badamas, 2008). All these phenomena lead to low performance of the organizations. Thus, this study intends to relate information security culture to organizational performance.

The sector that requires a comprehensive information security activities is banking. This is because of its financial nature of business. There are many financial scandals and crimes that occur in Nigeria (Akinsuyi, 2009). Thus, investigating information security culture in Nigerian banks is timely and thus becomes the interest of this study.

From the above discussion, it is clear that information security culture is the mediating factor in going-to-be developed framework of this study. It is obvious that few studies have been conducted on information security culture but not information security

culture as a mediating variable between information security practices and organizational performance in Nigerian banks in particular. Descriptively, it is observed that information that are collected, processed and stored electronically are exposed to the risks of theft and can easily be attacked by fraudsters (Soludo, 2010, 2009; Half year report by the Nigerian Capital Market, 2009; Owolabi, 2007). Hence, a clarion calls on information security infrastructure because if top secret information falls into the wrong hands, this could lead to a breach of security with negative consequences.

In addition, the role of banks in the development of the economy in the western world had been discussed in the literature (Dongli, 2009; Evans, 2008). This should also be applicable to emerging economies like Nigeria. the best of the researcher's knowledge, not much study was done on information security culture as a mediating variable on the relationship between information security practices and organizational performance in Nigeria. The Nigerian banking sector experience drastic growth during the post consolidation, thus; the industry and the regulators are not sufficiently prepared to sustain and monitor the explosive growth of the banking sector and as such performance was reduced (Soludo, 2010, 2009; Half year report by the Nigerian Capital Market, 2009; Owolabi, 2007). Hence, sophisticated and effective information security activities are required in any organizations including banks. This is to ensure business competitiveness and survivability.

To recapitulate, this study intends to examine the determinants of information security culture for effective and efficient business activities in achieving organizational

performance in the banking sector in Nigeria. This is to avoid the risks associated with information security failure caused by human failure of inappropriate security practices, inappropriate standard, policies and procedures. Having described the background of this study, the next section will be dedicated to the problem statement of the research.

1.2 Problem Statement

The organizations value information security culture because it plays a vital role in the overall response leading to competitive advantage in the global market (Babatunde & Selamat 2012; Alnatheer & Nelson, 2009). In line with the thought of Babatunde et al. (2012), Alnatheer et al. (2009) argued that the establishment of information security give a better performance within the organization.

One of the performance indicators is profit figure which is derived from Accounting Information System (AIS). AIS is defined as a collection of resources utilized to transform financial and other data into usable information (Gabrasilase & Lessa, 2011; Bodnar & Hopwood 2010). The explicit knowledge of AIS indicates that three factors were involved, namely technology, process and human factors that produce the confidentiality, integrity and availability (Parson et al., 2010; Huang, 2007; Brown et al; 2006).

When information security is not properly secured and managed, it causes chaos due to unwillingness of employees to handle security challenges (Shahri & Ismail, 2012; Parson et al., 2010; Alnatheer & Nelson, 2009; Finne, 1998). Therefore, information asset must

be well protected through the establishment of information security culture. This in turn ensures the achievement of organizational objectives and enhances organizational performance. Therefore, failure to establish good information security culture exposes an organization to the following characteristics of the threats: (1) confidentiality such as theft of data; (2) integrity such as virus attack or alteration on files or document, social engineering attack and (3) availability such as denial of service (Parson et al., 2010; Huang, 2007; Brown et al; 2006; Gordon et al; 2006; Gragg, 2002).

According to the International Federation of Information Processing Working Group (IFIPWG) 11.1, information security activities cover a range of issues from both management and technical aspects that support the establishment of information security culture (IFIP, 1992). In other words, information security practices consist of operational, technical and human elements that develop information security culture among employees (Huang et al. 2007; Besnard & Arief, 2004; Kenning, 2001). Thus, it focuses on how to reduce malicious acts through a robust information security culture within the organizations. There will be a chaos if human factors are not given adequate consideration, such human factors as error, failures, non-competence of the employees, inappropriate information security practices, and social engineering attacks (Parsons et al., 2010; Huang, et al., 2007; Chan et al., 2005).

Aeilo (2008) argued that personality traits are vulnerable to social engineering attack because it is likely to appear to be legitimate and if the attacker can form a rapport with the victim, this makes them vulnerable to instruction. Vulnerability to security attack

could be associated with individual trust. In vulnerable situation, succumbing to social engineering attack is quite possible (Workman, 2008). In order to correct the defect of vulnerability through the human and attack. Proper information security practices and information security culture need to be implemented.

The banking sector crisis in Nigeria is linked to lack of information security culture and information technology (IT) gap (Martins & Odunfa, 2012; Olugbode et al., 2008). The crisis could have been restrained to a large extent if the supervisory process are driven by adequate IT tools. IT brought about significant changes in the way banks process and store data. In addition, the telecommunication networks play a positive role in the expansion and integration of the information systems, within and among banks facilitating data accessibility to different users (Martins & Odunfa, 2012; Olugbode et al., 2008). Frauds result in huge financial losses to banks and their customers because of ineffective information security practices. Please refer to Table 1.1 for details.

Table 1.1
Fraud and Forgery Cases Reported to NDIC

| Year | Number of Reported Cases | The amount involved (Millions) | Expected/ Actual Loss (Millions) |
|------|--------------------------|--------------------------------|----------------------------------|
| 1998 | 573 | 3,196.51 | 692.25 |
| 1999 | 195 | 7,404.28 | 2,730.06 |
| 2000 | 403 | 2,851.11 | 1,080.57 |
| 2001 | 943 | 11,243.94 | 906.30 |
| 2002 | 796 | 12,919.55 | 1,299.69 |

Source: Nigerian Deposit Insurance Corporation (NDIC)

This study is in response to the human-based information security errors that brought about the failure which could be termed as lack of information security culture in the

Nigerian banking (Asai & Fernando, 2011; Parsons et al, 2010; Huang et al., 2010; Samy et al., 2009; Hearth & Rao, 2009; Ehikamenor, 2003).

However, scholars on information security argued that people are the most important security component (Shahri & Ismail, 2012; Williams, 2009; Ma et al., 2008; Parsons et al., 2010; Andersons, 2002). In the organizational settings, people such as employees, management (Chief Information Security Officer, Chief Information Officer) or board of directors forms an integral part of the security system and people are often overlooked as part of the security components (Parsons et al., 2010; Shahri & Ismail, 2010; Andress, 2008; 2002). In turn, it is also imperative that the users must understand how to protect the organizational information. Thus, there is a clarion call for information security activities and in turn information security culture among the employees that will foster effective business activities for a better performance. In short, the rising of security breaches and computer hackers require an organization to put in place security measure to survive (Asai & Fernando, 2011; Samy et al., 2009).

Previous researchers revealed that majority of the security flaws are attributed to system administrators' failure to update software patches and the desire to remain on the top of the latest development in the information security world (Eloff & Eloff, 2003). Although information security is more of human failures rather than technological, security alertness cannot be achieved through technological tools because information security

breaches are caused by human factors (Asai & Fernando, 2011; Samy et al., 2009; Hearth & Rao, 2009).

The bone of contention here is the failure in system administration as a result of human failure. It should be noted that people handle the systems and no systems can operate on its own. The human factor such as failure is attributed to the culture and/or workload of administrators. The increasingly complex system also requires administrators to be expert in various technologies, which are often beyond the comprehension of many systems administrators (Shahri & Ismail, 2012; Stranders et al., 2009; DiArcy et al., 2009; Van Niekerk & Von Solms, 2007; Bianco, 2001).

By and large, Enron Company could have still been in existence today if its information had not been destroyed by the irresponsible top management. But with the promulgation of Sarbanes-Oxley Act (SOX Act, 2002), loss of organizational information are now being protected. Hence, without an information securities practices planned by the management, the organizations are exposed to security threats and vulnerabilities; and this inevitably leads to security breaches (Lechler, et al., 2011; Huang et al., 2007; Samy et al., 2009; Von Solms, 2005; 2000). Researchers in information security area regard human factor as the weakest link in a security solution (Parsons et al., 2010; Huang,et al., 2007; Besnard & Arief, 2004). This requires a comprehensive action to establish information security culture amongst employees in order to avoid irresponsible actions that can jeopardize performance of the organizations.

However, other activities that could resolve security issues includes employing appropriately skilled resources, the development and implementation of policies and procedures, conducting risk assessments, training programs and educational awareness along with top management support and security standards. As suggested by Zakaria (2013), all these activities will become routine, in turn routine becomes norm and in turn norm becomes culture in the organization. This study intends to investigate this continuum from the perspective of Nigerian banks.

The Nigerian banks are faced with the challenges of how to secure their information from the fraudsters. Therefore, the need to establish an effective information security culture arises. It is paramount to establish information security culture within the banking sector. This will reduce risks associated with security breaches and non implementation of information security practices that will affect organizational performance negatively. This is illustrated in Figure 1.2 below as:

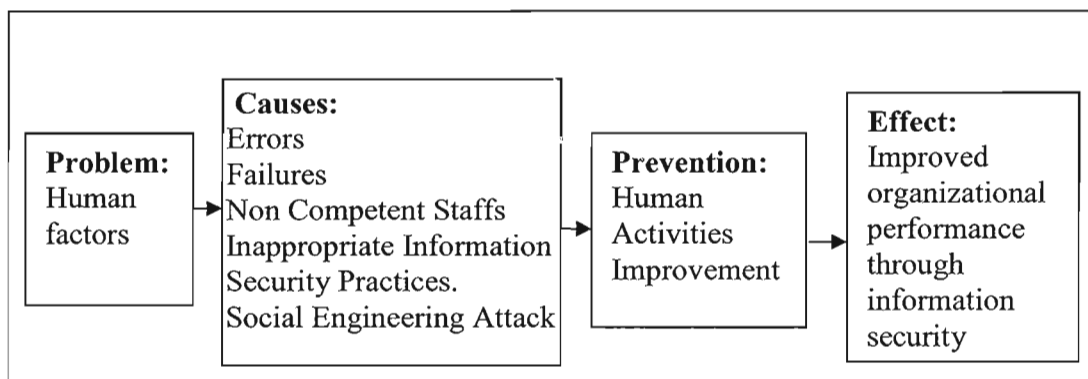


Figure 1.2
Improved Organizational Performance through Information Security Culture

In line with previous studies, this study focuses on improving human activities in order to ensure effective implementation of information security practices. This in turn will create information security culture within the organization. There will be a chaos if human factors are not given adequate consideration. Few of these human factors as enumerated by Parsons et al. (2010), Huang, et al. (2007) and Chan et al., (2005) are error failures, non-competence of the employees, inappropriate information security activities and social engineering attacks. This study therefore wants to investigate all these issues in details.

1.3 Research Questions

Based on the above discussion, this research intends to answer the following main research questions:

1. How are elements such as technological, organizational and environmental factors influence organizational performance.
2. What is the relationship between technological, organizational and environmental factors and information security culture?
3. Does information security culture mediate the relationship between information security practices and organizational performance?

1.4 Research Questions

Based on the above discussion, this research intends to answer the following main research questions:

1. To determine the technological, organizational and environmental factors influencing organizational performance.

2. To investigate the relationship between technological, organizational and environmental factors and information security culture
3. To examine whether information security culture mediate the relationship between information security practices and organizational performance.

1.5 Scope of the Study

The study focuses on the effective establishment of information security culture in the Nigerian banking sector. The essence is to improve on the volume of sales, profit growth and expansion of the financial sector through the establishment of information security culture which invariably will increase sales and profitability. In turn, it will foster a platform for effective and efficient decision making that lead to organizational performance.

This study investigates banks in Nigeria with large population of over 160 millions Nigerians. It therefore becomes imperatives to focus on a specific direction in order to accomplish its stipulated goals. Also, this study focuses on the human factors which could be regarded as human errors and failures due to the non competence of the employees, IT knowledge of the users, lack of executive support and non implementation of information security practices. This study concentrates on the factors of information security practices that will eventually inculcate information security culture and in turn improve organizational performance in the banking sector.

1.6 Significance of the Study

The significance of the study could be based on the aforementioned theoretical gap that could foster banking industry through an information security culture in order to improve banking performance. Information security culture is still in the early stage of development where several issues are still being identified and conceptualized (Almatheer & Nelson, 2009). Likewise, the findings will serve as a guide for development of information security culture in banking operations where human errors will be minimized (Sanusi, 2011; Parsons et al., 2010). Organizational performance enhances business values and continuity; all these require investors and stockbrokers to indicate their loyalty and continuity with the bank.

Moreover, the current phenomenon of the wiki lead highlights the leakage of sensitive information whereby almost the nations with powerful economy secret information was revealed, buttress the fact that there are information security threats and vulnerabilities. Although, most of the organizations have implemented information security practices, changes in technology presumed to be the reason why there are continuous security breaches both internal and external incidents which require a continuous study.

Lastly, the present study enriches the knowledge through the research theoretical framework for the development of information security culture not only in the banking sector but other sectors such as public sector, SMEs and higher educational institutions. It will give a guide and path/focus for the researchers in information security systems. Hence, it is assumed that the findings of the study will provide a basis for future research

in the accounting information system in particular and information security system in general.

1.7 Organization of the Chapters

This thesis is divided into seven chapters which review the necessary information on information security practices that could be used to establish information security culture and eventually affect banking performance in Nigeria. Below is the organization of the thesis:

Chapter 1 discusses the introduction to the research work of this study. It presents the research problem followed by the research questions and objectives, the scope of the study with the discussion on the significance of the study while the remaining sections enumerate the areas not covered which will serve as suggestions for future research.

Chapter 2 provides a review on the models and theories related to information security practices, information security culture and organizational performance.

Chapter 3 provides the research hypotheses and methodology that was used to achieve the objective as well as to test the hypotheses.

Chapter 4 discusses the research instrument development. It emphasizes on the questionnaire development, the examination of the validity, content validity and the testing of the reliability of the instruments developed.

Chapter 5 presents the analysis and discusses the empirical findings and results obtained from the analysis. It gives an estimation of the response rates, reliability and validity and questionnaire validation. The final discussion will be based on demographic structure response and the hierarchical regression analysis.

Chapter 6 provides the discussion and implications of the study from the theoretical and managerial point of views based on the findings of the survey in chapter five while the refined model is presented.

Chapter 7 offers the conclusion based on the key findings from the research. It also discussed the limitations as well as suggestions and recommendations for future research on information security practices that enhance organizational performance.

1.8 Definitions of Crucial Terms

Although different scholars have different meaning but for the purpose of this study, the following terms used in this study are defined as follows:

Information Security

Information security is a multidimensional discipline that covers areas such as computer science, sociology, accounting and management. It implies that, an organization is required to protect information assets (Elachgar et al., 2012; Akinsuyi, 2009; Brown & Heywood, 2005; Pathak, 2006; Hang et al., 20

Information Security Awareness

Information security awareness is defined as activities that foster employees' sensitivity through education about the threat and vulnerabilities of information system and the recognition of the need to protect data, information and the means of processing them (Gebrasilase & Lessa, 2011; Richardson, 2007; Besnard & Arief, 2004; Wilson & Hash, 2003).

Information Security Culture

Generally, information security culture is defined as norms, beliefs that guide against the behavior of employees by stipulating what employees need to do within the organization (Fritzgerald, 2007; Aggrawal, 2003; Schein, 1999). It is geared towards shaping the behavior of the employee as well as helping employees to understand organizational policies and beliefs (Lim et al., Shahri & Ismail, 2012; 2009; Christopher, 2008; Zakaria, 2013; 2007).

Organizational Performance

The word performance is often used in the business world to mean the outcome of an activity that has been carried out. It is the change in the financial position of an organization as a result of activities carried out through a sound management, strong governance to achieve a better result (Sharukhalid, 2011; Cartoon, 2004).

Information Security In-sourcing

Information security in-sourcing is using IT expertise within the organization to cope with the changing in IT and the knowledge in IT (Simon et al., 2007; Samdder & Kadiyah, 2006). No organization will survive especially during the advent of sophisticated technology without IT experts' knowledge.

Information System Security

This term is used in this study to mean a set of people, data and procedure that work together to provide useful information. The word system implies various components such as technology, technical and human factors that seek a common objective of supporting an organization's activities to produce efficient organizational performance (Ajbacly et al., 2012; Herath & Rao, 2009; Briney, 2001).

1.9 Summary

The above section discuss the overall information security culture to may lead to increasing organizational performance in a broad perspective and the need to establish an information security culture in the Nigerian banking sector. Nigerian banks encounter challenges in the information security perspective, compliance with security standards, security awareness and security policy and procedures. Recently, there was bank reform with emphasis on the implementation of information security practices in order to enhance competitive advantage globally and for efficient organizational performance. Thus this study intends to examine the continuum of information security practices,

information security culture and ultimately organizational performance from the perspective of banking sector.

This chapter covers a wide range of sub topic needed to be discussed in chapter one. It ranges from the introduction, research questions and objectives, the research gaps, the importance and contribution of the research followed by the background of the research where information security practices, information security culture and organizational performance in Nigerian context is discussed in detail.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter discusses the literature review of the study. The theoretical framework of this study is premised on the previous literature and findings of scholars in the field of information security culture. To expatiate further, a research model of the framework is designed, and clearly shown in this chapter. Information security culture is linked with accounting activities such as confidentiality, integrity and availability. Basically, the chapter discusses extensively the concept of technology, organization and environmental theory (TOE theory), with the supporting theories such as security system theory, security policy theory and risk management theory to develop the theoretical framework. These theories will be discussed later in this chapter.

2.2 Overview of the Nigerian Banking Sector

In Nigeria, the banking system experienced an unprecedented crisis triggered by the global events which brought about the financial meltdown in the banking sector in 2009. Many Nigerian banks had to be rescued from collapse. In order to stabilize the system, improve organizational performance, and return confidence to the markets and investors, the Central Bank of Nigeria injected N620 billions liquidity into the banking sector and replaced the leadership of eight banks (Soludo, 2010).

N= Nigerian currency

However, the cogent lesson from the crisis is that banks have the potential for growth. Hence, bank's growth will apparently require information security culture. Measures such as security management bring sanity to the banking in order to avert malpractices (e.g. fraud). By establishing information security culture, the banking sector in Nigeria will ensure risk and management control, financial stability, healthy evolution and the development of the real economy (Soludo, 2010). This study therefore is premised on establishing effective and efficient information security culture that will improve banking performance. The definition and description of information security are dealt with in the following sections.

2.3 Information Security

Information security is a multidimensional discipline that covers areas such as computer science, sociology accounting and management (Elachgar et al., 2012; Akinsuyi, 2009; Brown & Heywood, 2005; Pathak, 2006; Hang et al., 2003). An organization is required to protect information assets to prevent security breaches (Asai & Fernando, 2011).

Going from the foregoing, information security can further be divided into two; namely, technical aspect and social aspect. This study focuses on the social aspect of information security. This is because most of the security failures are due to human errors (Asai & Fernando, 2011; Padayachee, 2012; Shahri & Ismail, 2012; Haung Ran & Salvendy, 2007; Cahn et al., 2005). Few examples of social based information security are information security management (ISM), information security governance (ISG) and

information technology governance (ITG). These examples are illustrated in Figure 2.1 below as:

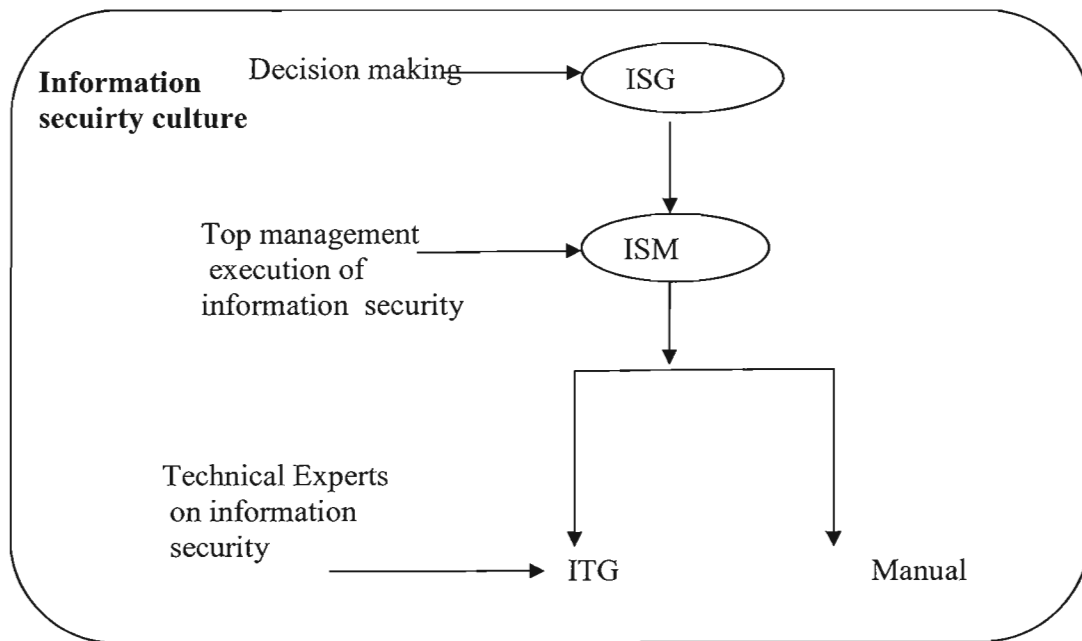


Figure 2.1
Information Security Transformation

2.3.1 Information Security Governance

Information security governance (ISG) is a field of accounting information system, which deals with the strategic alignment, performance management and management of resources in order to ensure availability, integrity, confidentiality and traceability of information security (Elachgar et al., 2012). Hence, ISG is used to establishing and maintaining a secured environment, taking into account the policies, standards, guidelines, codes-of-practices, technology, human issues, legal and ethical issues (Elachgar et al., 2007; Eloff & Eloff, 2003).

In line with the position of several scholars, Elachgar et al. (2007) identified approaches to ISG as: (1) strategic perspective that addresses the corporate governance, policies and pure management issue; (2) human perspective approach addresses the issues of security culture, awareness, training, ethics and other human issues; and (3) technology perspective approach that is focused on the hardware and software products.

Under a perfect situation, ISG is an overall management of information security. Information System Audit and Control Association (2012) opined that ISG is a “strategic alignment, value creation, performance management and management of resources against the requirement of company’s business” (Elachgar et al., 2012). Hence, the independent review of the security system and procedure are important to ensure that the organizations protect and confirm that the system is working as designed (Swanson, 2000).

On the same clime, the driving force behind information security will be the security officer with the executive power, likely to be the chief information officer or the managing director. It is a pity that most organizations do not have a chief information officer who is knowledgeable in both business operations as well as IT, as a result leaving information security into the hands of the IT department. The purpose of information security is to protect an organizations valuable information and knowledge resources such as information, data, hardware and software (Parks et al., 2011; Parsons et al., 2010; Pathak, 2001). Therefore, the application of appropriate security measures becomes

inevitable. However, it could be said that the success of ISG depends on human beings such as the employees within the organization, whose behavior need to be channelled towards security culture. In turn, establishing information security culture amongs employees is a necessity. This is what this research intends to contribute.

In a nutshell, this study defines ISG as the overall security practices whereby policies, procedures and culture are available to enforce and monitor the security issues. Thus, establishing information security governance through information security practices is a must for every organization, including the banking sector (Elachgar et al., 2012).

2.3.2 Information Security Management

Information security management is defined as the ability of securing information asset from distortions of confidentiality, integrity and availability (Huang et al., 2010; Brown & Heywood, 2005). It is the responsibility of the management to protect information considers most vital assets of the organization (BS 7799-2, 1999; ISO 27001; Martins, 2012). This will in turn ensure that organizational objectives, vision and mission are successfully achieved.

Also, Karyda et al. (2005, pg246-260) defined ISM “as a stream of management activities that aims to protect information assets and secure the framework of an organization where the information system is operated” This could be achieved by having an organizational structure that is supported with well defined roles for the responsibility of

information, business processes, applications, infrastructure and others. Thus, the aim of the ISM is to protect information from uncalled and unauthorized act that could lead to threat with the use of computer to ensure confidentiality, availability and integrity of information (Brown & Heywood, 2005; Hong, Chi, Chao & Tang, 2003).

The purpose of having an ISM is to provide an overview of the security requirements and describe the controls in place or planned responsibilities and expected behavior of all individuals who access the system (Babatunde & Selamat, 2012a & 2012b). The ISM is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager.

Information security management brings structure and governance to the information security function within an organization (Pironti, 2005). Thus, the success of ISM depends largely on human factors. The activities of information security become routine, routine become norms and norms will eventually become culture (Zakaria, 2013). This is the interest of this study.

2.3.3 Information Technology Governance

The concept of information technology governance (ITG) emerged in the late 1990s when Brown (1997) and Sambamurthy and Zikmund (1999) wrote about the ITG

arrangement and framework”. The scholars advocated that ITG arrangements represent “organizations’ IT-related authority patterns”. Information technology governance’s objective is to define structures, processes, mechanisms, decision making rights and responsibility about main IT issues on one hand, and control and monitor the effectiveness of such decisions, and mitigate IT-related risks in order to achieve an organization’s objectives on the other (Lechler,Wetzel & Jankowski, 2011; Zakaria, 2006).

Now, the question which needs an urgent answer: “What is the difference between ITG, ITC and ISG?” It is hard to differentiate between information security plan and good management practices and IT control frameworks. ISO 38500 helps in clarifying ITG by describing it as the management system used by directors (2008, June: A new ISO Standard for Corporate Governance of Information Technology – World and The ISO 38500 Governance Standard).

In addition, Carr et al. (2012; 2007) opined that IT confers a strategic advantage. This line of criticism might imply that significant attention to ITG is not a worthwhile pursuit for senior corporate leadership. However, Carr et al. (2007) posited further that there is counterbalancing concern for effective information technology risk management. Therefore, the manifestation of ITG objectives through detailed process controls, e.g. in the context of project management, is a frequently controversial matter in large scale IT.

Contrastingly, information security plan frameworks are ITG corporate policies (privacy), business process owners, records retention, IT department, security, standards, practices and procedures, system documentation management, regulatory compliance, escalation procedure, disclosure procedures and lastly contract administration and vendor management.

However, a well-balanced approach to ITG is made up of a variety of sets that match on organization circumstances and requirements (Gupta & Hammond, 2005). Thus, the difficulties in achieving a balance between financial transparency and cost-effective data capture in information technology financial management, e.g., to enable chargeback, is a continual topic of discussion in the professional literature and can be seen as a practical limitation to information security such as IT steering committee/priority process, alignment with business objectives, information technology strategy and architectural standards, IT project tracking support for strategic enterprise initiatives.

In summary, organizational security and IT components reflect the same core components as those found in overall enterprise security activities. The message to the management in any organization is that, there is more to oversee in support of enterprise security than traditional IT management, such as records retention or protection of intellectual assets (information) where the information is not necessarily automated. This highlights the role of employees in ensuring the success of ITG. In turn, establishing information security culture is critical in any organization including banks. This is the contribution of this research.

2.3.4 Information Security Culture

Information security culture is defined as a learning process within an organization through security activities (Zakaria, 2013). If security activities are tuned to acceptable manner, it will eventually create an appropriate security culture (Zakaria, 2013). Implicit in this is that information security is paramount. Thus, every organization including banks needs to motivate and encourage their staff to uphold the concept and principles of information security which eventually will create information security culture. To ensure information security activities are regularly implemented, every staff member must take information security as their way of life or culture. For this to take place, every organization must provide a conducive environment for inculcating information security culture among the staff. In this case, all staffs will have a high level of concern and willingness to secure organizational information or assets. The aim of this study is to determine the factors that can be used to establish information security culture within the organizations. This study defines information security culture as the norms and values that guide employee's behavior towards information security activities within an organization.

The issue of information security culture is increasingly becoming important because it is at the early stage where diverse phenomena are yet to be discovered and theoreticalized (Shahri & Ismail, 2012; Parsons et al., 2010; Alnathrer & Nelson, 2009; Huang et al., 2007; Brook et al., 2002; Kankanhalli et al., 2003). Thus, the need arises to inculcate information security culture as the main features for efficient performance in the banking sector. Hence, information security culture should support banking activities so that it

becomes part and parcel of the employees' daily lives to avoid security failures (Padyachhee, 2010; Gebrasilase & Lessa, 2011; Chen, Medlin & Shaw, 2008; Thomson et al., 2006).

Moreover, Gupta and Hammond (2005) and Ajbacly et al. (2007) argued that management must invest in information security culture to prevent abuse or threat. Insecurity of information systems is an obvious challenge; organizational activities should be aligned with the established information security culture (Ruighaver, Maaynard & Chang, 2007; Van Niekerk & Von Solms, 2005). Establishing information security culture could reduce abuse or threat of information system.

The focus of this study is the establishment of security culture for banking performance. The compliance and the willingness of banking staff to implement information security activities should be considered as very imperative (see Fig. 1.1). Hence, information security activities such as the improvement of staff competency, staff awareness and training on security matters and the reduction of security incidents should be established within the banks. The improvement of staff competency, staff awareness and training on security matters and reduction of security incidents will not only improve staff and management but will increase for increase organizational performance and give an organization an edge or niche to compete efficiently and effectively in the competitive global market.

In addition, Glaser and Pallas (2007) stated that establishing the information security culture is considered as a public good. Public good in information security means the information by the one cannot be affected by the other (Glaser & Pallas, 2007). In economic theory, a public good is characterized by two, namely; non-rivalry in consumption or use and non-excludability (Glaser & Pallas, 2007). Non-rivalry refers to the value and the availability of the goods not being decreased by its usage while non-excludability could be referring to no individual party is being barred from using the goods. This is to say that securing organizational information will benefit all staff members.

Also, if there is no security put in place, the direct benefits equal to zero and vice versa. Krause and Tipton (2002) opined that managing information security enables the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. Thus, information security culture assist top management to plan, it will not only address the issues of vulnerability, which represent a high level of risk, but also the implementation of security activities in an organization. The security culture policy defines how security issues should be handled, address the appropriate use of the organizational resources, the requirements on individuals who request and maintain accounts, the acceptable methods of connecting to the organizational LAN remotely, the way information is protected from unauthorized access, disclosure, corruption, and loss, the procedures for adding new devices to the

network, and the rules regarding the use of privileged system accounts (Oppenheimer et al., 1997).

Martins and Odunfa (2012) found that the annual cost of cyber crime was about \$150 billion. 6.4% of the online fraud in the United States in 2011 was carried out by Nigerian . This shows that there is need to conduct pragmatic studies on how to reduce online fraud. This can only be achieved if information security culture is embraced. The focus of this study is therefore is to establish security culture for the improvement of organizational performance in general and banking performance in particular.

Based on the above discussion, the researcher defines information security culture as a process of managing information security through the willingness and compliance of employees in order to maintain the strategy of implementing a security culture. Having said this, obtaining an understanding of the factors militating against establishing an effective information security culture is paramount. Section 2.5 discusses this in details.

2.4 The Importance of Information Security Culture

Information security culture promotes best security practices among staff in the organization (Elchagar et al., 2012). In a situation where non competent staffs do not recognize threats, the result is always information security chaos. Information security culture assists organizations in establishing appropriate security practices that will enable staff to reduce information security errors and failures. It gives room for information

security awareness, training programs for coping with threats, and social engineering attacks. The outcome of information security culture within organizations will improve human activities/practices and in turn improve the organizational performance. In other words, information security culture need to be established in every organization including banks.

2.5 The Relationship between Information Security Culture and Organizational Performance

The aim of information security culture is to protect information from uncalled and unauthorized act which could lead to threat with the use of computer (Huang, Rau & Salvendy 2010; Samy, Ahmad & Ismail, 2009; Elchagar, Bouladour, Makoudi & Regragui, 2012; Hong, Chi, Chao & Tang, 2003). In other words, the purpose of information security culture is to ensure confidentiality, availability and integrity of information within the organization (Huang, et al., 2007; Brown & Heywood, 2005). Thus, securing and protecting information asset brings structure and governance to the information security function within organizations (Elchagar et al., 2012; Pironti, 2005). It also allows business continuity; to keep pace with legal compliance and achieving competitive advantage. Therefore, establishing information security culture is secondary to the need of making profit (Kruger & Kearney, 2006; Pathak, 2006; Burkit, 2002).

On the other hand, the main objective of the organization is to increase sales volume, profit and create a niche for a competitive advantage in the global market. Human beings

are the brain behind improving performance. Hence, the need for security culture becomes inevitable in order to enhance a better performance.

2.6 Establishing Effective Information Security Culture

From the above discussion, it is clear that there is a need to establish an effective information security culture in the organizations because information security culture is an integral part of information security (Elchagar et al., 2012; Von Solms & Von Solms, 2007). Information security culture is created within the organization initially through information security practices. Thus, employee behaviors need to be tailored towards appropriate information security practices (Dzazali & Zolait, 2012).

Culture is the norm, value and belief shared among individuals, society, organizations and nations (Zakaria, 2013; Schein, 1999). Organizational culture embraces the norms, procedures, policies within the organization. To establish information security culture, every staff member must observe and appreciate good norms, procedures and policies in all information security activities. To assist this process, understanding the determinants of information security activities is of paramount importance. The main concern of this study is how to establish culture to avert the non compliance of the staff to information security.

Based on the previous studies (Weill & Ross, 2004; Von Solms, 2000; Barafort et al., 2004), the factors that affect information security practices in an organization considered

in this study are as follows: (1) technological factors including perceived technology advancement and information security in-sourcing; (2) environmental factors such as compliance with security standards and government policy and regulations; and (3) organizational factors such as size of the organization, information security awareness, information security policies and procedures, perceived training programs, information security risk, threat and vulnerability, information security risks control, perceived management support and commitment, motivation of employees and perceived job roles and responsibilities.

By the same token, information security culture influences the dependent variable which is organizational performance. In other words, information security culture is the mediating variable in this research; thus, cause a change in the strength of the relationship (Sekaran & Bougie, 2009; 2006). From the discussion in section 2.3.1-2.3.3 above, it can be seen that it is very important for staff members to practice information security consistently. This leads to information security routines, norms and eventually culture. That is why this study wants to establish information security culture among the employees in the organization in particular banking sector. The description of each element is provided in section 2.6.1 - 2.6.3.

2.6.1 Technological Factors

Based on previous studies on information security culture, technological factors are divided into two which are perceived technology advancement and information security

in-sourcing. The description of each factor is offered in the following subsections 2.6.1.1 - 2.6.1.2.

2.6.1.1 Perceived Technology Advancement

The reformation of the banking sector through IT has been a global business agenda in the west, Asia and the third world countries. The third world countries are expected to go along with this movement. In fact, every organization employs the use of technology on a daily basis in order to gain competitive advantage (Asai & Fernando, 2011; Ehikamenor, 2003). However, IT had brought about significant changes in the way the banks processed and stored data; adding that the telecommunication networks had played a positive role in the expansion and integration of the information systems, within and among banks facilitating data accessibility to different users (Martins, & Odunfa, 2012; Kaliannan & Awang, 2010).

By and large, managing IT function has become the most difficult phenomenon in recent years, especially the technical know-how due to the increasingly sophisticated online business transactions (E-business), diversity of technology platforms and components in an organization, reduced costs and improved operations that will affect profitability (Martins & Odunfa, 2012; Parsons et al., 2010). It also reduces time to market and time to respond to the requirements of the business, new legislation and individual liability and reliance on IT as a critical enabler of many compliance, regulatory, corporate governance effectiveness and organizational effectiveness capabilities (Ville, Kraemer & Gurbaxani, 2004; Kohli & Devaraj, 2003; Yam, 1998;

Hoffman, 1998). Most of the managers agree on the necessity of considering IT as an organizational strategic player (Boynton et al., 1994; Orlikowski & Barley, 2001; Sambamurthy, 2000; Venkatraman & Henderson, 1998).

The above phenomena highlight the effort of information security plan based on technology advancement. Being equipped with adequate IT enables the organizations to implement information security activities effectively and efficiently. Moreover, IT plays vital developmental role in the banking industry by increasing the volume of sales, higher level of operation and realizing economics of scales and hence need to be treated as an investment in the bank's future success (Grainger-Smith & Oppenheim, 1994; Hill, 1999). Thus, perceived technology advancement need to be considered in the process of establishing information security culture. This results in the inclusion of perceived technology advancement in the research theoretical framework.

2.6.1.2 Information Security In-sourcing

To cope with the rapidly changing IT, an organization may decide to strategically go into in-sourcing (Babatunde & Selamat, 2011; Samdder & Kadiyah, 2006).. Thus, recruiting an in-house development by using experts within the organization in order to develop and maintain IT systems becomes necessary. Recruiting IT expertise is necessary because no organization will succeed without collaborating with experts that have knowledge on IT (Samdder & Kadiyah, 2006). The banking industry is faced with challenges of increasingly globalized banking system (Soludo, 2010). On this note, it will be appropriate if banks recruit chief security officers with vast knowledge not only on

IS/IT but also on business perspectives for a smooth organization of information security culture and keeping pace with competitive world (Samadder & Kadiyala, 2006). Information security in-sourcing will enhance information security managers from being technical to more professional towards negotiation and supervision (Simon et al., 2007). Moreover, it is better to establish in-sourcing within the organization by using the IT experts, chief information security officers and chief information officers that are well versed with knowledge of information security rather than outsourcing to other firms (Samadder & Kadiyah, 2009; Wright, 2004).

The establishment of good in-sourcing activities could develop good information security culture. This enables effective information control and in essence leads to relevant and reliable information. Consequently, right decision making could be established and ultimately ensured effective organizational performance. Thus, it seems that there is a potential relationship between information security in-sourcing and information security culture on one hand, and ultimately organizational performance on the other. This results in the inclusion of information security in-sourcing in the theoretical framework of the study.

2.6.2 Environmental Factors

Based on the previous studies on information security culture, environmental factors are divided into two factors. These factors are international security standards and perceived government rules and regulation. The description of each factor is offered in subsections 2.6.2.1 - 2.6.2.2.

2.6.2.1 International Security Standards

Usually, an organization is prone to threats if appropriate precautions are not in place. This eventually leads to increase in the cost of managing unstructured information (Lech et al., 2011; Huang et al., 2010; Samy et al., 2009; Petrides, 2004). In Nigeria, according to Federal Financial Institute Examinations Council (FFIEC), there are information security breaches, which lead to manifestation of the cyber/information security legislations. The legislations comply with ISO 27001: 2013 requirements that reduce the threat of successful information security breaches and inspire confidence in investors and users (Huang et al., 2010; Akinsuyi, 2009). Hence, compliance with international standards will expose the organization to the assessment and verification opportunities.

By and large, banks are compelled to comply with the International Security Standard and British Standard Institute (BSI) 27000th series. However, the series of 27001: 2013 are related to ISG for guidance, auditing, reviewing and metrics as defined by the international Organization for Standardization (ISO) JTC1/SC27 roadmap. ISO is a set of standards and methods used to be the very reference for specialists where documents could be identified as valuable materials for people dealing with information security standard.

With the advent of ISO 27001 (formerly known as ISO 17799), information system code of practice helps the organizations to take information security seriously. This is because ISO/IEC 27001: 2013 certification is the world's highest accreditation for information protection and security from the ISO. The ISO/IEC 17799-1: 2013 certification specifies

requirements for ISG and is recognition of compliance with the stringent requirement of the standards and regulations for handling all organizational information.

The process of acquiring ISO/27001:2013 certification could be lengthy and time-consuming (Martins & Odunfa, 2012). Nevertheless, some Nigerian banks are embracing it. Thus, First Bank Plc got its assessment and verification from BSI (Omu, 2010 This Day Newspaper, 2010). Also, Digital Jewel, a consulting firm which facilitated the certifications of Fidelity Banks and Unity banks received the ISO 27001:2013 from the British Standards Institute (Martins& Odunfa, 2012). This trend of BSI certification is making waves in the Nigerian banking sector. The duty of the BSI is to audit and verify bank's information security activities. This helps the bank to be at par with leading international and multi-lateral corporate organizations including the International Monetary Fund and the World Bank in the area of security and protection of customers' information.

The First Bank Plc Managing Director, Mr. Bisi Onasanya was of the opinion that the certification confirms that the bank has adopted and complied with the highest known management standards in information security in the world. This shows the strength of the bank investment not only on technology, but also on human development in order to improve information security culture (Omu, 2010: This Day Newspaper, September, 2010). The above standards stipulate a wide range of security issues such as system policy, system organization compliance, physical control system organization and others. Akinsuyi (2009) argued that there is a new information security legislations enacted in

Europe and North America that will make it mandatory for the organizations to implement adequate information security controls commensurate to the risks that may accrue to systems within their environments.

Based on the above discussion, it is clear that the role of international security standards is critical to the establishment of a robust information security activities and in turn information security culture. This will ensure a robust information control and in turn creates relevant and reliable information processing. Relevant and reliable information enables right decision making and eventually creates effective business activities. All these lead to better organizational performance. Thus, international security standard is included in the theoretical framework of the study as one of the determinants of information security culture that will ultimately lead to organizational performance.

2.6.2.2 Perceived Government Rules and Regulations

The societal culture may influence organizations if and only if, each organization does not abide by the norms that guide its employees in the society. Perceived government rules and regulations play an important role in information security culture (Cui, Zhang, & Huang, 2006). The regulatory and policy-making bodies in Nigeria are the Central Bank of Nigeria (CBN) and the Nigerian Deposit Insurance Corporation (NDIC). These bodies are emphasizing on securing information scrupulous activities (Martins & Odunfa, 2012). Also, the regulatory bodies adopt few of the international regulatory bodies such as Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, Basel II and the European Data Privacy Directive (EDPD). Regulations and acts enacted by these bodies do not only

maintain information security but also increase the integrity of the information system in the organizations (Domínguez, 2009).

However, by the international standard and the development of information security legislations, the Nigerian banking system is not fully integrated into international financial system. Information security standards remain stagnant in some part of the country (NDIC 2009, CBN Annual Report, 2009, Akinsuyi, 2009). Hence, the collaboration of NDIC and CBN to combat the problem of information security breaches in Nigeria is paramount.

Perceived government rules and regulations propel the willingness of the management and staff on security matters. This eventually forces the banking sector to establish good ISG, internal control and security measures. All these lead to establishment of information security culture. In turn, organizational information systems are able to control the right information to the people at the right time. This scenario ensures effective decision making process and eventually effective business operations. In short, it could be said that there is a potential relationship between government policies and regulations and information security culture and ultimately better organizational performance. Thus, all these elements are included in this research theoretical framework.

2.6.3 Organizational Factors

Based on the previous studies on information security, organizational factors are divided into eight, which are size of the organization, information security awareness,

information security policy and procedure, perceived training program, perceived information security risks, threat and vulnerabilities, motivation of employees, perceived management support and commitment and perceived job roles and responsibilities. The description of each factor is offered in subsections 2.6.3.1 - 2.6.3.8.

2.6.3.1 Size of the Organization

The implementation of information security activities involves cost; it must be supported by adequate resources such as cash, experts and others. Security awareness and training programs of employees involve huge cost especially when it needs to be carried out periodically for information security assessment and evaluation efficiency (Wilson & Simon, 2005). As the number of employees in the organization increases, more strategic activities need to be imbibed. Thus, it is imperative that employees understand security procedures on a daily basis through a clear organizational set of rules and the need to strictly follow it (Wilson & Simon, 2005).

Fenny et al. (1992) posited that information security activities must be monitored by the CISO to ensure its success. Implicit in this scenario is that big organizations are more capable of implementing information security activities than the small and medium organizations. This is because big organizations have adequate cash, IT experts, and greater economies of scales that can take risks related to IT and have the capability to sustain effective and efficient organizational performance compared to small and medium

enterprises (Lippert & Govindarajulu, 2006; Gibbs & Kraemer, 2004; Zhu et al; 2003; Kuan & Chau, 2001; Thong, 1999).

In addition, big organizations benefit from the information security standard than the small organizations because they rely on standard (Chang & Ho, 2006; Ghobadian & Gallear, 2007). On the contrary, small and medium organization are said to be sub-standard because they may not get enough resources to carry out ISO 27001:2005 effectively in information security culture and objectives (Chang & Ho, 2006). Thus, size of the organization need to be considered in the process of establishing information security culture. This result in the inclusion of size of the organization in the research theoretical framework.

2.6.3.2 Information Security Development

Information security development is very much needed in this computer age. It is needed because information communication technology inventions are changing the financial institutions' operational activities to meet with the competitive demands of the stakeholders (Babatunde & Selamat, 2012). And, organizations are compelled to follow the trend of this new development in order to be at pace with the global trend (Kaliannan & Awang, 2010). The tools of information security development such as information security awareness, perceived training programs, information security policy and procedure help in the establishment of information security culture in the organization (National Institute of Standard & Technology, (NIST) (SP) 800-30). The definition and description of each activity (norm) are provided in the next three subsections.

2.6.3.2.1 Information Security Awareness

Information security awareness is defined as a group of activities to create employees sensitivity to the threat and vulnerabilities of the system and the recognition of the need to protect data, information and the means of processing them (Dominguez, 2007; Zakaria, 2007; Peltier, 2005; Besnard & Arief, 2004; Von Solm, 2000). The organization that neglects learning cannot survive in this computer age of the ICT inventions. Thus, learning is a continuous process because security awareness is the most effective countermeasures against human factor threat to information security (Parson et al., 2010; Ernst & Young, 2007; Wilson & Hash, 2003).

Information security is viewed as a serious phenomenon to business values. And, it reduces risks so as to achieve the objectives of the organization. The risk involved in information security incidents cannot be derived from the technological tools; rather, employees are the brain behind security failures. Hence, the need arises for employees' security awareness on security avertness (Parsons, et al., 2010; Herath & Rao, 2009; Alnatheer & Nelson, 2009; Huang et al., 2007; Kruger & Kearney, 2006; Besnard & Arief, 2004; Parker, 2002). The employees' need to be informed through the learning process. This starts with building strong information security awareness among the employees through education and training because employees have problems in understanding security attributes (Funnel, 2005). According to Wilson and Hash (2003), awareness cannot be referred to as training because awareness is not training and the purpose of awareness should aim at security. Nevertheless, scholars of information security emphasized the need of employee security awareness based on the fact that

individuals are susceptible to security attack due to personality traits (Parsons et al., 2010). In addition, security incidents caused by the insiders are on the increase (Parsons et al., 2010; Workman, 2008; Zakaria, 2007; Briteny, 2001; Von Solm, 2000). The Computer Security Act of 1987 stated that federal agencies are required by law to provide security awareness to all end users of information security.

It is very unfortunate that a survey carried out by Computer Crime and Security 2007 in the USA indicated that 18% of the organizations do not use any form of security awareness while 35% who employed security awareness fail to measure its effectiveness (Richardson, 2007). Therefore, when the employees are aware of the IT policies and procedures, they will in turn be a catalyst to effective functioning and protection of the information security which ultimately will reduce the stress of the security breaches. The awareness of the importance of information security culture will lead the management to plan organizational information security (Gatewood, 2005). Stan Gatewood of the University of Georgia (2005) said that, "If you have no security plan, how will you know if you are doing it right? You will be reacting to every little thing that bumps in the night".

Security awareness and security training programs should not be considered as one but information security awareness pave way for security training programs. In other words, without security awareness, there will be no training. Thus, information security awareness and security training programs go hand in hand. Previous researchers were of the opinion that information security awareness and information security training and

educational programs are the same while others did not consider them to be (Enisa, 2006; Besnard & Arief, 2004; Hansche, 2001a; Qing et al; 2000; Siponen, 2000). To appreciate this argument, the element of information security awareness and training and educational programs are separated in this research.

To recapitulate, it is argued that information security awareness propels information security activities in the organizations which eventually become information security. This in turn ensures effective systems, decision making and ultimately better organizational performance. Thus, information security awareness, information security culture and organizational performance are included in the research theoretical framework.

2.6.3.2.2 Information Security Policy and Procedure

Information security policy and procedure are important instruments used in information security to demonstrate the need for and scope of information security and to influence employees' behavior on what to do and what not to do (Chan et al., 2005; Whiteman & Mattord, 2003; Gragg, 2002; Hone & Eloff, 2002). It stipulates the policies, procedures and structure to be followed in the organizations.

Changing in the technology know-how gives rise to security risks, hence the use of risk management theory in this regard is very imperative since these risks are much more outgrowing the security practices, policies, procedures; and training programs increase

the knowledge of the employees (DiArcy et al., 2009; Von Solms, 2007; Abu-Musa, 2003). The backbone of the system security policy is a blueprint to drive information security projects from design to implementation, validation and operations (Anderson, 2008; 2001). Successful security design, implementation and operational assurance depend on how policy is developed. Flaws in the policy may likely propagate down to the operational stage.

However, a good security policy must explicitly state the protection mechanisms such as what employees should do and what not to do and how breaches are to be detected. In other words, security policy is capable of influencing employees' behavior towards compliance with top management visions and objectives (Thomson & Von Solms, 2007; Whiteman & Mattord, 2003; Hone & Eloff, 2002). It should be periodically reviewed in order to ensure that an appropriate assurance level is maintained. Also the security policy should include appropriate procedures for handling and responding to security incidents and natural disasters, and appropriate hiring practices for minimizing employee-related threats (National Institute of Science and Technology Special Publication 800-16, pp.12). After putting system security policy in place, an information security plan is developed.

Practically, information security policy in the second wave (Von Solms, 2000, 2005) expresses top management's commitment towards protecting the information assets. There are many international standards that explain the procedures and controls that

should be co-opted into information security policy such as ISO 27001:2005 and BSI in order to mitigate the threats of information security culture.

By and large, information security policy and procedure could encourage information security activities and in turn information security culture. This continuum provides a platform for effective and efficient information processing and in turn decision making. Good decision making leads to better performance. Thus, it could be said that there is a potential relationship between information security policy and procedure, information security culture and ultimately organizational performance. This rationalizes their inclusion in this research theoretical framework.

2.6.3.2. 3 Perceived Training Programs

The employees are the greatest assets of an organization. And, a well trained employee makes information security system very viable (Parsons et al., 2010; Kaplan-William, 2009; Babatunde & Selamat, 2012). Training programs are the prerequisite for the information security development process because a well organized training program will increase security awareness and lead to greater participation in the security management practices (Qingxiong, Schmidt, Herberger & Pearson, 2009). ISO 27001: 2005 provides content for training in the field of the security system culture and practices inside the organizations and activities required by information security standard.

The Organization for Economic Cooperation and Development (OECD) guidelines for the security of information system and networks stipulated that: “Towards a culture of security underlines the need for a greater awareness and understanding of security issues and practices to develop a common background among citizens, particularly ICT practitioners”. Moreover, information security training and education programs should include evaluation and implementation of IT programs. To keep abreast, with the rapid technology changes, there should be courses emancipated to meet the new challenges of the changes. Hence, training programs must be flexible to meet the new challenges of securing information.

However, the IT personnel and CISO in an attempt to develop an effective information security avail themselves of going for security awareness program in order to update themselves on the current trends in security measures. The IT department should not be left out as well. Also, the use and the reading of educative CPA journals where information on reducing the threat levels of accounting information system challenges for management, accountants, auditors and academicians could serve as an avenue of the training program. Implicit in the above discussion is that perceived training program could encourage information security activities and in turn information security culture through a high level of security awareness amongst management and staffs. This leads to effective and efficient information processing and in turn organizational performance. Thus, perceived training program, information security culture and organizational performance are included in the theoretical framework of the study.

2.6.3.3 Perceived Information Security Risk, Threat and Vulnerabilities

Risk is defined as the destruction to a procedure of information that emerged from unplanned incidents that can harmfully impact the course of information (Elky, 2006). In other words, risks bring about the possibility of an unplanned event or occurrence which jeopardizes the organizational goals or objectives. The ability to identify the most effective security controls to reduce risks has been the major concern in security management. Risk analysis and risk management could serve as a means of controlling risk (Kankanhalli, Teo, Tan & Wei, 2003, National Institute of Standards & Technology (NIST) (SP) 800-30).

The manual code of practice (CoP) for information security management was published in 1993 by the British Institute and became a standard in 1995. This has assisted and will continue to assist international or conglomerate companies in their operational development and setting because it provides a basis for the companies to develop, implement and measure information security practices effectively. It also gives room to confidence in inter-company's trading (ISO 27001: 2005, British Standard, 7799; Von Solms, 1999).

Risks are associated with the organizations because today is computer age; hence, organizations like to gain more competitive advantage over their counterparts through the use of the computer. Thus, the tendency of security threat and unwanted security incidents abound (Von Solms, 1999; Kankanhalli, Teo, Tan & Wei, 2003). According to

previous scholars, information security threat is defined as an intruder to the smooth running of information security which can take various forms such as interruption, interception, modification and fabrication (Usamni, 2008; Elky, 2006; National Institute of Standards & Technology (NIST) Special Publication 2003 pp.800-30; Pfleeger, 1989).

Usamni (2008) divided threat into four categories, namely, attack through email, spam associated threats, malware and Phishing. Malware threat reduces system network and others. In the case of threats to email, it disallows the employees to have access to the original data of the organization. Phishing threat on the other hand, involves the hacking of vital information especially hacking of credit card information, emails, or account information (Parsons et al., 2010; Mohammad & Suborna, 2009). Thus, Parsons et al. (2010) suggested that humans are the focus of the social engineering attack, because no single solution to information security improvement, diver's techniques should be used when dealing with computer security and human interaction with security systems. Hence, training employees will be of the greatest weapon against security breaches.

By and large, Straub and Welke (1998) found that the extent and nature of the information security threats are caused by the environment, it is either organizations are not absolutely protected or even prepared to alleviate the security threats. Hence, in an attempt to reduce exposure to common security threats, top managers must carry out a risk assessment of both internal and external threats to identify where the risks come from because organizational assets have come under relentless threat and there is a need to protect them from hackers (Oyetola, 2012; Akinsuyi, 2009).

According to User (2006), information system should have five key elements namely, confidentiality, integrity, availability, network security, application security and host security. All these cannot be established if data cannot be easily intercepted modified and fabricated (Butross & Ackers, 1990). These phenomena highlighted the need to have security control of information system. In the light of corporate scandals such as Enron, Parmalat, Adelphi, World Com and others, corporate leaders will be more closely monitored and held accountable for their inactions under the new Security Exchange Commission (SEC) regulations (SOX Act, 2002). This new accountability includes significant fines and jail term. A continuing stream of regulatory actions on topics ranging from anti-terrorism, anti-spam and privacy to document retention continually challenge enterprise of all sizes. In many cases, compliance must be obtained by the use of technical solutions.

Kwok and Dennis (1999) developed an information security model as part of a consultancy study for a banking organization, and this model has been extended in a collaborative research project with the National Australian Bank, funded by the Australian Research Council. The model was initially developed for risk analysis studies, as illustrated in Figure 2.2. It is therefore adapted in security audits in various organizations. In short, the model may serve as the essential security documentation for security officer, who is aiming of motivating information security culture activities , in turn inculcating information security culture to increase performance, bearing in mind that risks come from both internal and external environments.

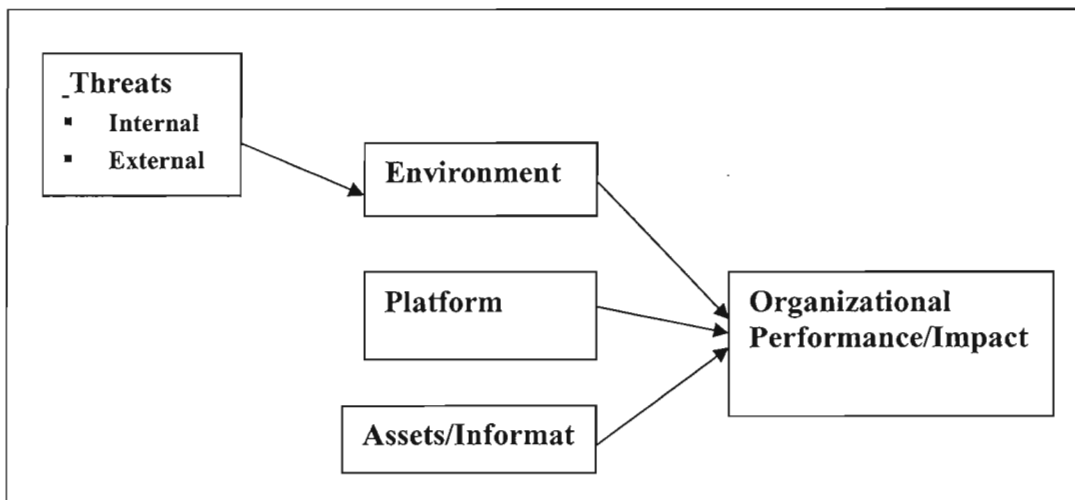


Figure 2.2
Adapted Risk Data Repository Model (Dennis, 1999)

An essential feature of the above model is that it represents, at any one time, the best set of security information available and is useful even when incomplete. When information is added to the risk data repository (RDR), it may be linked to existing components of the model, providing an essential level of cross reference, often omitted from paper documentation. It is postulated that the RDR could serve as an auditing conformance tool for the information systems standards, in addition to its role in risk modeling. The model is not only represent the best set of information currently available to the security officer, but also highlights the entities that are relevant to the security officer that are not currently available in the organizational risk data repository.

In Figure 2.2 RDR comprises of three domains: (1) environment: all those features that effectively host or support the operation of the information processing system (equipment, buildings, staff and others. (2) platform: logical, description of information

processing system and its defenses; and (3) assets: the data and processes that are to be protected because misuse of these assets would have a deleterious effect on the business operations of the organization.

From a risk viewpoint, the model depicts the fact that an external threat will impact on the information processing systems' environment. Thus, causing potential effect on the operation of the system and if the defenses are inadequate then causing some potential effect (confidentiality, integrity and availability) to the information assets which will lead to low performance. The model should contain sufficient information about its entities, and the links between the entities, to provide the best available information on the risks in relation to improved performance. The normal routine of security activities through the establishment of security culture serves imperatives to avert security breaches, which invariably will improve performance.

In overall, the understanding of security risk, threats and vulnerabilities could affect the decision to implement related information security activities. And, in turn, information security culture within the organization will produce a better performance. This is because of high level of confidentiality, integrity and availability of information as the outcome of security measures within the organization enables effective planning and controlling and eventually better operational results such as high profit and low costs. In short, it could be said that there is a potential relationship between perceived risk, threat

and vulnerabilities, information security culture and ultimately organizational performance. These elements are then included in the research theoretical framework.

2.6.3.4 Motivation of Employees

This is an act of rewarding the employees for a well done job and this could be in the form of incentives, rewards and even punishments to bring sanity to the organization (Milkovich & Newman, 1999). The employees, especially the end users of an IT system, do not know the consequences of their action. Some were of the opinion that IT helps them to carry out their obligations timely. While others were of the opinion that it hinders rather than of a necessity. That is why an organization needs to spell out the threat and the repercussions of not fully involving in the protection of their information (Hansche, 2002).

In addition, previous scholars have shown, in their studies that incentives and disincentives such as rewards and sanctions are the prerequisite for motivating employees in complying with security rules and regulations (Boss & Kirsch 2007, Lee & Lee 2002; Lee et al. 2003; Straub & Nance 1990; Willison, 2006). When employees are motivated through rewards or incentives, they would comply with the organizational information security policy, information international security standards, perform their duties efficiently and effectively.

From the above discussion, it is clear that establishing a high level of motivation amongst employees enables information security activities and in turn produces information

security culture within the organizations. This supports the establishment of relevant and reliable information and in turn robust decision making process. The outcome of this continuum is better performance. In other words, there is a potential relationship between motivation of employees, information security culture and organizational performance. Thus, they are embedded in this research theoretical framework.

2.6.3.5. Perceived Management Support and Commitment

Top management support and commitment becomes inevitable for effective establishment of information security as a norm and culture in the organizations (Babatunde & Selamat, 2011, 2012; Elchagar et al., 2012; Zakaria, 2005). This will enable organizations to efficiently improve its information processing and compete in the global market (Babatunde & Selamat, 2012). Scholars have discussed the influence of top management participation as a success factor in managing information system but not as the information security culture that can gear organizational performance (Qingxion, 2008; Liang et al., 2007; Sharma & Yetto, 2003; Purvis et al., 2001; Jarvenpaa & Ives 1991; Armstrong & Sambamurthy, 1999).

Some scholars recognized the cognitive beliefs of employees that they are being influenced by the executive management team (Liang et al., 2007; Sharma & Yetto, 2003; Purvis et al., 2001; Jarvenpaa & Ives 1991; Armstrong & Sambamurthy 1999). While Qingxion, (2008) suggested that intending researchers on information security activities should consider top management support as its influencing factors that eventually can improve organizational performance. Thus, management support and

commitment from the employees towards information security activities emanates from the top executives (Wright, 1994). And, when top management participates in information security initiatives, it gives an impression of their support and other employees will not see initiatives as an extra burden but a signal of how to value the initiatives.

Secondly, they understand their business to the best of their knowledge (Thong et al., 1996). Information security governance through the top management support expedites the implementation of information security activities initiatives as well as bringing information security culture alignment with the corporate objective and strategies (Liang et al., 2007; Sharma & Yetto, 2003; Purvis et al., 2001; Marcus, 1981; Javenpaa & Ives, 1991). Rapidly changing technology calls for huge investments in information security activities. Therefore, top management is in best position to identify business niches and opportunities.

Previous researchers have demonstrated that management commitment is positively associated with the perceived ease of use of security practices in the organization (Ismail, 2009; Chang & Ho, 2006; de Guinea et al., 2005; Foong, 1999; Igarria et al., 1997). These studies stipulated that top management supports and participation is an important factor for managing IS effectively for a better performance. Additionally, it is also found that companies that receive management supports are able to increase security awareness among employees through active programs (Domínguez, 2009).

Moreover, to be successful in business operation, Ismail et al (2007) argued that there is a need to implement a strategic IT plan, and this should be supported by IT structures and governance. More importantly, the commitment from the top management leads organizational plans into actions. Inability of the top management in supporting information security programs will lead to inadequate planning (Ismail et al., 2008). In turn, an organization could be vulnerable to risks of threat and hackers because proper security measures are not in place. Computer security does not start with the implementation of firewalls or software, but with the top management enforcing security policies (Ismail et al., 2007).

Perceived top management commitment and support also enhance information security implementation effectiveness (Aggrawal, 2003; Sharma & Yetton, 2003; Tompkins, 2002; Marcus, 1981). Gupta et al. (2005) in their study of information security among American SMEs found that there is a difference between an organization that has strong management support and commitment than the one with little support and commitment from the top management, for the former will engage in more corrective and preventive measures in information security activities than the latter.

In addition, perceived top management support and commitments enable the awareness and training programs, commitment to information security policy and the allocation of more resources to the information security activities (Sharma & Yetton, 2003). They should understand the importance of their involvement in information security culture activities because they contribute to information security implementation success, create

an organizational performance structure that can facilitate the implementation of information system security initiatives (Qing, 2005; Ragu-Nathan et al., 2004; Sharma & Yetton, 2003; Marcus, 1981).

In summary, it is argued that perceived top management support and commitment encourages the implementation of information security activities. Ultimately, these activities establish information security culture. This continuum in turn leads to better organizational performance through better decision making and controlling processes. Thus, perceived top management support and commitment, information security culture and organizational performance are included in this research framework.

2.6.4.6 Perceived Job Roles and Responsibilities

A clear job roles and responsibility enable an organization to perform its functions effectively and efficiently (Abu-Zineh, 2006; Toval et al., 2002). For instance, allocating information security responsibilities amongst the employees has been an integral part of the information security success (Toval, et al; 2002). Hence, a clear definition of information security tasks for every employee is considered as success factor in information security practices (Zineh, 2006; Bjorck, 2001). Abu-Zineh (2006) defined information security responsibilities as designating information ownership to employees and thus enable them to efficiently perform their information security duties. In other words, the employees should be aware of information security requirements throughout the life cycle of information process (Nosworthy, 2000).

Additionally, Hone and Eloff (2002) and Wilson and Simon (2005) argued that information security policies enable clear guidelines and instructions. It comprises all information security responsibilities that enable the employees to know what is exactly expected when protecting information assets. In short, there is a potential relationship between clear job roles and responsibilities and information security practices and eventually information security culture. The increase in information security culture, in turn, leads to better organizational performance. Thus, all of them are included in this research theoretical framework.

2.7 Information Security Culture as a Mediating Variable

From the above discussion, it is clear that information security culture acts as a mediating variable research theoretical framework. Culture is defined as a system of values, norms and beliefs that influence society, organizations and political systems (Robbins, 2005; Brown, 1995; Hofstede, 1997; Baldwin et al., 1999). Culture is also a learned process which could serve as motivation to employee not only to perform but to be loyal to information security practices for organizational performance (Robbins, 2005; Hofstede, 1997). Thus, it has to do with power distance, individualism, collectivism, quantity and quality of life, uncertainty avoidance and orientation for short and long term (Robbins, 2005).

Organizational culture provides the social glue that gives an organizations identity, coherence, shape and direction (Robins, 2005). Also, scholars suggested that organizational culture influences an employee's commitment, involvement, and

commitment (Deal & Kennedy, 1982; Peters & Waterman, 1982). The difference between national and organizational culture is just that national culture comprises of the norms, beliefs of the entire nation while organization culture is meant to guide the employees within the organization. Thus, information security culture represents the norms and values that propel employees to comply with information security practices to improve organizational performance. Robbins (2005) posited that national culture, organizational culture and employees' behavior are correlated.

In addition, culture is further defined as the backbone of efficient business value because it guides and enables employees to be committed to the organization (Schein, 1999, Denison, 1990). In other words, it acts like guidance to shape the employees' behavior in order to fulfill organizational mission and vision (Denison, 1990; Schein, 1999). Furthermore, it is an approved method in which employees' duties are carried out in the organization (Blake & Mouton, 1969; Schein, 1999; Lim et al., 2009).

Moreover, an organization establishes information security culture by motivating their employees through training, adhering to privacy principles, and participating in security making processes and risk analyses and including management commitment to security (Beachboard, 2004, Von Solm, 2004). The impact of information security culture on the aspect of performance improvement, information policy and managerial effectiveness cannot be over emphasized (Claver, Llopis & Gonzalez, 2003; Gasco, 2003; Beachboard, 2004, Von Solms, 2004). When information security culture is established

in the organization, it helps in establishing with the employees by providing acceptable rules and standards (Lim et al., 2009). In other words, it acts as a control measure that guides and shapes employees attitudes and behaviors. Robey and Boudreau (1999) opined that organizational security culture causes the resistance towards new technology and transformation.

However, Christopian (2008) was of the opinion that it is difficult to assess organizational culture in relation to knowledge management. Organizational culture is related to a society or nation where the organization operates (Connar, 1997). Bearing the above discussion in mind, this research argues that organizational information security culture should be seen as the embodiment of organized activities for business value and as a gateway for effectiveness in meeting the challenges of the global competitiveness rather than opposing 'new technology or transformation'. The antidote of an information security culture is training where the mindsets of the employees are prepared or nurtured towards new technology (Aggrawal, 2003).

By and large, information security culture is considered as the main features of organizations in order to increase performance (Gebrasilase Lessa, 2011). Previous studies argued that information security culture is interrelated with organizational culture because it guides the employees' behaviors in information security (Ramachandran et al., 2008; Andress & Fonseca, 2000; Von Solms, 2000; Dhillon, 1997), and in turn beliefs that information security culture should be embedded into the organizational culture.

Some researchers postulated that there are challenges in inculcating information security culture because of its critical reason to the success or failure of the overall information system performance (Zakaria, 2007; Knapp, et al., 2006, Chia et al., 2006; Kraemer & Carayon, 2005). Lim et al. (2009) and Fitzgerald (2007) uncovered that the organizations have the option to establish information security culture or not, while Dzazali and Zolait (2012) argued that employees' behavior need to be changed regarding information security issues. Alnatheer and Nelson (2009) found that information security culture and information security practices are the most challenging factors in implementing security management in Saudi Arabia.

However, from the previous researches on information system, there is a need to emphasize employees' behavior and the support of organizational activities so that information security culture becomes employees' nature (Alnatheer & Nelson, 2009; Chen, Medlin & Shaw, 2008; Martins & Eloff, 2007). In line with the inconsistent findings of the previous studies, it is argued that information security culture will strengthen the relationship between information security activities and organizational performance. Thus, this study uses information security culture as a mediator between information security activities and organizational performance in order to strengthen and energize the relationship between them. When information security practices are in place in the organization through information security culture, organizational performance will be enhanced (Frasier, Baron & Tix, 2004; Baron & Kenny, 1986).

Based on the above discussion, it is argued that information security culture has a potential to affect the performance in the banking sector. Thus, it is included in this research theoretical framework as mediating variable between information security practices and organizational performance.

2.8 Organizational Performance as a Dependent Variable

From the above discussion, it is clear that organizational performance acts as a dependent variable in this research theoretical framework. To be specific the dependent variable is organizational performance. The use of performance indicator to verify the effectiveness of information security practices and in turn information security culture is relatively new (Elchagar et al., 2012). Although stipulated by ISO/ IEC 27001, the indicator does not stipulate how and why. Information security risks are considered as major challenges faced by organizations because an external security phenomenon is much less than internal security (Elchagar et al., 2012; Olugbode et al., 2008; Kraemer & Gubaxani, 2004; Ville et al., 2004; Briney, 2001).

The main objective of an organization is to increase sales volume, profit and create a niche for a competitive advantage in the global market. Human beings are the brain behind improving performance either negatively or positively. Hence, the need for establishing information security culture becomes inevitable. However, the desire of the top management in the organization for information security will equally serve as a catalyst to solve the effect of information security risks in the organization (Ransbotham & Mitra, 2009; Lohmeyer et al., 2002; Brancheau et al., 1996).

Managing information is more than operating procedures and processes in which crucial components such as organizational infrastructure, human factors, technology and information security activities are involved. Therefore, information security resources are critical assets that support the mission of the organization. Lederer and Gardiner (1992) supported this argument by saying that the effectiveness of security control depends on the system management. If not properly handled, it could lead to misfortune that may eventually jeopardize performance in the organizations. Information security is never produced by a member of the management; rather it ensures that all members are contributing to effective management of security practice. Hence, the need arises for clear communication of information security from the top management down to the lower management in order to have a positive organizational performance (Carr, Amedia, Kaynak & Hale, 2008).

North (1990) was of the opinion that a group of individual e.g. employers-employees are bound by some common purpose to achieve organizational performance. In other words, everybody in the organization makes things work especially when information security is concerned. Solms (2000, pp. 616-618) stipulated that, the standardization of certificate and security, metrics emerged due to top management continuously asking about the progress and result of technical, management, institutional wave and that of the employee were recognized as relevant for information system which led to a postulation to the establishment of culture in information security (the fourth wave). To achieve maximum security for effective organizational performance, cooperation in terms of coordination, participation and motivation from the top management down to the lower level could be

of great help. This study includes the fourth wave (information security culture) as the basis of discussion. Based on this discussion it is included in the research framework.

2.9 Underpinning Theories

The underpinning theories that explain the interaction between information security practices and organizational performance are drawn mainly from technological-organizational-environment theory (TOE theory). This is further supported by security system theory and security policy theory. This is explained in Subsections 2.9.1 - 2.9.3 below.

2.9.1 Technological, Organizational and Environmental Theory

To understand the critical success factors of information security culture and in turn organizational performance in the banking sector TOE theory is adopted. Tomartzky and Fleischer (1990) developed TOE theory that best describes organizational elements that affect organization in decision making. The theory consist of three elements, namely, technology, organization and the environment. The technological context imbibe that organizations are influenced by both internal and external factors such as the adoption of new IT, the advancement of IT in-sourcing and the diffuse of IT knowledge and skills. The phenomena with the organization consists of organizational context, such as the size of the organization, motivation of employees, perceived management support and commitment, policy, information security awareness, perceived training programs and others, while environmental context includes international security standards, perceived government rules and regulations.

The empirical studies such as Ifinedo (2011), Intan Salwani et al. (2009), Kraemer and Govindarajulu (2006), Zhu and Kraemer (2005), Zhu et al. (2004, 2003), Thong, (1999), Chau and Tam, (1997) and Iacovou et al, (1995) supported the use of Tomartzky and Fleischer's (1990) framework. As the use of TOE theory is pervasive in the information system area, it is adopted in this research theoretical framework. Thus, this research theoretical framework has three constructs which are technological, environmental and organizational constructs (information security practices). The implementation of information security practices enables information security culture to be established efficiently and effectively. In turn, the organization will be able to increase its performance, have a niche and competitive advantage.

2.9.2 Security Policy Theory

The security policy theory assists the organizations to establish, implement and maintain its objectives (Gupta et al., 2001; Hong et al., 2000). Kabay (1996) posited that the establishment of a security policy should be able to maintain, assess and persuade the top management on one hand, and analyze information security requirements on the other. In short, the security policy theory is applicable in this study because information security policy can motivate information security practices. This is evident from the inclusion of an organizational factor in this research theoretical framework.

2.9.3 Security System Theory

Information security research builds on established system properties, principles, laws and theories that have been developed and polished for several years using empirical data (Skyttner, 1996; Yngström, 1996; Kowalski, 1994). Security systems theory is a body of concepts and methods for the description, analysis and design of complex entities (Finkelstein, 1988). The classical domain in which security systems theory is applicable is that of the information processing and computing systems, all of which consist of component equipments functioning together as a whole (Boulding, 1956). Apart from difficulties faced in classifying systems, systems principles which are relevant to systems security must also be dealt with. A principle is a generalization founded on empirical data not yet qualified into a law (Skyttner, 1996).

Information systems, like organizations are social systems which use technology to help achieve its goals. Checkland (1981) foresaw the systems as 'human activity systems'. In short, security system theory is applied in this study because of its determinant factors of information security practices, in which this study is premised on. This is evident from the inclusion information security practices and organizational performance as the dependent variable in this research theoretical framework.

2.10 The Proposed Theoretical Framework

Based on the above discussion, it is declared that the independent variables of this study are made up of: (1) technological context- perceived technology advancement, information security in-sourcing; (2) environmental context- international security

standard, perceived government rules and regulation; and (3) organizational context - information security policy and procedure, information security awareness, perceived training programs, perceived information security risk threat and vulnerability, motivation of employees, perceived management support and commitment and perceived job roles and responsibilities. On the other hand, information security culture is the mediating factor while the dependent variable is organizational performance. The diagram of the relationship between independent variables, mediating variable and the dependent variable is illustrated in Figure 2.3.

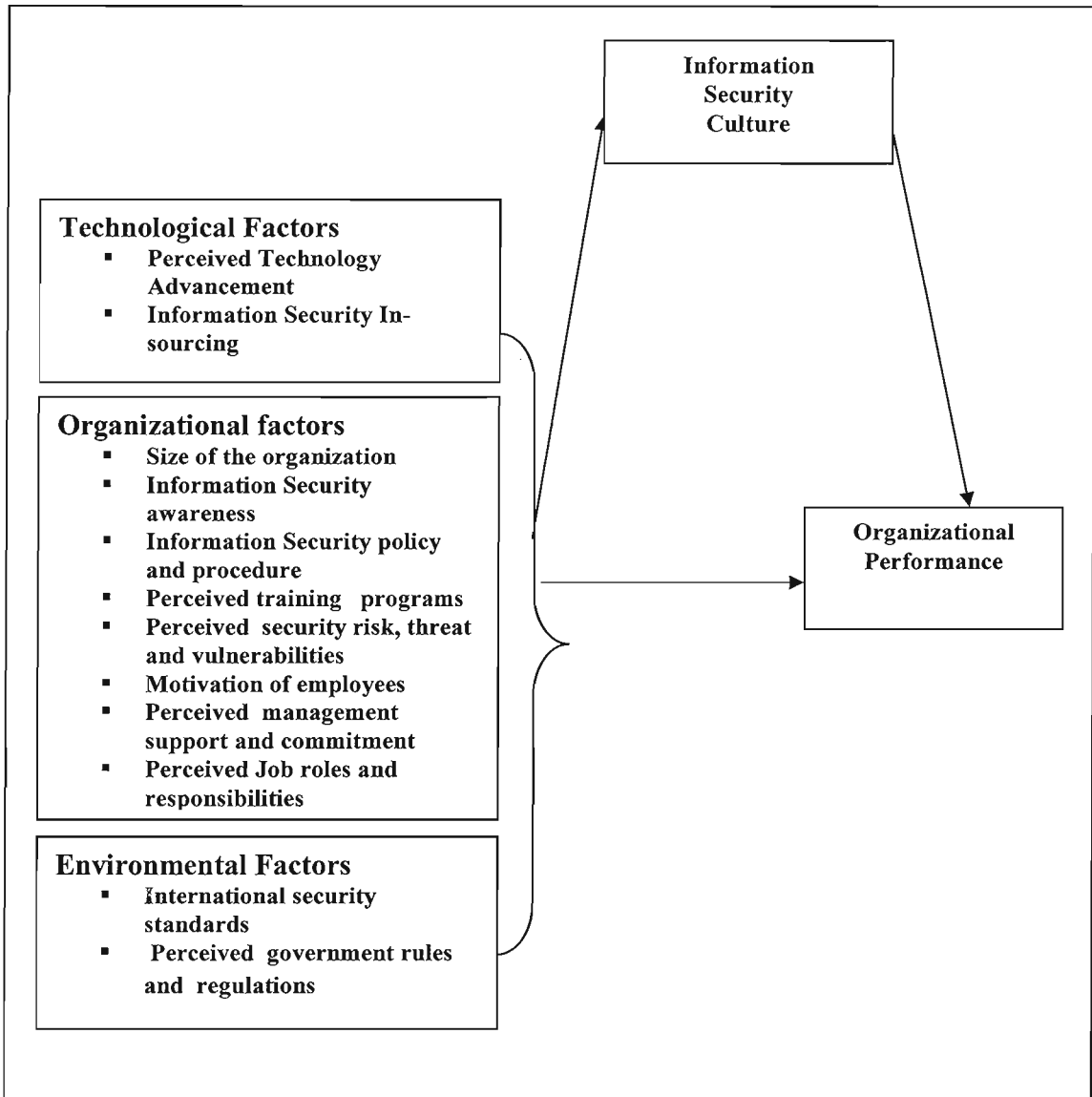


Figure 2.3
The Proposed Theoretical Framework

2.11 Summary

In summary, this chapter discusses the literature that relates to information security. The study adopted information security culture as mediating variable between information security activities and organizational performance. The focus of the study is on the need

for establishing information security culture in order to improve organizational performance in the Nigerian banking sector. To validate the research framework, a systematic research methodology is discussed in chapter 3.

Table 2.1
Summary of Literature Review

| No | Section | Outcome |
|-----------|----------------|--|
| 1 | 2.2 | Highlighting Nigeria's banks as a case study |
| 2 | 2.3 | Discussion on information security transformation |
| 3 | 2.4 | Importance of information security culture |
| 4 | 2.5 | The relationship between information security and organization performance |
| 5 | 2.6 | Establishing Information security culture on independent variables |
| 6 | 2.7 | Information security culture as a mediating variable |
| 7 | 2.8 | Organizational performance as a dependent variable |
| 8 | 2.8 | Supporting independent variables, dependent variable, mediating variable with underpinning theories. |
| 9 | 2.9 | Establishing proposed theoretical framework |

CHAPTER THREE

RESEARCH HYPOTHESES AND METHODOLOGY

3.1 Introduction

This chapter presents the methodology that was used to achieve the study objectives in chapter one and to test the hypothesis of the study. To validate the theoretical framework discussed in chapter two, quantitative paradigm was used. This was made possible through the use of questionnaires to achieve a better understanding of the information security culture. The discussion, among others, includes: research design, hypothesis development, population, sample, and statistical techniques that were used to analyze the data. The summary is offered at the end of this chapter.

3.2 Hypothesis Development

This section discusses the hypotheses of both the main effect and indirect effect relationship of the variables that are developed in this research study. These hypotheses are developed based on the framework in figure 2.3.

3.2.1 The Main Effect

The main effect often referred to as a direct effect, measures the direct relationship between information security practices and organizational performance.

3.2.1.1 Perceived Technology Advancement

This is the era where IT is increasing in usage globally. Thus, managing IT function has become the most difficult phenomenon in recent years. The technical know-how due to increasingly sophisticated online business transactions (E-business) is becoming an issue. The top executives are compelled to IT as an organizational strategic player in inculcating information security culture (Boynton et al., 1994; Orlikowski & Barley, 2001; Sambamurthy, 2000; Venkatraman & Henderson, 1998; Grainger-Smith and Oppenheim, 1994; Hill, 1999). Therefore, this hypothesis is proposed:

H1: There is a significant relationship between the perceived technology advancement and organizational performance.

3.2.1.2 Information Security In-sourcing

The organizations sometime lack expertise in the information security issues. Therefore, these organizations are induced to rely on information security from internal advisors to support their information security practices in achieving organizational performance that will lead to competitive advantage. Some of these organizations are unable to meet the need of the global challenges, hence they outsource for the IT experts outside and to keep at pace with competitive world (Samadder & Kadiyala, 2006). Therefore, the following hypothesis proposed that:

H2: There is a significant relationship between information security in-sourcing and Organizational performance.

3.2.1.3 International Security Standards

The standards aim to enhance the confidence of stakeholder among the organizations (ISO/ IEC/17799-1; 2005; 277001). Adopting international standards provides an organization with an adequate assurance to safely interact with each other, and give confidence to the investors (ISO/ IEC/17799-1; 2005; 277001). Implementing these standards will significantly affect organizational performance and improve an organization's information security objectives (NIST; ISO, 277001). This, in turn, enhances organizational performance that gives business continuity (Omu 2010: New Vista for banking operations; This Day Newspaper, September 2010). For this reason, it is hypothesized that:

H3: There is a significant relationship between compliance with international security standards and organizational performance.

3.2.1.4 Perceived Government Rules and Regulations

The regulatory bodies such as Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, Basel II, and the European Data Privacy Directive, Central Bank of Nigeria and the Nigerian Deposit Insurance Corporation allow the organizations not only to maintain information security but also to increase the integrity of their information system (Domínguez, 2009). The Central Bank of Nigeria and the Nigerian Deposit Insurance Corporation are the regulating bodies of the Nigerian banking system. More importantly, Central Bank of Nigeria is the apex ruling body of the Nigerian banks because the Nigerian banking system is not fully integrated with international financial system. Information security

standards remain static in some part of the country (NDIC 2009, CBN Annual Report, 2009, Akinsuyi, 2009). Therefore, the following hypothesis is proposed.

H4: There is a significant relationship between perceived government regulation and organizational performance.

3.2.1.5 Size of the Organization

As organizational strategies change over time due to innovation, the need to strategically be on the safe side to meet with the competitive demand of the present changes in technology provided by the ICT inventions is stressed (Wang & Zhao, 2011; Kalianna & Awang, 2010). Every organization requires different security needs, and organizational goal to achieve better performance (Wang & Zhao, 2011; Kalianna & Awang, 2010). Thus, the larger the size of the organization the bigger the prerequisite for information security practices that can gear up for a better performance (Sovalainen, 2000; Wood, 1999; Scweithzer, 1992).

Many organizations do not possess good security documentation either because the effort of data collection is so high that they are inhibited from undertaking the risk analysis study, or if such a study is undertaken, the resulting documentation is not formatted, which lends itself to ease of updating and use (Kwok & Longley, 1999). Fenny et al. (1992) found that information security activities must be monitored by chief information officer to ensure its success. Implicit in this scenario is that large organizations have adequate cash, information technology experts, capability and the need to establish

effective and efficient information security plan compared with small and medium enterprises. Therefore, the following hypothesis is proposed.

H5: There is a significant relationship between the size of the organization and organizational performance.

3.2.1.6 Information Security Awareness

Information security awareness could be termed as a countermeasure against human errors and failures (Parsons et al., 2010). It enables an organization's employees to understand information security aspects (Parsons et al., 2010; Besnard & Arief, 2004). To avert the issue of human factors such as errors and failures in carrying out information security practices, employees should be provided with security awareness as part of initial initiative to be embarked upon as soon as they are employed in the organization. Such awareness should be done on a regular basis and must be given appropriate assessment and evaluation.

Security awareness will be productive when management leads by example (Zakaria, 2005). Unfortunately, a lot of organizations still think that the technical solution is all that is required to solve information security issues. Besnard and Arief (2004) opined that employee education enables people to be aware of the consequence of their actions. However, a research carried out by Computer Crime and Security (2007) found that 18% of organization do not use any form of security awareness and even those organizations

who create awareness refuse to measure the efficiency of the awareness programs (Richardson, 2007).

According to Peltier (2005), there are three elements in the learning curve of information security, namely, information security awareness, training programs and education. In addition, Domínguez (2009) found out in his study that the organizations that implement information security awareness receive management support for the security awareness programs. Therefore, the hypothesis is stated as thus:

H6: There is a significant relationship between information security awareness and organizational performance.

3.2.1.7 Information Security Policies and Procedures

The organizational goal of implementing policy is to influence behavior through decisions and actions taken (Thompson, et al., 2006; Whiteman & Mattord, 2003). Information security policy and procedure is imperative parameter used in security practices. It spells out what employee should do and what not to do for a better performance (Parson et al., 2010; Hone & Eloff, 2003; Whiteman & Mattord, 2003). It stipulates the policies, procedures and structure to be followed in the organization.

Practically, information security policy and procedure indicates the top management's commitment towards protection of the information assets. There are many international standards that explain the procedures and controls of Information security policy and

procedure. Adopting these international standards gives Information security policy and procedure an integral role in the success of organizational performance. Hence, the following hypothesis is proposed.

H7: There is a significant relationship between information security policy and organizational performance.

3.2.1.8 Perceived Training Programs

The perceived training programs are the prerequisite for information system security development process and lack of training contributes to inadequate security, especially where employees are concerned (Babatunde & Selamat, 2012; Domínguez, 2009; Zakaria, 2007; Peltier, 2005; Briteny, 2001). The developed set of security processes provides valid content for training in the field of security management in the organizations. Parker (1984) opined that “An effective information security program incorporates a combination of technological and human controls in order to avoid the loss of information, deter accidental or intentional unauthorized activities, prevent unauthorized data access, detect a loss or impending loss, recover after a loss has occurred, and correct system vulnerabilities to prevent the same loss from happening again”.

Beside the ISO 27001 (2013) requirements, the above processes represent an overview of activities required by the international security standard. The Organization for Economic Cooperation and Development Guidelines for the Security of Information

Systems and Networks stated that: “Towards a culture of security underlines” the need for a greater awareness and understanding of security issues and practices to develop a common background among citizens, particularly information communication technology practitioners.

Moreover, IT personnel and chief information security officer, in an attempt to improve organizational performance through the implementation of information security practices, can avail themselves of going for security awareness and training programs in order to update themselves of the current trends in security measures. To implement a successful information security practices within the organization, employee training should not be overlooked because human factors influence behavior and due to employees knowledge that are limited, there is a possibility of not knowing degree of the information risks (Parson et al., 2010; Wilson & Simon, 2005; Fischhoff, 2002; Kenning, 2001).

The previous researchers such as Schlienger and Teufel (2002), Wright (1998) and Zakaria (2007) were of the opinion that overlooking employees’ training could lead to internal security incident. Also, there is a need for use and reading of educative CPA journals where information on reducing the threat levels of accounting information system challenges for management, accountants, auditors and academicians could serve as an avenue for the training program. In line with this, the below proposition is made:

H8: There is a significant relationship between the perceived training programs and organizational performance.

3.2.1.9 Perceived Information Security Risk, Threat and Vulnerabilities

Risk is associated with the organization. Thus, the organizations are prone to risks. A deep understanding of the risks will lead managers to seek for control (Straub & Welke, 1998). The previous researchers concluded that there are threats and vulnerabilities to information assets. The threats reduce system network, and vulnerabilities enable hacking into vital information. Hence, employees will not have easy access to information and, if not addressed, will jeopardize organizational performance (Pfleeger, 1989; Usamni, 2008; Mohammad & Suborna, 2009).

Organization need to be proactive to protect their information because of enormous increasing threats and vulnerabilities. Thus, perceived information security policy and procedure plays an imperative part in achieving organizational strategic plans with little or no threats to information. Straub and Welke (1998) found that the extent and nature of the information security threats and vulnerabilities are caused by the environment. Organizations are either not absolutely unprotected or even prepared to alleviate the security threats. Based on the inclusion of information security threat and vulnerabilities in the framework, the following hypothesis is developed.

H9: There is a significant relationship between perceived information security risks threat and vulnerabilities and organizational performance.

3.2.1.10 Motivation of Employees

Information security participants, managers, and those handling different areas in the organization are to be motivated to securely exploit the information security activities (Miskell & Miskell, 1991; Maslow, 1997). The great scholars focus was on the human factors and in what way these factors could be managed for successful implementation of information security activities (Parker, 2002). Motivation is directly linked to job performance because it will affect the entire management (Miskell & Miskell, 1991; Maslow, 1997).

When performance is affected, organizational performance will be hindered. It is imperative that the motivation enables employees to be highly convinced about the benefits of information security efforts towards organizational performance while rewards encourage employees to do more. In fact, employees that are motivated through benefits such as rewards and remuneration in form of bonuses, incentives, promotion, and satisfaction with conducive working environment will increase growth and organizational performance (Mozina, 2002; Rosenbloom & Hillman, 1991; Miskell & Miskell, 1991; Maslow, 1997). Therefore, the following hypothesis is proposed.

H10: There is a significant relationship between motivation of employees and organizational performance.

3.2.1.11 Perceived Top Management Support and Commitment

Perceived top management support and commitment highlight the commitments given by the top executives in all activities of the organization, especially the protection of information security. Previous scholars have discussed just a little about the influence of the top management support as a success factor in enabling information security (Chang, & Ho, 2006; Alshawaf et al., 2005; Kearns & Lederer, 2004; Kankanhalli et al.; 2003; Chou & Jou, 1999). Their studies focused on the relationship between organizational size and industry type (Chang & Ho, 2006; Alshawaf et al., 2005; Kearns & Lederer, 2004; Kankanhalli et al.; 2003, Chou & Jou, 1999).

In addition, Chan and Ho (2006), Ettredge and Richardson (2002) were of the opinion that further studies should include top management support as part of the information security governance, the fourth wave of information security (Elanchgar, Boulafourd, Makoudi and Regragui, 2012). However, leaders who live by example makes information security possible (Zakaria, 2005). Top management's support and commitment have been found to be part of the fourth wave (Boulafourd et al; 2012) because it is responsible for initiating awareness and training programs, commitment to the information security policies and procedures (ISPP), and allocation of more resources to the improvement of information security environment (Domínguez, 2009). Thus, the following is hypothesized is:

H11: There is a significant relationship between perceived top management support and organizational performance.

3.2.1.12 Perceived Job Roles and Responsibilities

Job allocation or division of labor plays an important role in clarifying and defining how the responsibilities of information security are performed by the employees within the organization (Toval et al., 2002). The structuring and allocation of the job responsibilities and roles could be such that the organizations define and clarify information security tasks for every employee, and are considered as defining factors in the information security success (Bjorck, 2001, Sami Abu-Zineh 2006). Therefore, the following hypothesis is proposed

H12: There is a significant relationship between perceived job responsibilities and organizational performance.

Table 3.1 below summarizes the relationship of the research questions 1 and the hypotheses of the determinants of TOE factors that influence organizational performance.

Table 3.1

Summary of TOE Factors and Organizational Performance

| Research Questions | Hypotheses |
|---|---|
| What elements such as technological, organizational and environmental factors that influences organizational performance? | H ₁ : There is a significant relationship between perceived technology advancement and organizational performance |
| | H ₂ : There is a significant relationship between information security in-sourcing and organizational performance |
| | H ₃ : There is a significant relationship between international security standards and organizational performance |
| | H ₄ : There is a significant relationship between perceived government rules and regulations and organizational performance |
| | H ₅ : There is a significant relationship between size of organization and organizational performance |
| | H ₆ : There is a significant relationship between information security awareness and organizational performance |
| | H ₇ : There is a significant relationship between information security policies and procedures and organizational performance |
| | H ₈ : There is a significant relationship between perceived training programs and organizational performance |
| | H ₉ : There is a significant relationship between information security risk threat and vulnerabilities and organizational performance. |
| | H ₁₀ : There is a significant relationship between motivation of employees and organizational performance organizational performance. |
| | H ₁₁ : There is a significant relationship between perceived top management support and commitment and organizational performance. |
| | H ₁₂ : There is a significant relationship between perceived job roles and responsibilities and organizational performance |

As discussed in chapter 2, this research also intends to investigate the establishment of information security culture. Thus, the above factors are linked to the establishment of information security culture. Table 3.2 illustrates the hypotheses of the relationship between technological, organizational and environmental factors and information security culture.

Table 3.2

Summary of Hypotheses on TOE Factors and Information Security Culture

| Research Questions | Hypotheses |
|--|--|
| What is the relationship between TOE factors and information security culture? | H ₁₃ : There is a significant relationship between perceived technology advancement and information security culture |
| | H ₁₄ : There is a significant relationship between information security in-sourcing and information security culture |
| | H ₁₅ : There is a significant relationship between international security standards and information security culture |
| | H ₁₆ : There is a significant relationship between perceived government rules and regulations and information security culture |
| | H ₁₇ : There is a significant relationship between size of organization and information security culture |
| | H ₁₈ : There is a significant relationship between information security awareness and information security culture |
| | H ₁₉ : There is a significant relationship between information security policies and procedures and information security culture |
| | H ₂₀ : There is a significant relationship between perceived training programs and information security culture |
| | H ₂₁ : There is a significant relationship between information security risk threat and vulnerabilities and information security culture. |
| | H ₂₂ : There is a significant relationship between motivation of employees and information security culture |
| | H ₂₃ : There is a significant relationship between perceived top management support and commitment and information security culture. |
| | H ₂₄ : There is a significant relationship between perceived job roles and responsibilities and information security culture |

3.3 The Indirect Effect

The present study also endeavored to examine the effect of information security culture as a mediator between information security activities and organizational performance. The researcher wants to investigate the role of information security culture as a mediator between information security activities and organizational performance. The researcher deem it right to study the effect as the area has not been explored. It is only assumed by few researchers that information security activities can influence organizational performance, while others suggested that it will strengthen the relationship if it is used as a mediator. In this study, the possible effect of information security culture with information security activities will be considered as exploratory (Subramanian, 2009). As suggested by Sekaran (1998) and Subramanian (2009), a situation where the relationships have never been previously explored, a non-directional hypothesis should be formulated. Therefore, the following non-directional hypotheses are hereby developed in this research.

3.3.1 Information Security Culture as a Mediating Variable

A mediator is subjective or objective in nature because it affects the strength and directions of a relationship between a predictor and the criterion (Baron & Kenny, 1998; Sekaran, 2003; Muller et al; 2005). The mediating effect implies that the relationship between the predictor and criterion varies as a function of the outcome called a mediator (Aguinis, 1995). Hence, Ramayah (2011) and Baron and Kenny (1986) refer to mediating variable as a contingent variable because it changes the strength and the form of the relationship by specifying occurrence in a particular effect. A mediator also refers

to as intervening variable that occurs between a given time that independent variable functions to influence the dependent variable and the effect on the dependent variable (Sekaran, 2003).

Also, the effect of both criterion and prediction relationship depends on the degree or worth and importance of mediator (Holmbeck, 1997). This indicates that, the relationship between information security practices and organizational performance varies as a function of the information security culture because it enhances the indirect relationship between the two variables. Sometimes, the direction between the two variables may be positive or negative or even otherwise (Lindley & Walker, 1993). Thus, information security culture hopefully will mediate positively the relationship between information security practices and the organizational performance cannot be underrated. This is because mediators are introduced to strengthen the relationship between the predictor and criterion (Baron & Kenny, 1986; Holmbeck, 1997).

By and large, mediation is categorized into: (1) test of causal steps, (2) test of difference in coefficient, and (3) test of the product of the coefficient (MacKinnon, Warsi & Dwyer, 2002).

3.3.1.1 Test of Causal Steps

There are four causal steps and approaches for mediation to transpire according to Judd and Kenny (1981), Baron and Kenny (1986) such as (1) the total influence of

technological factors, organizational factor and environmental factors (TOE factors) on organizational performance and must be significant (2) the effect of TOE factors on information security culture must also be significant (3) the influence of information security culture on organizational performance controlled for TOE factors must be relevantly significant (4) the direct influence of TOE factors on organizational performance for information security culture (b^1) must not be significant.

However, there are distinctions between partial and full mediation. Baron and Kenny (1986) explain that in a phenomenon where all the four steps are met with a model is referred to as full mediation models. While there will be a partial mediation, where the requirement in step 4 mentioned above is that b^1 is relatively ^{less} than b , rather than b_1 is relatively not substantial.

By and large, the differences in coefficient tests are conducted by considering the overall difference between TOE factors (X) on organizational performance and the direct effect of TOE (X) on organizational performance (Y) adjusted for Information Security culture (M), the total effect less direct effect ($b-b_1$) and dividing by the standard error of the differences. This value could be compared against a t- distribution to test for the significance. The core difference between the ranges of difference in coefficient test is the use of different methods for calculating the standard error of the differences.

3.3.1.2 Product Coefficient Test

According to MacKinnon and Fritz (2007) product coefficient test relate to the products of the coefficient of the independent variable to the mediating variable- a , and the coefficient from the mediating variable to the adjusted for the independent variable, β which is divided by the standard error product to create a test statistic. This test statistic accordingly evaluated against a normal distribution to test for the significance. Regardless of the differences between the product of coefficient test and the difference in coefficient tests, MacKinnon et al (1995) pointed out that $b-b_1 = a\beta$ for ordinary least square regression. This is sometimes not true where logistic regression models are concerned.

In this study, information security culture is introduced as a mediating variable in order to strengthen the relationship between information security practices and organizational performance (Barron & Kenny, 1986) as rightly discussed above. An organization establishes an information security culture by motivating their staff through training and using internal controls to obey security principles such as trust, and strictly adhering to privacy principles, and participation in security making processes and risk analyses, including management commitment to security, budget and security (Christopher, 2008). This is evidence that information security culture will enhance security culture to improve performance in the organization. It is succinctly that relating organization with knowledge management could be difficult, but will be much better when relating it to a society or nation where the organization operates (Connar, 1997; Christopher, 2008).

Based on this, the following hypotheses were proposed. Please refer to Table 3.3. Table 3.3: Relationship of the Research Questions 3, the hypotheses of the mediating effect of information security culture on the relationship between TOE factors and organizational performance.

Table 3.3
Summary of the Hypotheses of the Mediating Effect of ISC on TOE Factors and Organizational Performance

| Research Questions | Hypotheses |
|--|--|
| Does information security culture mediate the relationship between TOE factors and the organizational performance? | <p>H₂₅: information security culture mediates the relationship between perceived technology advancement and organizational performance.</p> <p>H₂₆: information security culture mediates the relationship between information security in-sourcing and organizational performance.</p> <p>H₂₇: information security culture mediates the relationship between international security standards and organizational performance.</p> <p>H₂₈: information security culture mediates between government rules and regulations and organizational performance</p> <p>H₂₉: information security culture mediates the relationship between size of organization and organizational performance.</p> <p>H₃₀: information security culture mediates the relationship between information security awareness and organizational performance.</p> <p>H₃₁: information security culture mediates the relationship between information security policy and procedure and organizational performance</p> <p>H₃₂: information security culture mediates the relationship between the perceived training programs and organizational performance.</p> <p>H₃₃: information security culture mediates the relationship between perceived information security risk, threat and vulnerabilities and organizational performance.</p> <p>H₃₄: information security culture mediates the relationship between perceived top management support and commitment and organizational performance.</p> <p>H₃₅: information security culture mediates the relationship between motivation of employees and organizational performance..</p> <p>H₃₆: information security culture mediates the relationship between perceived job roles and responsibilities and organizational performance.</p> |

3.4 Research Design

Research design is carried out to provide necessary information on the research and then hypothesize in an accurate manner (Hair, Money, Samuel & Page, 2010; 2007; Sekaran & Bougie, 2011, 2010, 2009). It is also an avenue for the researcher to use series of investigation to carry out data collection.

Research design is categorized into exploratory, descriptive and causal (Hair et al., 2010; 2009; 2007). Descriptive research is used to collect data based on the description of the research topic. It consists of structured questions through questionnaires, interview and observation. It is divided into longitudinal and cross-sectional studies (Hair et al., 2010). In a longitudinal study, the data are collected from the same element at multiple sources in time while causal seeks to examine whether one event causes another, this could be before and after the study. Lastly, cross-sectional study is frequently used in social research because it involves the use of data collection at a point in time to get a quality data on two or more occasions. This shows their level of relationships upon examination and ability to achieve a purposeful obligation (Hair et al., 2010; Denscombe, 2010). Thus, this study employs cross-sectional form of data collection to elicit information from the Nigerian banking sector.

This study employed quantitative method of data collection. It involves the use of survey questionnaires. The justification for the choice of quantitative approach is supported by researchers such as Sekaran and Bougie (2009, 2010, and 2011) and De Vaus (2011), who pointed out that quantitative research, is the most suitable approach of examining

persons' opinion as the reason behind their motive for any action, behavior and attitude. In addition, Alex (2010) argued that quantitative research design is the best methodological approach to employ in a descriptive research that tends to examine social theoretical notions in a practical concept. Using survey questionnaires helps researchers to make a deduction and then extrapolate it to a large population (De Vaus, 2011; Domínguez, 2009; Emeka, 2009; Ehikamenor, 2009; Silverman, 2000).

3.5 Research Equation

John (2008) defined research equation in regression statistical techniques as a means of describing the relationship between two or more predictors and criterion. Research equation could as well be achieved when employing the regression line that represents X-Y coordinates as best fits, where Y stands for the criterion (dependent variable) and X stands for predictors (independent variables). Based on the discussion above, the relationship between the Y and X is hereby defined:

$$Y = \alpha + \beta X$$

Where α is the value of the Y intercept

β is the regression coefficient defined by the gradient

Y signifies the predicted value of the dependent variable and

X signifies the predicted value of the independent variable.

It is imperative for multiple regressions to depict the relationship between one variable known as the dependent variable (Y) and several independent variables (X1, X2, X3, X4...Xn) where n represents the number of variables that are involved. Thus, multiple

independent variables are concurrently used to predict the criterion (dependent variable) with the mathematical expression as the followings:

$$Y = \alpha + \beta X_1 + \beta X_2 + \beta X_3 + \beta X_4 + \dots + \beta X_n.$$

However, the predictive value of each predictor will be assessed using coefficient of the each of the predictors and any coefficient value that is zero indicates small effect on Y (criterion or dependent variable). For any given value, the coefficient b permits the prediction of the resulting change in Y. The following research variables are as follows:

$$\Delta OP \epsilon = \alpha + \beta PTA + \beta ISI + \beta ISS + \beta PGRR + \beta SO + \beta ISA + \beta PTP + \beta PISRTV + \beta ISPP + \beta PTMSC + \beta MOE + \beta PJRR + \beta ISC + \epsilon$$

Where

OP = Organizational Performance

ISC= Information Security Culture

PTA=Perceived Technology Advancement

ISI = Information Security In-sourcing

ISS = International Security Standard

PGRR= Perceived Government Rules & Regulation

SO = Size of the Organization

ISA= Information Security Awareness

PTP= Perceived Training Programs

PISRTV=Perceived Information Security Risk, Threat and Vulnerability

ISPP= Information Security Policy and Procedure

PTMSC= Perceived Management Support and Commitment

MOE= Motivation of Employees

PJRR= Perceived Job Roles and responsibilities.

3.5.1 Simple Regression Analysis

Where one independent variable is hypothesized to affect the dependent variable, the summative effect is equal to both direct and indirect effects (Sekaran & Bougie, 2010; Fritz & Mackinno, 2007). Thus, the equation is as follows:

$$Y = a_1 + bx + \epsilon_1 \dots \dots \dots (1)$$

$$Y = a_2 + b^1x + \epsilon_2 \dots \dots \dots (2)$$

$$Y = a_3 + ax + \epsilon_3 \dots \dots \dots (3)$$

Where

ϵ represents errors in prediction between estimated Y and actual Y

β represents the effect of M on Y adjusted for X

b represents the estimated total effect of X on Y

a represents the estimated effect of X on M

3.5.2 Multiple Regression Analysis

Multiple regressions analysis is necessary where there are more independent variables because it is an avenue to evaluate the relationship between dependent and independent variables (Sekaran & Bougie, 2010). Thus, Fritz and Mackinnon (2007) regression coefficients are employed in this study as follows:

$$Y = a_1 + bx_1 + bx_1 + bx_2 + bx_3 + bx_n \dots \dots \dots (1)$$

$$Y = a_2 + b1x_1 + bx_1 + bx_2 + bx_3 + bx_n \dots \dots \dots (2)$$

$$M = a_3 + ax_1 + ax_2 + ax_3 + ax_n \dots \dots \dots (3)$$

3.5.2.1 Direct Relationship Equation 1

$$OP(Y) = a_1 + PTA(bx_1) + ISI(bx_2) + SO(bx_3) + ISA(bx_4) + ISPP(bx_5) + PTP(bx_6) + PSRTV(bx_7) + MOE(bx_8) + PMSC(bx_9) + PJRR(bx_{10}) + ISS(bx_{11}) + PGRR(bx_{12})$$

Where

OP = Organizational Performance (Y)

ISC= Information Security Culture (MV)

PTA=Perceived Technology Advancement (bx₁)

ISI = Information Security In-sourcing(bx₂)

SO = Size of the Organization(bx₃)

ISA= Information Security Awareness(bx₄)

PTP= Perceived Training Programs(bx₅)

PISRTV=Perceived Information Security Risk, Threat and Vulnerability(bx₆)

ISPP= Information Security Policy and Procedure(bx₇)

PTMSC= Perceived Management Support and Commitment(bx₈)

MOE= Motivation of Employees(bx₉)

PJRR= Perceived Job Roles and responsibilities (bx₁₀)

ISS = International Security Standard(bx₁₁)

PGRR= Perceived Government Rules & Regulation(bx₁₂)

3.5.2.2 Indirect Relationship Equation 2

$$ISC(M) = a_3 + PTA(ax_1) + ISI(ax_2) + SO(ax_3) + ISA(ax_4) + ISPP(ax_5) + PTP(ax_6) + PSRTV(ax_7) + MOE(ax_8) + PMSC(ax_9) + PJRR(ax_{10}) + ISS(ax_{11}) + PGRR(ax_{12})$$

Where

b The effect of Perceived Technology Advancement, International Security Standard, Information Security In-Sourcing, Perceived Government Rules and Regulation, Size of

Organization, Information Security Awareness, Perceived Training Programs, Perceived Information Security Risk Threat and Vulnerability, Information Security Policy and Procedure, Perceived Management Support and Commitment, Motivation of Employee, Perceived Job Rules and Roles on Organizational Performance.

b_1 The estimated direct effect of Perceived Technology Advancement, International Security Standard, Information Security In-Sourcing, Perceived Government Rules and Regulation, Size of Organization, Information Security Awareness, Perceived Training Programs, Perceived Information Security Risk Threat and Vulnerability, Information Security Policy and Procedure, Perceived Management Support and Commitment, Motivation of Employee, Perceived Job Rules and Roles on Organizational Performance adjusted for Information Security Culture.

a The estimated effect of Perceived Technology Advancement, International Security Standard, Information Security In-Sourcing, Perceived Government Rules and Regulation, Size of Organization, Information Security Awareness, Perceived Training Programs, Information Security Risk Threat and Vulnerability, Information Security Policy and Procedure, Perceive Top Management Support and Commitment, Motivation of Employee, Perceive Job Rules and Regulations and Information Security Culture

β represents the estimated effect of Information Security Culture

a_1, a_2, a_3 represents the intercept.

3.6 Population and Sample

3.6.1 Population

The Nigerian commercial banks are the population of the study. Nigeria has 24 consolidated commercial banks with 5,407 branches spread across the federation. Table 3.3 below shows the 24 consolidated commercial banks in arranging order.

Table 3.4
Total Number of Nigerian Banks

| | | |
|---------------------------------|-------------------------------------|--|
| 1. Access Bank Nig. Ltd | 9. Fin Bank Plc | 17. First Bank Nigeria Plc |
| 2. Keystone (Afri Bank). | 10. Zenith Bank Plc. | 18. Sterling Bank Nig. Ltd |
| 3. Bank PHB(Platinum Habib Bank | 11. First City Monumental Bank Plc. | 19. Oceanic Bank International Nigeria Plc |
| 4. Spring Bank Nig. Ltd | 12. Unity Bank of Nig. Ltd | 20. Intercontinental Bank Plc |
| 5. Stanbic IBTC Bank Ltd | 13. Skye Bank | 21. Guaranty Trust Bank Plc |
| 6. Diamond Bank Plc | 14. Equitorial Trust Bank Ltd | 22. Enterprise Bank Plc |
| 7. Ecobank Nigeria Plc | 15. Fidelity Bank Plc | 23. Nigeria International Bank |
| 8. Union Bank of Nig. Ltd | 16. Wema Bank Plc | 24. Guarantee Trust Bank Plc |

Source: Central Bank of Nigeria, 2010

3.6.2 Sample of the Study

A sample is a subset of the entire population that is chosen for a course of study (Sekaran, 2011, 2010, 2009; Hau & Marsh, 2004; Cavana et al., 2001; Krejcie & Morgan, 1970).

Previous researchers have employed the survey to generalize their findings drawn from a

sample from the population within an acceptable perimeter of a given random error (Sekaran & Bougie, 2010; Fritz & Mackinnon, 2007; Cavana et al., 2001).

However, Bartlett, Kotrlik and Higgins (2001) provided a formula and table for determining the sample size based on Cochran's (1977) formula (see Appendix B-3, Table 3.4). For a population size of 1,000 and Alpha level is 0.005, the sample size for a continuous data is 106. Hair et al. (2010) provided a rule of thumb to determine the sample size. 15 respondents for each variable to be estimated in the model are adequate to achieve normality because large samples of 1,000 or more make the statistical significance test sensitive.

In multivariate analysis, the sample size should be 10 times larger as the number of variables in the study. In a case where samples are to be divided into sub-samples, for instance, minimum sample size of thirty for each category is required. Their sample size determination is based on Roscoe (1975) rule of thumb (see Appendix B, Table 3.5).

In addition, Gay and Diehl (1996) postulated that in descriptive research, the sample size of 10% of the population is regarded as a minimum while 20% can be used for sample. However, Sekaran, (2011; 2010; 2009) argued that sample size between thirty and five hundred should be sufficient. It depends on the sampling design and research question that is being investigated. This study adopted Isreal (1992) and on Yamane (1967) formula as follows:

$$n = \frac{N}{1 + N(e)^2}$$

Where:

n = required sample size.

N = population size

E = error margin

With a population of 5407 bank branches made of the 24 consolidated commercial banks and the error margin of 0.05, the sample size hence will be:

$$n = \frac{5407}{1 + 5407(0.05)^2}$$

$$n = \frac{5407}{1 + 5407(0.0025)}$$

$$n = \frac{5407}{13.52}$$

$$n = 399.92$$

By and large, the sample size for this study was 399.92. This is appropriate because the minimum requirement is 100. Five hundred (500) questionnaires were sent out to the consolidated commercial banks in Nigeria to get a high response rate (refer to Table 5.1), 328 were returned giving 65.6% response rate. The filled questionnaires were further trimmed down to 204 during the treatment of data screening using Mahalanobis for detecting outliers. Hence, 204 were finally used for this study.

Since there are only 24 commercial banks in Nigeria, the researcher finds it easy to administer the instrument in the commercial banks across the country. Therefore, the sample of this study equals the population of the study. Thus, the sample of the study is same as the population of the study.

3.6.3 Sampling Framework

The sampling frame is the list of the entire element in the population where the sample is drawn. Therefore, the sample frame in this study is one hundred (100) branches of the 5,407 branches of the commercial banks in Nigeria (Creswell, 2012). This is to enable the researcher to examine the determinant of information security practices on information security culture towards achieving organizational performance in the banking sector. This study employs the use of non-random probability sampling technique. Five (5) questionnaires were administered on each branch and four (4) branches of each consolidated commercial bank were selected on proportionate basis. In all, five hundred (500) questionnaires were administered to get high response rate, representing 100%. Three hundred and twenty eight (328) questionnaires were returned, implying that the response rate is given as 65.6%. Data was collected through self-administered questionnaires from the branches of the Nigerian consolidated commercial banks in Nigeria. Table 3.5 below illustrates the proportionate distribution of the questionnaires to the consolidated commercial banks in Nigeria.

Table 3.5

Distribution of Questionnaires using Non-Probability Sampling

| No | Banks | Questionnaire Distributed | Percentage % |
|----|--|---------------------------|--------------|
| 1 | Access Bank Nig. Ltd | 20 | 4% |
| 2 | Keystone (Afri Bank). | 20 | 4% |
| 3 | Bank PHB(Platinum Habib Bank | 20 | 4% |
| 4 | EcoBank Nig. Ltd | 20 | 4% |
| 5 | Fidelity bank | 20 | 4% |
| 6 | Sterling Bank Nig. Ltd | 20 | 4% |
| 7 | Oceanic Bank International Nigeria Plc | 20 | 4% |
| 8 | Union Bank of Nigeria | 20 | 4% |
| 9 | Fin Bank Plc | 20 | 4% |
| 10 | Diamond Bank | 20 | 4% |
| 11 | First City Monument Nig, Plc | 20 | 4% |
| 12 | Unity Bank of Nig. Ltd | 20 | 4% |
| 13 | Guaranty Trust Bank Plc | 20 | 4% |
| 14 | Enterprise Bank Plc | 20 | 4% |
| 15 | Standard Chartered Bank Plc | 20 | 4% |
| 16 | Savanah Bank Plc. | 20 | 4% |
| 17 | Skye Bank | 20 | 4% |
| 18 | Equitorial Trust Bank | 20 | 4% |
| 19 | Spring Bank Nig. Ltd | 20 | 4% |
| 20 | Stanbic IBTC Bank Ltd | 20 | 4% |
| 21 | Wema Bank | 25 | 5% |
| 22 | Zenith Bank | 25 | 5% |
| 23 | Intercontinental Bank | 25 | 5% |
| 24 | First Bank Nigeria plc | 25 | 5% |
| | Total | 500 | 100% |

However, in each of the banks, copies of the questionnaires were distributed to the top, middle and lower managers (chief information officer, chief information security officer) to elicit information relating to information security culture towards organizational performance. The involvement of the top managers will make the research more feasible

because they are the brain behind practices in terms of policy decision making, commitment to strategic planning, training and others in the organization.

3.6.3.1 Unit of Analysis

According to Sekaran and Bougie (2010), unit of analysis is defined as the overall data collected during data collection processes. In this study, the prominence is on establishing information security culture among bank's employees that will foster organizational performance. Thus, organization was the unit of analysis.

3.7 Research Activities

The researcher in this section recognizes the research activities which include the research instrument development, primary data collection and data techniques. The discussions about research activities are provided in subsections 3.7.1 – 3.7.3 below.

3.7.1 Research Instrument Development

A survey questionnaire is a data collection technique, which is an efficient mechanism when researchers know exactly what is required and how to measure variables of interest. Questionnaires can be administered personally, mailed to the respondents, or electronically distributed; each method of communication has its advantages and disadvantages with respect to ease, reach, time, cost, response rate and computer literacy (Sekaran & Bougie, 2011; 2010; 2009). The most widely used of data survey technique is a questionnaire (DeVaus, 2011; Ismail, 2007; DeVaus, 1986).

This study adapted questionnaires because developing a new questionnaire need to be validated through reliability test to confirm the reliability of the measures (Straub et al., 2004). Thus, factor analysis was used because most of the questionnaires were adapted from different sources (Sekaran & Bougie, 2011, 2010 2009; Hair et al., 2010). Survey questionnaires are widely used by researchers, especially researchers in information security (DeVaus, 2011; 1986; Ismail, 2007; Straub et al., 2004; Zakaria, 2004; De Vaus, 1986). This study makes use of a questionnaire survey. It consists of the demographic information, open ended questions and the five Likert scales to get a response from the levels of management within the banking hall. An in-depth discussion on instrument development is offered in chapter 4.

3.7.2 Data Collection

The primary data were collected through questionnaire survey from the practitioners in the Nigerian commercial banking sector. This process was considered suitable because it allows the researcher to have a personal encounter with the respondents in order to explain the motive of the research study and research instruments (Sekaran and Bougie, 2011, 2010; 2009; Ismail, 2007; Straub et al., 2004; Ismail, 2004; De Vaus, 1986).

By and large, the data collection process started from where the researcher obtained a letter of introduction from Othman Yeop Abdullah Graduate School of Business. The letter of introduction was addressed to the managers of the Nigerian Banks. Data were collected through personal distribution and retrieval from the respondents. The data

collection process involved the researcher visiting the banks to distribute the questionnaires. Though the bank employees have tight schedules, the researcher was able to complete the distribution of the questionnaires. Most of the practitioners of Nigerian banks exhibited cooperation in completing the questionnaires on time after several visits while others required much more visitation.

3.7.3 Data Analysis Techniques

As it has been discussed in section 3.7.2 above, data were collected with the use of a designed questionnaire with mapped procedures. This procedure involves a questionnaire designed using 5 point Likert scale of strongly disagree, disagree, neutral, agree and strongly agree. It contained a classified and categorized items.

The instrument is tested through validity and reliability test because conducting a pilot test among few selected practitioners in the banking sector in Nigeria. Data analysis cannot be considered accurate without going through the processes of descriptive analysis, factor analysis, test of differences, correlation analysis and multiple regressions analysis in order to achieve the objectives of the study.

3.7.3.1 Test for Difference

This study employed non-response bias to test the differences between early response and late response to ensure that no response bias was involved (Coakes & Ong, 2011).

3.7.3.2 Descriptive Statistics

The purpose of descriptive statistics is to provide the demographic information of the respondents. Pallant (2007) argued that descriptive statistics enable a researcher to verify if there is any violation to statistical tools used and deal with the research questions in the research. This research employed variation statistics namely means, standard deviation, frequencies, percentages and useful charts to depict the respondent's response to organizational performance in Nigeria.

3.7.3.3 Factor Analysis

Factor analysis is defined as statistical tools employed to decrease a large component of items into nearest minimum level (Hair et al., 2010 & 2007). Basically, there are two major types of factor analysis: confirmatory factor analysis and exploratory factor analysis. The items of the construct were offered to EFA using Special Package for Social Science (SPSS18). The used of SPSS version 18, was to facilitate the calculation of statistical tools such as descriptive statistics, Cronbach's alpha, analysis of variance (ANOVA), exploratory factor analysis and hierarchical multiple regression (Selamat et al., 2008; Dwivedi, 2007).

Factor analysis was then used because most of the questionnaires were adapted from different sources (Sekaran & Bougie, 2011, 2010, 2009; Hair et al., 2010). This analysis was carried out to examine the fitness of each construct for factor analysis using Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO), Bartlett's Test of Sphericity (BTS). The factors extracted were further verified to know whether the values of

communality, anti image values, correlation coefficient, Eigenvalues and total variance met the required minimum value of factor analysis. Also, rotation was employed using Varimax in order to explain the best simplified form to be attained (Hair et al., 2012, 2011, 2010).

In overall, it is crucial to note that this study clearly followed the rule of thumb of (Coakes & Ong, 2011; Hair et al., 2011, 2010; Pallant, 2007; Meyers et al., 2006) in evaluating the result of EFA (KMO $< .5$, factor loading ± 0.3 to 0.4 , total variance cumulative should be $.60$ and above).

3.7.3.4 Correlation Analysis

To measure the linear relationship between multiple independent and dependent variables, correlation analysis was used in this study (Meyer, et al., 2006). The purpose of correlation analysis is to maximize the inter-correlation between the low-dimensional projections of the two sets of variables and to explore a linear combination of one set of variables and different linear composite of another set of variables that will constitute a maximal correlation (Hair et al., 2011, 2010).

The rule of thumb of Meyer (2006) was employed to illustrate the interpretation of the strength of the relationship between the variables. In this study, 1%,5% and 10% were employed to ascertain the significance level at 1%,5% and 10% ($p < 0.01$, $p < 0.05$, $P < .10$) and the correlation of (± 0.5 , ± 0.3 & ± 0.1) is assumed to be large, moderate and small.

Lastly, the hierarchical multiple regressions were used to measure the relationship between the independent variables, dependent and mediating variables. If it is statistically significant, such model is considered significantly mediated (Hair et al., 2011; 2010; Baron & Kenny, 1986). This study considered in regards to mediator that (1) TOE factors (IV) statistically significantly related to organizational performance (DV), (2) TOE factors is significantly related to information security culture (MV), (3) when TOE factors and information security culture is regressed against organizational performance, information security culture is significant (Ramayah, 2011; Baron & Kenny, 1986), and (4) In view of the fact from third steps mentioned above, if the beta value of TOE factors decreases / increases, if it is still significant hence, partial mediation/full mediation occurs such model is considered significantly mediated (Hair et al., 2011, 2010; Baron and Kenny, 1986).

3.7.3.5 Multiple Regression Analysis

Multiple regression analysis is one of the most widely used techniques in the analysis of data in social sciences (Bryman & Cramer, 2001). The technique can be used to examine

the relationship between a single dependent variable and several independent variables (Hair et al., 2011, 2010; Tabachnick & Fidell, 2001). The ability of the researcher to identify the dimension of variables in the relationship of empirical research is of great value in data analysis (Hair et al; 2011, 2010). That was the reason why the study used factor analysis under extraction method of the principal component factoring with rotation method of Varimax and Kaiser Normalization to analyze organizational performance, technological, organizational and environmental factors as well as information security culture (Coakes & Ong, 2011). Thus, the subsequent reliability analysis of each of the variables was computed.

Additionally, the objective of the analysis was to predict the changes in the dependent variable in response to changes in the independent variables, whereby each independent variable is weighted by the regression analysis procedure to ensure maximal prediction from the set of independent variables (Hair et al., 2011, 2010). To ascertain the reliability of the measurement scales and to check the degree at which the items that make up the scale coherent or make sense, because Cronbach's alpha is normally used to estimate reliability in a given situation (Cortina, 1993; Santos, 1999). Hence, it was used in this study. The most common measurement used in measuring internal consistency is coefficient alpha (Cohen et al; 2003; Santos, 1999; Cronbach, 1951). Therefore, Cronbach's alpha checks the internal consistency reliability or average correlation of scales (Santos, 1999). It checks whether the items that make up the scale actually measure the same underlying construct (Pallant, 2007).

For a scale to be reliable, its Cronbach's alpha value should be above .7 (Pallant, 2001; George & Mallery, 2003). Although, Hair et al (2010, 2011) argued that conventional guideline suggested alpha of .6, and that too much restriction on alpha makes its power to decrease. Thus, a researcher must reconsider an alpha level so that an appropriate choice of the level of alpha level could be made. Also, the following rules of thumb were proposed by George & Mallery (2003) on Cronbach's alpha value as thus: "> .9 – Excellent, > .8 – Good, > .7 – Acceptable, > .6 – Questionable, > .5 – Poor, and < .5 – Unacceptable". Thus, this study employs alpha level of .7 as an acceptable value.

3.8 Operational Definitions of Crucial Variables

The terms such as organizational performance, perceived technology advancement, information security In-sourcing, international security standard, perceived government rules and regulations, the size of the organization, information security awareness, information security policy and procedure, and perceived information security risks, threat and vulnerability, perceived top management support and commitment, motivation of employees, perceived job roles and responsibilities, and information security culture are used in the study. In this study, the independent variables are information security practices while the dependent variable is the organizational performance. The information security practices and dependent variable are mediated by information security culture. Therefore, the following terms are defined in the context of this study.

3.8.1 Organizational Performance

Governance in many banks failed due to the non-challant attitude of the board of directors. The board is often being misled by executive management. They are participating in obtaining unsecured loans at the expense of depositors and not having the qualifications to enforce good corporate governance on bank management (half year report by Nigerian Capital market, 2013; Martins and Odunfa, 2012; 2009).

The banking sector crisis that hinders the growth of the financial stability had been linked to major failures in corporate governance; information security governance, lack of adequate information security culture, lack of investor and consumers' sophistication; inadequate disclosure and transparency about the financial position of banks; critical gaps in the regulatory framework and regulations; uneven supervision and enforcement and information technology gap also contributed immensely.

3.8.2 Perceived Technology Advancement

The ability of an organization to cope with the advent of technology lies on how to use computer in order to gain competitive advantage. Perceived technology advancement is assumed to assist the management of information security for efficient performance.

3.8.3 Information Security In-sourcing

Information in-sourcing is considered when organizations look beyond their usual precincts to outsource their information technology activities in order to achieve improvements in global markets (McIvor et al., 2009, Lankford & Parsa, 1999; McIvor et

al., 2009; Franceschini et al., 2003). It is an avenue where organization turns to experts for information security needs (Wood, 2008). The organization with high level of international connection will consider the changes in the international environment to develop approaches that will enable them to respond appropriately (Farell, 2010). In-sourcing reduces costs and gives an edge to gain competitive advantage.

3.8.4 International Security Standard

The managers of information system are to comply with the stipulated requirements in ISO 27001- 2005 guidelines to the management of information technology security, General Accepted Information Security Principles (GAAP) and the code of practice for information security management (BS 7799; Solms, 1998; Wood, 2008). ISO 27001 requirements reduce the threat of successful information security and inspire confidence in investors and users (Akinsuyi, 2009).

3.8.5 Perceived Government Rules and Regulations

Organizations are situated within a society, underlying its own regulations and norms. The governing board in this society needs to be strictly adhered to.

3.8.6 Size of the Organization

Size of organization is defined as the extent to which organization is encompassed in terms of resources (Govindarajulu, 2006; Kuan & Chau, 2001), knowing for sure that effective information security will involve huge capital. Hence, organization with limited

resources may be hindered in carrying out their operational activities in establishing security culture. Chang and Ho (2006), Zhu et al. (2005) and Thong (1999) argued that big organizations have the potential of effectively establish information security culture compare with the SMEs.

3.8.7 Information Security Awareness

The objective of information security is risk reduction. When information security awareness is efficient and effective, organizational information loss will reduce (Parker, 2002). Scholars on information security management and culture such as Dominguez (2007), Zakaria (2007), Peltier (2005) and Von Solm (2000) defined security awareness as activities that create the employees' sensitivity to the threat and vulnerabilities of the system and the recognition of the need to protect data, information and the means of processing them. Also, the Computer Security Act of 1987 stated that federal agencies are required by law to provide security awareness to all end users of information system. Thus, the need of employee security awareness is based on the fact that securities incidents are caused by the insiders are on the increase (Zakaria, 2007; Briteny, 2001; Von Solms, 2000).

3.8.8 Information Security Policy and Procedure

Information security policy and procedure is an important instrument used in establishing information security culture and implementing information security activities (Hone & Eloff, 2002). It stipulates the policies, procedures and structure to be followed in the organization.

3.8.9 Perceived Information Security Risks, Threats and Vulnerability

Risks are associated with the organizations in this era of computer age. Hence, the organization will like to gain more competitive advantage over their counterparts through the use of IT. Thus, the tendency of security threat and unwanted security incidents are about to occur (Kankanhalli, Teo, Tan & Wei, 2003; Von Solms, 1999). In other words, the organizations are prone to risks.

Industry at its individual level inherits different levels of risk and threat due to its operational activities, hence, the need to safeguard information assets. Financial organization is more capable of managing threats as at when due. Kankanhalli et al. (2003) argued that some industry sectors such as financial organizations are more concerned with information security; hence they go the extra mile with information security culture practices. When there is a lack of information security activities cautions, it will have an adverse effect on organizational performance if not properly handled.

The information security threat is an intruder to the smooth running of an information system. It can take various forms such as interruption, interception, modification and fabrication (Pfleeger, 1989). The information security threat is divided into four categories, attack through email, spam associated threats, malware and phishing.

3.8.10 Perceived Training Programs

The Organizational Economic Committee Development provides guidelines for the security of information system (OECD Guideline, 2005). It stipulates that: “Towards a culture of security underlines the need for a greater awareness and understanding of security issues and practices to develop a common background among citizens, particularly information communication technology practitioners”. Therefore, perceived training programs are the prerequisite for the security development process and a well organized training program will increase security awareness and the acquired understanding will lead to greater participation in security activities (Qingxiong, Schmidt, Herberger & Pearson, 2009).

3.8.11 Motivation of Employees

Organization in whose priority is security need to recognize the motivation of employees in their security programs (Parker, 2002). Employees could be motivated through benefits, rewards and remuneration in the form of bonuses, incentives, promotion, and satisfaction with conducive working environment. They increase growth and organizational performance (Mozina, 2002; Rosenbloom & Hillman, 1991; Miskell & Miskell, 1991; Maslow, 1997).

3.8.12 Perceived Top Management Support and Commitment

Perceived management support and commitment is defined as the commitment and support given by the top management to its organizational programs in protecting information security assets of the organization. Perceived top management support and

commitment has been found to be responsible in initiating awareness and training programs (Domínguez, 2009). The subordinate will always emulate their leaders; hence leaders who live by example give room for other employees within the organization to follow their steps (Abu-Zineh, 2006).

3.8.13 Perceived Job Roles and Responsibilities

Job allocation or division of labor is defined as the manner of how the responsibilities and roles of information security are performed by the employees within the organization (Toval et al., 2002). The allocation of job responsibilities clarify information security tasks for every employee which could be considered as factor in measuring information security culture and organizational performance success (Bjorck, 2001; Sami Abu-Zineh, 2006).

3.8.14 Information Security Culture

Generally, culture is defined as norms, beliefs that guide against the behavior of employees by stipulating what employees need to do within the organization (Schein, 2009). The issue of information security is increasingly important (Brook et al, 2002; Kankanhalli et al, 2003). Organizational culture plays an important role in implementing information security activities as holistic approach (Andress, 2000; Connolly, 2000; Martins & Eloff, 2001). Hence, there is a need for the employees to strictly follow the procedure, policies otherwise, rewards and punishments may be applied. The existence of a mediating effect implies that the relationship between two variables x and y varies as a function of the value of the other variable (Z) refers to as a mediator (Aguinis, 1995;

Zedeck, 1971).

In this study, the third variable employed is information security culture. Thus, information security culture is employed to mediate the relationship between information security activities and organizational performance.

3.9 Summary

The chapter provides how the research objectives are to be achieved using various procedures. The survey questionnaire designed were analyzed using descriptive statistics, correlation analysis, factor analysis, reliability and multiple regressions. Lastly, operational definitions were offered. The next chapter will discuss in details the research instrument development.

CHAPTER FOUR

RESEARCH INSTRUMENT DEVELOPMENT

4.1 Introduction

This section discusses the measurement of the variables through a research instrument found in other previous studies. To have a clear picture of this chapter, the researcher provides the details as follows: (1) questionnaire development; and (2) refinement of the questionnaire.

4.2 Questionnaire Development

A survey questionnaire is a data collection technique, which is an efficient mechanism when researchers know exactly what is required and how to measure variables of interest questionnaires (Creswell, 2012; DeVaus, 2011; Descombe, 2010; Sekaran & Bougie, 2010). Questionnaires can be administered personally, mailed to the respondents, or electronically distributed; each method of communication has its advantages and disadvantages with respect to ease, reach, time, cost, response rate and computer literacy (Sekaran & Bougie, 2003).

The most widely used data survey technique in quantitative research is questionnaires (Creswell, 2012; DeVaus, 2011; Descombe, 2010; Sekaran & Bougie, 2010; Zikmud, 2003; Martin & Eloff, 2001 & Martins, 2000). This study adapted questionnaires. Because developing a new questionnaire will require validation of instrument in which reliability test will be conducted to confirm the reliability of the measures (Straub et al.,

2004). Thus, factor analysis was used because most of the questionnaires are adapted from different sources (Sekaran & Bougie, 2011, 2010; Hair et al., 2011, 2010).

4.2.1 The Organization of the Questionnaire

The questionnaire was structured in accordance with the ideology of Dillman (1978). The idea of Dillman (1978) is that the questionnaire should void of ambiguous, succinctly ordered in a manner that is understandable by the respondents. If these are applied during questionnaire development, it would increase respondents' encouragement and ability to successfully complete the questionnaire. The research questionnaire was divided into three parts. The first part is mainly to obtain demographic information of the respondents. The second part used Likert scale to examine how strongly the respondents agree or disagree with the statement (Martins & Eloff, 2001).

The cross sectional reliability with five Likert scale perceived to be more applicable than the seven Likert scale (Cavana, et al., 2001; Martins & Eloff, 2001; McKelvie, 1978). This part has section A-E which aims to obtain information about technological, organizational, environmental factors, organizational performance, and information security culture while the last part is about the respondents' suggestions and comments. Table 4.6 on page 121 illustrates the summary of the organization of the questionnaire.

4.2.2 Organizational Performance

The element of the organizational performance questionnaire signifies the dependent variable of this research. The questionnaires were adapted from Pallas (2009), Weill & Ross (2004), Solms (2000) and Barafort et al. (2004). Table 4.1 shows the number of organizational performance. items and the sources.

Table 4.1
The Items and Sources Related to Organizational Performance

| D.V. | Items | Sources |
|----------------------------|--------------|---|
| Organizational Performance | 10 | Pallas, 2009; Weill & Ross, 2004; Von Solms, 2000; Barafort et al., 2004 |

4.2.3 Technological Factors

This section of the questionnaire was intended to obtain information on the perceived technology advancement and information security In-sourcing regarding organizational performance. Table 4.2 below provides variables such as perceived technology advancement and information security in-sourcing, the number of the items and the sources are given in Table 4.2 below:

Table 4.2
The Items and Sources Related to Technological Factors

| I.V. | Variables | Items | Sources |
|-----------------------|------------------|--------------|--|
| Technological Factors | PTA | 6 | Ehikamenor (2006), Akinsuyi (2009) |
| | ISI | 5 | Samadder and Kadiyah (2006); Gonzalez et al. (2010) |

4.2.4 Organizational Factors

The organizational factor was formulated to determine the influence of organizational dimension of the organizational performance. This section consists of ten subsections and the questions were adapted from Chang and Ho (2006), Raymond (1990), Hung, et al. (2005), Kankanhalli et. al. (2003), Alshawaf et al. (2005), Peltier (2005), Dominguez (2007), Hone and Ellof (2003), Briteny (2001), Martins and Eloff (2001), Tenfer (2002), Wright(1998), Straub and Welke (1998), Pfleeger (1989), Mohammed and Suborna (2009), Usamni (2008), Dominguez (2009), Parker (2002), Toval et al. (2002), Bkorck (2001), Abu Zinab (2006), Chang and Ho (2006), Ghobadian and Gullea (1991). Please refer to Table 4.3 for details.

Table 4.3

The Items and Sources Related to Organizational Factors

| Variables | Items | Sources |
|---|--------------|--|
| Size of organization | 5 | Hang and Ho (2006), Raymaond (1990), Hung et al. (2005), Kankanhalli et al. (2003), Alshawaf et al. (2005), Ghobadian and Gallea (1997). |
| Information Security Awareness | 6 | Peltier, 2005; Abu-zineh, (2006),Dominguez (2007), |
| Information Security Policy and Procedures | 7 | Hone and Ellof (2003) |
| Perceived Training Programs | 9 | Abu-zineh, (2006),Briteny (2001), Tenfer (2002), Wright (1998). |
| Perceived Information Security Risks, Threats and Vulnerability | 10 | Straub and Welke, 1998, Pfleeger (1989), Usamni (2008), Mohammed and Suborna (2009). |
| Perceived Top Management Support and Commitment. | 5 | Abu-zineh,(2006), Dominguez (2007) |
| Motivation of Employees | 9 | Abu-zineh,(2006), Parker (2002) |
| Perceived Job Roles and Responsibilities. | 6 | Toval et al., (2002), Bkorck (2001), Sami Abu Zineh (2006) |

4.2.5 Environmental Factors

Table 4.4 below illustrates the number of dimensions of environmental factors. Environmental factors have two dimensions (international security standard and government rules and regulations) of which organizational performance is determined. The international security standard has five items and government rules and regulations have three items to measure organizational performance. The sources of the items are illustrated in Table 4.4.

Table 4.4

The Items and Sources Related to Environmental Factors

| Independent Variables | Items | Sources |
|--|--------------|-----------------|
| International Security Standards | 5 | Omu (2010) |
| Perceived Government Rules & Regulations | 3 | Akinsuyi (2009) |

4.2.6 Information Security Culture

This is the last section of part 2. It was designed to measure information security culture. The researcher intended to examine the mediating effects of information security culture between all the dimensions of information security activities and organizational performance. Table 4.5 shows the number of items and their sources

Table 4.5

The Items and Sources Related to Information Security Culture

| Moderating Variables | Items | Sources |
|------------------------------|--------------|---|
| Information Security Culture | 10 | Zakaria, (2013; 2007) Chaula (2006), Schein (1999), Lindley and Walker (1993), Connar (2008), Robbins (2005), Martins and Eloff (2001). |

From the Table 4.6, the study employed two parts of scale in the questionnaire. Part 1 was on the demographic information of the respondent profile. The second part of the questionnaire has section A- N. Mckelvie (1978) opined that cross sectional reliability is much greater when Likert scale is employed rather than using seven Likert scale. The researcher therefore employed the use of five Likert scale to investigate how strongly the respondents disagree or agree with the items of the questionnaire in Part 2. According to Martins and Eloff (2001), Likert scale unfolds how best the respondents enable the researcher to communicate with the respondents in a simpler form. Lastly, Part 3 provides the comments and suggestions from the respondents.

Table 4.6

Summary of Organization of the Questionnaires

| Part | Sections | Content |
|-------------|-----------------|------------------------------|
| 1 | | Demographic Information |
| 2 | A | Technology Factors |
| | B | Organizational Factors |
| | C | Environmental Factors |
| | D | Organizational Performance |
| | E | Information Security Culture |
| 3 | | Comments/ Suggestions |

4.3 Refinement of the Questionnaire

From above, the developed measurement in this study was basically from extant literature. Cavana et al (2001) stated that the amount of pre-questionnaire testing is to redefine the research instrument. This is to ensure that all variables are measured appropriately on one hand, and ambiguity of words for clear understanding is avoided on the other.

To avoid the issue of outrageous, since the questionnaires are adapted from different sources, reliability and validity must be re-assessed and re-checked to avoid ambiguity of words (Pallant, 2007; Straub et al., 2004; Bouger & Fielder, 1995). Thus, before obtaining the main data for this research, there is a need to improve the quality of the data through content validity and pilot test. Such process leads to a valid data in which section 4.3.1 is dedicated to discuss the process in details.

4.3.1 Validity Test

The validity of a data simply means the ability of an instrument to measure what the researcher needed to measure (Neil, 2009). Hence, it is very clear that validity tends to represent the result of the test and not the test itself. The validity authenticates an instrument by measuring what the research intends to measure. Two ways of validating instruments were used in this study. The research instrument in this study was validated through construct validity. The process of validation is to improve the questionnaire that was developed and the researcher ensured that all items have an acceptable Kaiser-

Meyermer-Olkin (KMO) of .7, which is within the range of acceptable value (Sekaran et al., 2000; Muhammad, 2009). In this study, KMO was used to measure the sampling adequacy in order to give room for corrections. The research instrument was later improved upon based on the suggestions of the practitioners in the banking industry in Nigeria.

A second approach to validate this research instrument was content validity. Content validity could be termed as the degree to which instruments are able to explain the meaning of its content (Babbie, 1990). This study investigates the content validity by using extensive literature and practitioners in the Nigerian banking sector. Suggestions and comments of the practitioners in the banking sector serve as an improvement to the questionnaires of this research.

4.3.2 Pilot Test

The importance of a pilot test in research study cannot be overemphasized because it reduces the stress that the researcher could have encountered during the final analysis (Cavana et al., 2001). Therefore, it is very crucial to conduct a pilot study so as to assist the researcher to build a good foundation for the major study. The essence of the pilot study is to assist the researcher to discover problems that will arise from the questionnaires and provide the researcher the opportunities to make corrections and adjustment for the main study (Pallant, 2007; Straub et al., 2004; Bouger & Fielder, 1995).

Pilot study also provides opportunities for the researcher to acquire many experiences before the major study is conducted. For instance, the researcher is equipped on how data are analyzed, and the survey instrument is tested to ensure that the respondents understand the questionnaire and it is within the capacity of the respondents.

4.4 Reliability Test

The internal consistency type of reliability was used in this regard. Cronbach's alpha is an imperative persistent statistics which involve the use of test and formation (Cortina, 1993). Cronbach's alpha coefficient of .7 and above was used as a benchmark of indication of an acceptable Cronbach's alpha (Pallant, 2007; George & Mallery, 2003; Muhammad, 2009).

4.5 Reliability Analyses of Pilot Test

A pilot study was conducted on 30 branches of ten commercial banks in Lagos state to test the validity, direction of the questionnaires and the reliability. The researcher ensured that the responds of the pilot study was a succinct depiction of the main respondents for the study before administering the instrument to them. The respondents' feedback and comments indicated that the questionnaires were understandable and suggestions for rewordings were all noted by the researchers. The results of the pilot test are illustrated in Table 4.7.

Table 4.7
Reliability Analyses of Pilot Test' Result

| Variables | Code | No of items | Cronbach's Alpha |
|---|--------|-------------|------------------|
| Organizational. Performance | OP | 10 | 0.838 |
| Perceived Technology Advancement | PTA | 6 | 0.730 |
| Information Security In-sourcing | ISI | 5 | 0.650 |
| International Security Standards | ISS | 5 | 0.727 |
| Perceived Government Rules and Regulation | PGRR | 3 | 0.802 |
| Size of Organization | SO | 5 | 0.632 |
| Information Security Awareness | ISA | 6 | 0.633 |
| Information Security Policy and procedures | ISPP | 7 | 0.630 |
| Perceived Training and Educational Program | PTP | 9 | 0.805 |
| Perceived Information Security Risks Threat and Vulnerability | PISRTV | 7 | 0.784 |
| Top Management Supports and commitment | PTMSC | 5 | 0.853 |
| Motivation of Employees | MOE | 9 | 0.629 |
| Perceived Job Role and responsibilities | PJRR | 6 | 0.710 |
| Information Security Culture | ISC | 15 | 0.852 |

N=110

4.6 Summary

This chapter discusses the development of research instrument. It highlights on the organization of the questionnaire, refinement of the questionnaire, presentation of the demographic information of the respondents for the pilot test and reliability test results was presented. The data analysis and findings would be discussed in the next chapter.

CHAPTER FIVE

DATA ANALYSIS AND FINDINGS

5.1 Introduction

This chapter presents the discussions of the data analysis and findings obtained from the survey questionnaires. It also presents the whole data and descriptive analysis tools of two hundred and four (204) respondents from the twenty four commercial banks in Nigeria. The structure of the chapter is as follows: the first section is data cleaning, statistical assumptions; factor analysis used to test the construct validity, internal consistency and reliability analysis respectively. The findings from factor analysis, multiple and hierarchical regressions and demographic characteristics are presented. It also highlights the response rate, followed by the demographic profiles of the survey respondents and reliability test of the survey instrument. The findings of the information security culture and organizational performance are discussed in section 5.5.1 – 5.5.9.

5.2 Response Rate

Table 5.1 presents the overall questionnaire sent and the response rate of the received questionnaire.

Table 5.1
Response Rate of the Questionnaire

| Response | Frequency | Response Rate% |
|--|------------------|-----------------------|
| Overall Questionnaire distributed | | 500 |
| Uncompleted/wrongly filled questionnaire | 63 | |
| Usable questionnaire | <u>265</u> | |
| Questionnaire returned | 328 | |
| Questionnaire not -returned | <u>172</u> | |
| Response rate ¹ | | 65.6% |
| Usable response rate ² | | 53.0% |

As the response rate was 65.6%, it is considered to be adequate for data analysis. The following section will discuss non-respondent bias.

5.3 Non Respondent Bias

The non respondent bias is the process of dividing the sample of the respondents into early responses and late responses. In this study, early responses entail sample returned within two weeks of distribution while late responses are the sample returned after two weeks of distribution (Churchhill & Brown, 2004; Malhotra et al., 2006). Scholars posited that relying on participation that is voluntary result in the possibility that respondents and non respondents vary in some ways.

1 Questionnaire return/Questionnaire distributed (328/500)

2 Usable questionnaire /Questionnaire distributed (265/500)

A situation may arise that the non- respondent does not have the same characteristics as the timely respondents (Coakes & Ong, 2011; Matteson, Ivancevich & Smith, 1884; Armstrong & Overton, 1977). Thus, the existing literatures established that, the non-respondents sometimes differ analytically. The previous researchers such as Malhortra, et al. (2006) and Churchill and Brown (2004) argued empirically that, late respondents could be used in place of non-respondents because they would not have responded if they had not been given a thorough followed up.

Also, Malhortra et al. (2006) posited that the non-respondents are assumed to have a similar feature like the late respondents. Thus, to standardize this procedure, this study divided the sample into two (namely: early responses:- those that returned the questionnaires within two weeks after the distribution and late responses - those that returned the questionnaires after two weeks from the date of distribution. Table 5.2 below illustrates the test on non -response bias.

Table 5.2

The Test of Non- Respondents Bias Using Independent Sample T-test

| Variables | Levene's Test | Sig | Sig @ 95% Level |
|---|----------------------|------------|------------------------|
| Organizational Performance | 1.87 | .172 | Not Significant |
| Perceived Technology Advancement | 6.237 | .495 | Not Significant |
| Information Security In-sourcing | .110 | .741 | Not Significant |
| International Standard Security | .913 | .341 | Not Significant |
| Perceived Government Rules and Regulations | 5.559 | .828 | Not Significant |
| Size of the Organization | .048 | .827 | Not Significant |
| Information Security Awareness | 1.163 | .282 | Not Significant |
| Information Security Policy and Procedure | 4.323 | .339 | Not Significant |
| Perceived Training Programs | 4.253 | .240 | Not Significant |
| Perceived Information security risks, threats and vulnerability | .997 | .319 | Not Significant |
| Perceived Management Supports and Commitment | 2.384 | .124 | Not Significant |
| Motivation of Employee | 1.533 | .217 | Not Significant |
| Perceived Job Roles and Responsibilities | 2.579 | .110 | Not Significant |
| Information Security Culture | 1.465 | .227 | Not Significant |

Note: values are not significant

N/S: Not Significant

Based on Table 5.2 above, this study has classified 120 respondents as early responses and 84 respondents as late responses. Both descriptive test and Levene's test for equality of variance were conducted on the demographic and continuous variables. Hence, to test if there is any significant difference in the variables between the early and late response, t-test was examined in the two groups. The results show no significant difference at the level of .05 between the early and late responses (Coakes & Ong, 2011), which indicate that there is no non-response bias in this study.

5.4 Data Cleaning

The first step in data analysis is to check for errors made during the process of inputting data which could serve as a barrier to the researcher (Pallant, 2007). For instance, a researcher might want to input 1 and unknowingly key-in 4 to the system. In order to avoid garbage- in garbage – out, the researcher needs to re-check in order to identify outrageous data which can affect the result of some of the analysis and thereby make a valuable correction. During the data cleaning, the researcher noticed some outrageous data through the descriptive analysis (Pallant, 2007) and corrections were made before proceeding to further analysis. For any data to be perfectly ready for statistical analysis there are assumptions or rule of thumb that must be met (Coakes & Ong, 2010). These assumptions are as follows: (1) treatment of outliers among cases; (2) normality test; (3) multicollinearity test; and (4) homoscedasticity. Subsections 5.4.1-5.4.4 discusses these assumptions in details.

5.4.1 Treatment of Outliers among Cases

Outliers are very sensitive when it comes to the issue of multiple regressions. Hence, Pallant (2007) emphasized the need to check and re-check for outliers before analysis is carried out. Basically, there are approaches to detect outliers. Firstly, it can be done through Mahalanobis, residual plots and histogram. The detection of outliers in this study was through Mahalanobis and chi-square table employed to check for those cases that the Mahalanobis were above 124.32. The total of cases deleted was sixty-one (61), this reduced the number of respondents to two hundred and four (204) and in order to

eradicate outliers totally, the data were transformed and this paves way for meeting one of the assumptions of multiple regression.

5.4.2 Normality Test

The process of normality test availed the researcher to check whether the data is normally distributed. Therefore, it is part of assumption for running regression analysis. This was carried out using 204 respondents. Pallant (2007) argued that any data that is above 140 should be considered to be normal and sample data becomes normal when the sample is large (Jarrett & Kraft, 1989). The Mahalanobis test shows the data were normally distributed. The researcher makes sure that data are void of outliers before further analysis. The process brought up a new series of data which the researcher used to produce a normally distributed data.

Unfortunately, when compared with normal cleaning using Mahalanobis, the transformed data brought about multicollinearity that are non-transformed, hence, the result of data treatment using Mahalanobis was used for this study (Coakes & Ong, 2011; Hair et al., 2006). The researcher plotted the regression standardize residual in order to verify the normality of the data. From the histogram, the plot indicates that the cumulative probability of the organizational performance was succinctly clear. The observed residual is closely around the normal straight line. Hence, the normal P-P plots of other variables equally fulfilled the normality assumption. Figure 5.1 shows the normal P-P plot of regression standard residual.

Normal P-P Plot of Regression Standardized Residual

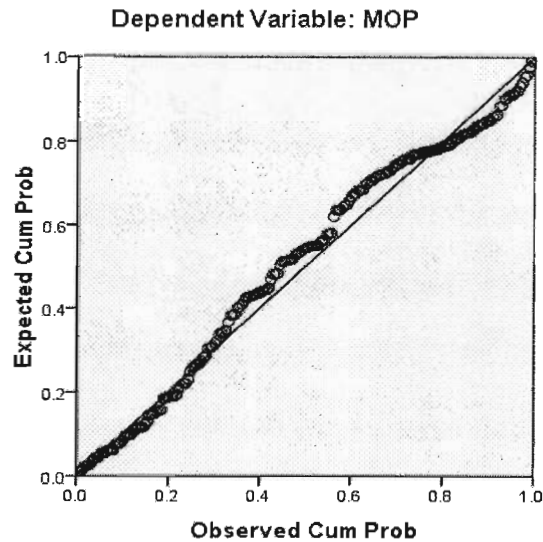


Figure 5.1
Normal P-P Plot of Regression Standardized Residual

5.4.3 Multicollinearity Test

The word multicollinearity could be defined as a measure or a degree of correlation among independent variables (Hair et al., 2010). Thus, multicollinearity test is the step to verify data before proceeding to regression analysis, checking multicollinearity dilemma can be done through bivariate of the independent variables. It is highly correlated when it is above 0.90 among itself (Hair et al., 2010; Muhammad, 2009). Whenever, multicollinearity is present among the variables, it constitutes nuisance by causing increases in the variance of regression and threat to the validity of the regression equation. The value of the Pearson correlation indicates the relationship between the independent variables and also it is a method of checking the multicollinearity (Hair et

al., 2010; Cooper & Schindler, 2003; Allison, 1999). Although, no specific standard for the amount of correlation that could pose as multicollinearity dilemma but previous scholars argued that the correlation of above 0.8 above constitute a problem (Cooper & Schindler, 2003; Allison, 1999). While, Hair et al. (2010) were of the opinion that 0.9 constitute multicollinearity.

In addition, the issue of variance inflated factor (VIF) and tolerance value are well noted in this study which stated that, VIF should not be greater than 10 while tolerance should be lower than .10. Anything contrary to this rule of thumb, then there is a multicollinearity problem (Aiken & West, 1991; Cohen & Cohen, 1983). However, there was no issue as both VIF and tolerance value were within the acceptable range. Hence, the issue of multicollinearity in this study was solved (Ramayah, 2011; Cohen et al., 2003; Aiken & West, 1991; Cohen & Cohen, 1983).

5.4.4 Homoscedasticity

Norusis (1999) posited that there is homoscedasticity phenomenon when the data distribution has no pattern and the residuals are scattered arbitrarily around the horizontal line. Thus, Hair et al. (2010) stated that the assumption of homoscedasticity necessitates that the dependent variable variance should be the same at all levels of all the independent variables of the error term. The rule of thumb is that, the Durbin- Waston value should be between 1.50 and 2.50. The Durbin-Waston could be used to test the independence error term (Norusis, 1999). The 1.770 in this study indicated that it met the

rule of thumb and assume that homoscedasticity of independence is not violated in this study. Having discussed the data cleaning for the study, the next section will discuss demographic information of the respondents.

5.5 Demographic Information of the Respondents

This section discusses the respondents' general information. Particularly, it provides all the respondents' information such as position, marital status, age, level of education attained, experience, number of employees in the bank, the overall number of employees and implementation of information security culture. All these are discussed in subsections 5.5.1-5.5.9.

5.5.1 Position of the Respondents

The targeted respondents were the lower, middle and top management. The researcher wanted to know if all these levels fully participated in the survey. Therefore, the views of the management levels are considered useful in relation to organizational performance.

Table 5.3 below provides the findings. It could be said that the respondents from all levels of management participated in this survey.

Table 5.3

The Respondents Position

| Position | Frequency | Percent |
|-------------------|------------|--------------|
| Managing Director | 9 | 4.4 |
| Top Management | 32 | 15.7 |
| Middle management | 73 | 35.8 |
| Lower Management | 90 | 44.1 |
| Total | 204 | 100.0 |

5.5.2 Gender of the Respondents

The results from Table 5.4 indicate that the majority of the respondents are males at 52.9% while 47.1% represent the female. Al-Gahtani et al. (2007) and Al-deek (2010) argued that the male is dominating the economic activities in the Arab world, which is also through in Africa with specific reference to Nigeria. This is contrary to Asian countries like Malaysia, Thailand, Indonesia and Singapore where both male and female are almost at par.

Table 5.4
The Respondents' Gender

| Gender | Frequency | Percentage % |
|--------------|------------|--------------|
| Male | 108 | 52.9 |
| Female | 96 | 47.1 |
| Total | 204 | 100.0 |

5.5.3 Age of the Respondents

The results show that the majority of the respondents are within the age bracket of 30 – 40 (63.7%), 41-50 was 32.8% and 51-60 represent 3.4%. This is illustrated in the Table 5.5 below.

Table 5.5
Respondents' Age

| Age | Frequency | Percentage% |
|--------------|------------|--------------|
| 30-40 | 130 | 63.7 |
| 41-50 | 67 | 32.8 |
| 51-60 | 7 | 3.4 |
| Total | 204 | 100.0 |

5.5.4 The Marital Status of the Respondents

The findings illustrated in Table 5.6 show that 70.1% of the respondents are married, while 29.9% were still single and searching. It could be said that both single and married participation in this survey enhances the considerable useful information for organizational performance.

Table 5.6
Respondents' Marital Status

| Status | Frequency | Percentage % |
|--------------|------------|--------------|
| Single | 61 | 29.9 |
| Married | 143 | 70.1 |
| Total | 204 | 100.0 |

5.5.5 Level of Education of the Respondents

The survey questionnaires consisted of five levels of educational background according to the Nigerian educational setting. These levels are West African School Certificate/ Senior Secondary Certificate (WAEC/SSCE), Technical College, (others), Ordinary National Diploma/ National certificate in education (OND/NCE), Bachelor of Science/ Higher National Diploma (BSC/ HND), Master of Science, Master of Business Administration (Masters) and Doctor of Philosophy (PhD). Table 5.7 below show that, 118 have first degree (57.8%), 66 have Masters degree (32.4%), 12 have school certificate/ OND (5.9%), 3 have WAEC/SSCE (1.5%), while others was 5 (2.5%). This

implies that the respondents are well educated and understood the items on the questionnaire. Hence, the results are shown in Table 5.7 below.

Table 5.7
Respondents' Level of Education

| Education | Frequency | Percentage % |
|--------------|------------|--------------|
| WAEC/SSCE | 3 | 1.5 |
| OND/NCE | 12 | 5.9 |
| BSC/HND | 118 | 57.8 |
| Masters | 66 | 32.4 |
| Others (PhD) | 5 | 2.5 |
| Total | 204 | 100.0 |

5.5.6 Experience of the Respondents

The majority of the respondents indicated that, they have at least 10 years of working experience (58.8%), 28.4% of the respondents have 11-24 years, while the third group of the respondent (12.7%) have 25 years and above. Kindly refer to Table 5.8 for more details.

Table 5.8
Respondents' Experience

| Experience | Frequency | Percentage% |
|-----------------|------------|--------------|
| 1-10yrs | 120 | 58.8 |
| 11-24yrs | 58 | 28.4 |
| 25yrs and above | 20 | 12.7 |
| Total | 204 | 100.0 |

5.5.7 Number of Employees in the Banks of the Respondents

Table 5.9 shows that 52.2% of the participating banks have 50-100 employees, 28% of the participating banks have 101-200 employees, 41% of the participating banks have 201-300 employees, 13.7% participating banks have 301- 400. The overall number of employees is within the range of 50- 400. This could be said that the majority of the employees of the banks refer to as respondents participated in the survey questionnaire. See Table 5.9 for details.

Table 5.9
Respondents' Number of Employees

| No of Employees | Frequency | Percentage% |
|-----------------|------------|--------------|
| 50-100 | 107 | 52.2 |
| 101-200 | 28 | 13.5 |
| 201-300 | 41 | 20.1 |
| 301-400 | 28 | 13.7 |
| Total | 204 | 100.0 |

5.5.8 Overall Number of the Employees

This section discusses the overall number of the employees. The questionnaires include: between 100-499, 500-999, 1000-1,999 and 2,000 and above. It is very interesting to know that majority of the respondents indicated 2,000 and above for the total number of employees. The result is illustrated in Table 5.10

Table 5.10

Respondents' Overall Number of Employees

| Overall No of Employees | Frequency | Percentage% |
|-------------------------|------------|--------------|
| 100-499 | 44 | 23.6 |
| 500-999 | 31 | 15.2 |
| 1000-1,999 | 70 | 34.3 |
| 2,000 and above | 59 | 28.9 |
| Total | 204 | 100.0 |

5.5.9 The Establishment of the Information Security Culture

The researcher wanted to know about the establishment of the information security culture in the banks. Table 5.11 shows that all the respondents indicated that their banks have information security culture.

Table 5.11

Response on establishment of information security culture

| ISC Establishment | Frequency | Percentage% |
|-------------------|-----------|-------------|
| Yes | 98 | 48 |
| No | 106 | 52 |

Table 5.12 provides the summary of the respondents' profile. Section 5.6 will discuss the goodness of measurement of the primary data collection.

Table 5.12
The Summary of the Respondents Profile

| Items | Min | Max | Frequency | Percentage% |
|-------------------|-----|-----|-----------|-------------|
| Sample | | | 204 | 100% |
| Position | 1 | 4 | | |
| Managing Director | | | 9 | 4.4 |
| Top manager | | | 32 | 15.7 |
| Middle Manager | | | 73 | 35.5 |
| Lower Manager | | | 90 | 44.1 |
| Total | | | 203 | 100 |
| Gender | 1 | 2 | | |
| Male | | | 108 | 52.9 |
| Female | | | 96 | 47.7 |
| Total | | | 204 | 100 |
| Age | 1 | 3 | | |
| 30-40 | | | 130 | 63.7 |
| 41-50 | | | 67 | 32.5 |
| 51-60 | | | 7 | 3.4 |
| Total | | | 204 | 100 |
| Marital Status | 1 | 2 | | |
| Single | | | 61 | 29.9 |
| Married | | | 143 | 70.1 |
| Total | | | 203 | 100 |
| Education | 1 | 5 | | |
| WAEC/SSCE | | | 13 | 6.4 |
| OND/HND | | | 120 | 59.1 |
| Masters | | | 63 | 31.0 |
| Others | | | 3 | 1.5 |
| Total | | | 204 | 100 |

Table 5.12 Continued

| | | | | |
|---|---|---|-----|------|
| Experience | 1 | 3 | | |
| 1-10 | | | 120 | 58.8 |
| 11-24 | | | 58 | 28.4 |
| 25 and above | | | 20 | 12.7 |
| Total | | | 204 | 100 |
| Number of Employees at Branch Level | 1 | 4 | | |
| 50-100 | | | 107 | 52.2 |
| 100-200 | | | 28 | 13.5 |
| 300-400 | | | 41 | 20.1 |
| 400-500 | | | 28 | 13.7 |
| Total | | | 204 | 100 |
| Overall Number of Employees | 1 | 3 | | |
| 100-499 | | | 44 | 21.6 |
| 1000-1,999 | | | 70 | 34.3 |
| 2000 and above | | | 59 | 28.9 |
| Total | | | 204 | 100 |
| Establishment of Information Security Culture | 1 | 2 | 98 | 48 |
| | | | 106 | 53 |
| Total | | | 204 | 100 |

5.6 Goodness of Measure

The measure of goodness and fitness of the research instrument was observed using validity and reliability test. The explanation of the fitness is discussed in Subsections

5.6.1- 5.6.3:

5.6.1 Validity Test

The validity infer to be the degree at which the instrument measured what it needed to be measured because it is very imperative that the measurement employed in the research actually make known the interpretation and meaning of the measurement (Zikmund et al., 2010; Babbie, 1990). As suggested by the previous scholars, this research adapted three types of validity which are: (1) content validity; (2) construct validity; and (3) criterion validity. Content validity refers to the manner in which the instrument unfolds the meaning which was intended to be (Babbie, 1990). On the other hand, construct validity specifies how well the result obtained fit to the theories (Zikmund, 2003). Thus, factor analysis was used in this study. The discussion on this is offered in subsection 5.6.3.

Lastly but not the least is the criterion validity. It refers to a degree at which scales positively correlated with other measures or specified of the same construct (Pallant, 2007). The criterion validity was examined in this study by using Pearson correlation, VIF and Tolerance Value as suggested by previous scholars (Kabiru, 2012; Friedman, Gold, Srivasta & Parkin, 2004; Emery, Crump & Bors, 2003). The discussion on criterion validity will be dealt with in Section 5.9.

5.6.2 Reliability Test

The researchers usually conduct a reliability test in order to check whether each variable is reliable with the sample of the research and the reliability of scale differs depending on the sample of the study (Neil, 2009; Pallant, 2007). Reliability assists in checking the

internal consistency of the measurement by using Cronbach's alpha. This study employed Cronbach's alpha coefficient of .6 and above as a benchmark of indication of an acceptable Cronbach's alpha (Hair et al., 2010; Muhammad, 2009; Pallant, 2007; Cronbach & Richard, 2004; George & Mallery, 2003; Nunnally, 1978; Cronbach, 1951).

5.6.3 Construct Validity Test

The previous scholars argued that factor analysis is used to assess the construct validity of any given test because it helps to reduce a large number of data into smaller new units or variables (Pallant, 2007). Factor analysis attempts to bring inter correlated variables together under one general underlying variable (Pallant, 2007). In other words, its aim is to reduce dimensionality of the original space and to give interpretation to the new space by reducing the number of new dimensions which are supposed to underlie the old ones (Rietveld & Van Hount, 1993). It could be that the variance is explained in the observed variable in terms of underlying factors (Habing, 2003).

Factor analysis was applied in this present study to measure constructs validity and to find out the sets of correlated variables. There are some rules to follow to show whether the data in this study are sufficient or not for factor analysis. First, the greater the value of KMO, the more communal the factors are, and the data would be more suitable for factor analysis (Kaiser, 1974). All the values representing Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO, MSA), Bartlett's Test of Sphericity (BTS), significant level, Total Variance Explained (TVE) and communality were all at acceptable values. Lastly,

factor analysis provides both the possibility of gaining a clear view of the data and using the output in subsequent analysis (Field, 2000; Rietveld & Van Hount, 1993). The next Sections 5.6.3.1 - 5.6.3.5 will illustrate the factor analysis results of dimensions on each construct.

5.6.3.1 Factor Analysis of Organizational Performance

The KMO, MSA and BTS results for organizational performance are illustrated in Table 5.13.

Table 5.13

KMO and Bartlett's Test of OP

| | | |
|--|--------------------|---------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .811 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 486.298 |
| | Df | 21 |
| | Sig. | .000 |

From Table 5.13, it can be seen that the value of KMO, MSA was 0.811 and Bartlett's test of Sphericity agreed with Kaiser (1974). Therefore, KMO, MSA and Bartlett' test of Sphericity were assured and the correlation among variables is suitable for factor analysis. The component values of organizational performance were extracted using latent root criterion, Principal component analysis was used to extract factors and it show cumulative variance of 64.754%. The communality of each item ranges above 0.4 while anti image correlation coefficient of each item was above .7 (see Appendix D-1 for communality result). The result met the criteria set for factor analysis. Hence, construct

validity for the organizational performance may be assumed. The Table 5.14 below illustrates the result.

*Table 5.14: The Extracted Component of Organizational Performance
Total Variance Explained of OP*

| Comp | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
|------|---------------------|----------|---------|-------------------------------------|----------|--------|-----------------------------------|----------|--------|
| | % of | | | % of | | | % of | | |
| | Total | Variance | Cum % | Total | Variance | Cum% | Total | Variance | Cum % |
| 1 | 3.737 | 46.712 | 46.712 | 3.737 | 46.712 | 46.712 | 2.643 | 33.043 | 33.043 |
| 2 | 1.132 | 14.155 | 60.866 | 1.132 | 14.155 | 60.866 | 2.226 | 27.824 | 60.866 |
| 3 | .713 | 8.915 | 69.781 | | | | | | |
| 4 | .693 | 8.667 | 78.449 | | | | | | |
| 5 | .596 | 7.453 | 85.902 | | | | | | |
| 6 | .448 | 5.594 | 91.496 | | | | | | |
| 7 | .385 | 4.817 | 96.312 | | | | | | |
| 8 | .295 | 3.688 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

Also, Table 5.15 below indicates the factor loading on organizational performance using Varimax rotation criterion to reduce the item in a meaningful manner.

Table 5.15

The Factor Loading for Organizational Performance Using Varimax Rotation

| Rotated Component Matrix (a) of Organizational Performance | | |
|--|-----------|------|
| Items | Component | |
| | 1 | 2 |
| OP6 | .877 | |
| OP7 | .834 | |
| OP4 | .640 | |
| OP5 | .627 | |
| OP1 | | .800 |
| OP2 | | .775 |
| OP3 | | .667 |

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

The results of the factor loading as shown in Table 5.15 above illustrate that the factor loading on OP using Varimax rotation criterion to reduce the item was in a meaningful manner. There are two factors loadings that were extracted for OP1 and OP2 but summated values was employed (Kabiru, 2012; Alabede, Arrifin & Idris, 2011; Fauzi, 2010). The practitioners in the banking sector in Nigeria saw the items for measuring organizational performance in a different perspective from the theory and this may be due to different phenomenon and geographical locations. However, the concern in this study is not on the new dimension but organizational performance as a whole. For this reason, factors extracted from the analysis were summated to obtain a total scale. This is consistent with the procedure used in other studies such as Kabiru, (2012), Alabede, Arrifin and Idris (2011), Fauzi (2010), and Elbama and Job (2007). The reliability test of the items of the 2 factors is shown in Table 5.16 and the indication is that the 4 items of

OP1 is 0.795 while 3 items of OP2 is 0.706. It should be noted from the above Table 5.16 that the OP summated value has the acceptable alpha of .822 (Hair et al., 2010; Nunnally, 1978).

Conversely, the study is not interested in each factor as produced by the factor analysis but on the whole scale of organizational performance. Therefore, the result was summated to get the average as it is practiced by Fauzi and Idris, (2009) and Alabede et al. (2011). The summary result is presented in Table 5.16 below:

*Table 5.16
The Summary of the Cronbach's alpha for the Organizational Performance*

| Factor | No of items | Cronbach's Alpha |
|-------------|-------------|------------------|
| OP | 4 | 0.795 |
| OP2 | 3 | 0.706 |
| OP Summated | 7 | 0.822 |

5.6.3.2 Factor Analysis of Technological Factors

As mentioned in Section 5.6.3.1, the same process for underlying dimensions of variables would stand for technological factors which consist of perceived technology advancement and information security In-sourcing. Hence, the KMO, MSA, Bartlett's test of Sphericity, df and significant for both perceive technological advancement and information security outsourcing are shown in Table 5.17a and 5.17b below:

Table 5.17a

KMO and Bartlett's Test of PTA

| | | |
|--|--------------------|---------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .717 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 310.232 |
| | df | 10 |
| | Sig. | .000 |

Table 5.17b

KMO and Bartlett's Test of ISI

| | | |
|--|--------------------|---------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .688 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 170.890 |
| | df | 10 |
| | Sig. | .000 |

From Table 5.17a, it can be seen that KMO, MSA for PTA was 0.717 and Bartlett's test of Sphericity 310.232, df at 10, significant .000, while in Table 5.17b, it can be seen that KMO, MSA for PTA was 0.688 and Bartlett's test of Sphericity 170.890, df at 10, significant .000. In accordance with Kaiser (1974), the results are considered as meritorious. In short, the correlation among variables is suitable for factor analysis. The communality of each item were at accepted values and correlation coefficient of each item was 0.64 (see Appendix D-4 for communality result). The two extracted factors are perceived technological advancement and information in-sourcing. Thus, Table 5.18a and Table 5.18b below shows that the two components of PTA and ISI variables were extracted which explained 55.394% and 64.536% of the cumulative variance respectively.

Table 5.18a
Total Variance Explained of PTA

| Comp | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | |
|------|---------------------|---------------|--------------|-------------------------------------|---------------|--------------|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 2.770 | 55.394 | 55.394 | 2.770 | 55.394 | 55.394 |
| 2 | .738 | 14.758 | 70.152 | | | |
| 3 | .659 | 13.182 | 83.334 | | | |
| 4 | .542 | 10.832 | 94.166 | | | |
| 5 | .292 | 5.834 | 100.000 | | | |

Extraction Method: Principal Component Analysis.

Table 5.18b
Total Variance Explained of ISI

| Comp | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
|------|---------------------|---------------|---------|-------------------------------------|---------------|--------|-----------------------------------|---------------|--------|
| | Total | % of Variance | Cum % | Total | % of Variance | Cum % | Total | % of Variance | Cum % |
| 1 | 2.222 | 44.443 | 44.443 | 2.222 | 44.443 | 44.443 | 1.623 | 32.466 | 32.466 |
| 2 | 1.005 | 20.093 | 64.536 | 1.005 | 20.093 | 64.536 | 1.603 | 32.070 | 64.536 |
| 3 | .761 | 15.211 | 79.747 | | | | | | |
| 4 | .579 | 11.572 | 91.318 | | | | | | |
| 5 | .434 | 8.682 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

The reliability test was then conducted by using the Cronbach's alpha. The results of the reliability test of the items for the 5 and 3 for both PTA and ISI factors are shown in Table 5.19. The indication of the result is that the Cronbach's alpha of 5 items for perceived technology advancement is 0.797 while 3 items of information security In-sourcing is 0.585 and 0.689, since the study is not interested in each factor as produced

by factor analysis, the result were summated to get an average value of 0.680 (Alabede et al. 2011; Fauzi & Idris, 2009). Due to low alpha value of ISI, it was excluded from further analysis. Thus, it enables this study to go for further analysis.

Table 5.19
The Summary of the Reliability Test of Technological Factors

| Technological factors | No of items | Cronbach's' Alpha |
|----------------------------------|--------------------|--------------------------|
| Perceive Technology Advancement | 5 | 0.797 |
| Information Security In-sourcing | 3 | 0.586 |
| Information Security In-sourcing | 2 | 0.689 |
| ISI Summated | 5 | 0.680 |

The Cronbach's alpha value of above .7 is considered acceptable (Nunnally, 1978; Hair et al., 2010). The suitability of the alpha value on perceived technological advancement enables the researcher to proceed to further analysis.

5.6.3.3 Factors Analysis of Organizational Factors

Sections 5.6.3.3.1- 5.6.3.3.8 illustrates the factor analysis conducted as follow:

5.6.3.3.1 Size of the Organization

From the factor analysis conducted, the size of the organization' KMO was 0.594 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 154.597 and significant at .000. The implication of KMO and Bartlett test of Sphericity values

specified that the data collected were suitable. The outcome of the extracted components of organizational factors using latent root criterion is shown in Appendix D-4. It explained 76.033 % of the cumulative variance with Eigenvalues of 9.633. The factor loading was above .8 while the majority of the communalities are above .5

The determination of the number of factors depends on the factor loading. Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained, each of the dimensions of the organizational factors was factorized and result is shown in Appendix D-4. The factor components of the variables are within acceptable range. Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.2 Information Security Awareness

From the factor analysis conducted, information security awareness, KMO was 0.820 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 593,347 and significant at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to organizational factors. Hence, the outcome of the extracted components of organizational factors using latent root criterion is shown in the Appendix D-4. It explained 60.970 % of the cumulative variance with Eigenvalues of 3.837. The factor loading was above .7 while the majority of the communality is above .5.

The determination of the number of factors depends on the factor loading. Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, the result obtained were factorized and result is shown in the appendix (see Appendix D-4). The factor components of the variables are within the acceptable range. Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.3 Information Security Policy and Procedure

From the factor analysis conducted, ISPP's KMO was 0.747 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 284.315 and significant at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to ISPP. The outcome of the extracted components using latent root criterion is shown in the appendix (see Appendix D-4). It explained 64.993 % of the cumulative variance with Eigenvalues of 6.720. The factor loading and the communality is at acceptable values.

The determination of the number of factors depends on the factor loading. Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained, the variable were factorized and result is shown in Appendix D-4. The factor components of the variables are within acceptable range.

Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.4 Perceived Training Programs

From the factor analysis conducted, PTP KMO was 0.822 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 440.918 and significant at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to PTP. The outcome of the extracted components using latent root criterion is shown in the appendix (see Appendix D-4). It explained 63.631 % of the cumulative variance with Eigenvalues of 5.235. The factor loading and the communality is at acceptable values.

The determination of the number of factors depends on the factor loading. Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained, the variable were factorized and result is shown in appendix D-4. The factor components of the variables are within acceptable range. Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.5 Perceived Information Security Threat, Risk and Vulnerabilities

From the factor analysis conducted, PISTRV KMO was 0.794 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 387.827 and significant

at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to PISTRV. Hence, the outcome of the extracted components using latent root criterion is shown in (see Appendix D-4). It explained 67.924 % of the cumulative variance with Eigenvalues of 5.035. The factor loading and the communalities are above .7 and .5 respectively, thus at the acceptable values.

However, the determination of the number of factors depends on the factor loading. Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained were factorized and result is shown in the appendix (see Appendix D-4). The factor components of the variables are within acceptable range. Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.6 Perceived Top Management Support and Commitment

From the factor analysis conducted, PTMSC KMO was 0.804 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 375.950 and significant at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to PTMSC. The outcome of the extracted components using latent root criterion is shown in appendix D-4. It explained 59.612 % of the cumulative variance with Eigenvalues of 6.256. The factor loading and the communality is also at acceptable values.

In addition, the determination of the number of factors depends on the factor loading, Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained, variable were factorized and result is shown in the appendix (see Appendix D-4). The factor components of the variables are within acceptable range. Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.7 Motivation of Employee

From the factor analysis conducted, MOE's KMO was 0.619 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 417.174 and significant at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to MOE. The outcome of the extracted components using latent root criterion is shown in appendix D-4. It explained 67.975 % of the cumulative variance with Eigenvalues of 3.334 with factor loading and the communality at acceptable values.

By and large, the determination of the number of factors depends on the factor loading, Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained were factorized and result is shown in the appendix D-4. The factor components of the variables are above .6 and .4 respectively. Thus, reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

5.6.3.3.8 Perceived Job Roles and Responsibilities

From the factor analysis conducted, the size of the organization' KMO was 0.655 which is good and estimable according to Kaiser (1974). The Bartlett Sphericity was 270.450 and significant at .000. The implication of KMO and Bartlett test of Sphericity values specified that the data collected were suitable with regards to PJRR. Hence, the outcome of the extracted components using latent root criterion, is shown in appendix D-4. It explained 51.449 % of the cumulative variance. The result of factor loading, communality and reliability are shown in (Appendix D-4). The factor loading and the communality are at acceptable values

However, the determination of the number of factors depends on the factor loading, Varimax rotation was used to reduce the items in order to make it more meaningful. Nevertheless, before the result was obtained were factorized and result is shown in the appendix (see Appendix D-4). The factor components of the variables are above .6 and communalities are above .4. This is within the acceptable range. Reliability test was conducted to know the internal consistency of the extracted factors. Table 5.20 illustrates the results for Cronbach's alpha.

Table 5.20

The Summary of Organizational Factors on Reliability Test

| Factors | No. of Items | Cronbach's Alpha |
|---|--------------|------------------|
| Size of the Organization | 4 | 0.680 |
| Information Security Awareness | 6 | 0.870 |
| Information Security Policy and procedure | 6 | 0.710 |
| Perceived Information | | |
| Security Risks, Threats and Vulnerability | 5 | 0.809 |
| Perceived Information | | |
| Security Threat, Risk and vulnerability | 4 | 0.763 |
| Perceived Training Programs | 5 | 0.819 |
| Perceived Top Management | | |
| Support and Commitment | 5 | 0.827 |
| Motivation of Employee | 3 | 0.712 |
| Perceived Job Roles and Responsibility | 5 | 0.747 |

The above results show that the majority of the variables obtained from organizational factors of Cronbach's alpha were above .7 (Nunnally, 1978). The majority of the anti image correlations were above .80 and above and this is in agreement with Hair et al. (2010). Notably, the size of organization obtained summated Cronbach's alpha of 0.680, information security awareness at 0.870, information security policy and procedure was 0.710, motivation of employee at 0.712 (Kabiru, 2012; Alabede, Arrifin & Idris, 2011; Fauzi, 2010; Hair et al., 2010). Hence, the researcher has confidence to proceed to further analysis.

5.6.3.4 Factor Analysis of Environmental Factors

Table 5.21a below portrays ISS MKO, MSA with .730. Bartlett's Test of Sphericity at 193.471, df of 6 and Significant at (.000). All these were in tune with Nunnally (1978). Therefore, it was suitable for factor analysis.

Table 5.21

KMO, MSA, Bartlett's Test of Sphericity, dr, and Significant of ISS

| | | |
|--|--------------------|---------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .730 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 193.471 |
| | Df | 6 |
| | Sig. | .000 |

Table 5.22 below indicates the factors that were extracted and with 58.055 percent of the cumulative variance. The factor loading of ISS was above .7. See the below Table 5.22 and Table 5.23.

Table 5.22

Total Variance Explained of ISS

| Comp | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | |
|------|---------------------|---------------|---------|-------------------------------------|---------------|--------|
| | Total | % of Variance | Cum % | Total | % of Variance | Cum % |
| 1 | 2.322 | 58.055 | 58.055 | 2.322 | 58.055 | 58.055 |
| 2 | .679 | 16.974 | 75.028 | | | |
| 3 | .585 | 14.635 | 89.663 | | | |
| 4 | .413 | 10.337 | 100.000 | | | |

Extraction Method: Principal Component Analysis.

Table 5.23

Rotated Component Matrix(a) of ISS

| | Component |
|------|-----------|
| | 1 |
| ISS1 | .789 |
| ISS2 | .769 |
| ISS3 | .765 |
| ISS4 | .722 |

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

However, Table 5.24a and Table 5.24b below portray MKO, MSA with .640. Bartlett's Test of Sphericity at 158.118 df of 3 and Significant at (.000). Also, the total variance explained was 67.030%. All these were in tune with Nunnally (1978). Therefore, it was suitable for factor analysis

Table 5.24a

KMO, MSA, Bartlett's Test of Sphericity, df and Significant of PGRR

| | | |
|---|--------------------|---------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy | | .640 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 158.118 |
| | df | 3 |
| | Sig. | .000 |

Table 5.24b

Total Variance Explained of PGRR

| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | |
|-----------|---------------------|------------|-----------------|-------------------------------------|------------|-----------------|
| | Total | % Variance | of Cumulative % | Total | % Variance | of Cumulative % |
| 1 | 2.011 | 67.030 | 67.030 | 2.011 | 67.030 | 67.030 |
| 2 | .629 | 20.955 | 87.985 | | | |
| 3 | .360 | 12.015 | 100.000 | | | |

Extraction Method: Principal Component Analysis.

The extracted factor was then computed for reliability. Table 5.25 below illustrates the environmental factor reliability test values which were above .7 (Nunnally, 1978). Thus, both factors are qualified for further analysis.

Table 5.25

The Summary of Reliability Test of Environmental factors

| Factors | No of items | Cronbach's Alpha |
|--|-------------|------------------|
| International Security Standards | 4 | .758 |
| Perceived Government Rules and Regulations | 3 | .747 |

5.6.3.5 Factor Analysis of Information Security Culture

Table 5.26 shows that KMO, MSA had 0.836, Bartlett's Test of Sphericity was 1.0543, df was 55, while Significant level was .000. This shows that information security culture was at acceptable ranges as posited by Nunnally (1978), and thus suitable for further analysis. The total variance was explained by 63.994 percent of the cumulative variance.

Table 5.26

KMO, MSA, Bartlett's Test of Sphericity, df, Significant of information security culture

| | | |
|---|--------------------|--------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy | | .844 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 1.1453 |
| | Df | 55 |
| | Sig. | .000 |

Table 5.27

*Extraction of Component for Information Security Culture Factors
Total Variance Explained of ISC*

| Com | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Sums of Rotation Squared Loadings | | |
|-----|---------------------|----------|---------|-------------------------------------|----------|--------|-----------------------------------|----------|--------|
| | Total | % of Var | Cum % | Total | % of Var | Cum % | Total | % of Var | Cum % |
| 1 | 4.922 | 44.745 | 44.745 | 4.922 | 44.745 | 44.745 | 4.208 | 38.251 | 38.251 |
| 2 | 1.853 | 16.843 | 61.588 | 1.853 | 16.843 | 61.588 | 2.567 | 23.338 | 61.588 |
| 3 | .846 | 7.694 | 69.283 | | | | | | |
| 4 | .725 | 6.595 | 75.878 | | | | | | |
| 5 | .605 | 5.498 | 81.376 | | | | | | |
| 6 | .554 | 5.035 | 86.411 | | | | | | |
| 7 | .444 | 4.036 | 90.447 | | | | | | |
| 8 | .341 | 3.099 | 93.545 | | | | | | |
| 9 | .307 | 2.790 | 96.335 | | | | | | |
| 10 | .271 | 2.461 | 98.796 | | | | | | |
| 11 | .132 | 1.204 | 100.000 | | | | | | |

Extraction Method: Principal Component Analysis.

Also, using component matrix, items were extracted into two factors. Hence, the result in

Table 5.28 presents the component matrix of information security culture.

Table 5.28

The Factor Loading Using Component Matrix on Information Security Culture

| | Component | |
|-------|-----------|------|
| | 1 | 2 |
| ISC11 | .896 | |
| ISC12 | .875 | |
| ISC14 | .797 | |
| ISC13 | .795 | |
| ISC10 | .779 | |
| ISC15 | .770 | |
| ISC3 | | .742 |
| ISC2 | | .687 |
| ISC4 | | .684 |
| ISC7 | | .641 |

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

Table 5.28 above indicates that there were slight changes in the factor loading of information security culture as a result of factor analysis, new variable renamed as organizational culture emerged. Table 5.29 below presents the reliability of the extracted factor by computing the Cronbach's Alpha value.

Table 5.29

The Summary of Reliability Test of Information Security Culture

| Factors | No of items | Cronbach's Alpha |
|----------------|--------------------|-------------------------|
| ISC | 6 | 0.914 |
| ISC2 | 5 | 0.741 |
| ISC Summated | 11 | 0.874 |

The indication of the reliability values from Table 5.29 is that both factors were acceptable since their alpha values were above .7 (Hair et al., 2010; Nunnally, 1978). Notably, ISC and ISC2 have acceptable alpha value of 0.914 and 0.741 respectively (Hair et al., 2010, Nunnally, 1978). Conversely, this study is not interested in each factor produced by the factor analysis but on the whole scale of ISC. Therefore, the results were summated to get an average value of 0.874 as it is practiced by Alabede et al. (2011) and Fauzi and Idris (2009). Table 5.30 below summarizes the validity and reliability test result of each dimension.

Table 5.30

The Summary of the Construct Validity and Reliability Results

| Construct | Items | Factor Loadings | KMO | % of Variance | Cronbach Alpha Value |
|-------------------------------|-------|--|--------|---------------|----------------------|
| DV | | | .811 | 64.754 | |
| OP | 7 | .877, .834, .640, .627, .800, .775, .667 | | | .822 |
| <u>Technological Factors</u> | | | | | |
| PTA | 5 | .776, .773, .751, .715, .704 | .717 | 55.394 | .797 |
| ISI | 5 | .820, .724, .583, .899, .793, | .688 | 64.536 | .680 |
| <u>Environmental Factors</u> | | | | | |
| ISS | 4 | .789, .769, .765, .722, | .730 | 58.055 | .758 |
| PGRR | 3 | .882, .799, .771 | .640 | 67.030 | .747 |
| <u>Organizational Factors</u> | | | | | |
| SO | 4 | .910, .850, .856, .808, .594 | 76.033 | .656 | |
| ISA | 6 | .847, .809, .784, .781, .747, .709 | .820 | 60.970 | .870 |
| ISPP | 3 | .820, .802, .711, .783, .751, .680 | .747 | 58.416 | .710 |
| PTP | 5 | .773, .770, .760, .703, .667 | .822 | 63.631 | .819 |
| PISTRV | 4 | .876, .771, .736, .703 | .794 | 67.924 | .809 |
| PTMSC | 4 | .854, .795, .791, .741, .668 | .808 | 59.612 | .827 |
| MOE | 3 | .843, .827, .669 | .619 | 67.975 | .712 |
| PJRRP | 5 | .774, .743, .738, .666, .659 | .655 | 51.449 | .763 |
| M V (ISC) | | | | | |
| ISC | 11 | .896, .875, .814, .796, .797, .795, .742, .687, .684, .666, .641 | .844 | 61.588 | .874 |

From the summary of all the factor loadings, it can be seen that the loaded factors are more than .4 and KMO was above .5 as suggested by Kaiser (1974). Moreover, the percentage of tolerance variance also show 50% and above, while the Cronbach's alpha was above .7 agreed with Hair et al., (2010). It is noted that information security in-sourcing and size of the organization have low alpha values and was excluded from further analysis. Table 5.31 below summarizes the component before and after factor loading.

Table 5.31
The Final Variables for Further Analysis

| Old Variable | Old Items | New Items |
|---|-----------|-----------|
| Organizational Performance | 8 | 7 |
| Perceived Technological Advancement | 6 | 5 |
| International Security Standard | 5 | 4 |
| Perceived Government Rules and Regulations | 3 | 3 |
| Information Security Awareness | 6 | 6 |
| Information Security Policy and Procedure | 7 | 3 |
| Perceived Training Programs | 9 | 4 |
| Perceived Information Security Risk, Threat and Vulnerability | 5 | 4 |
| Perceived Management Support and Commitment | 5 | 5 |
| Motivation of Employees | 9 | 3 |
| Perceived Job Roles and Responsibility | 6 | 5 |
| Information Security Culture | 15 | 11 |

In conclusion, due to the low Cronbach alpha values of the size of organization and information security in-sourcing variable during factor analysis, both variables were

excluded from further analysis (Hair et al., 2010, Nunally, 1978). Thus, the next section will discuss the re-statement of hypotheses.

5.7 The Re-Statement of Hypotheses

Based on the discussion in Subsection 5.6.3, the hypotheses of this research need to be re-stated because there are new variables. The summary of the re-statement of the hypotheses is provided in Table 5.32 below:

Table 5.32

The Re-statement of the Hypotheses

| Code | Statement of Hypotheses |
|------|--|
| H1 | Technological factors influence OP |
| H1.1 | Perceived Technology advancement influence OP |
| H2 | Environmental factors influence OP |
| H2.1 | International Security Standard influence OP |
| H2.2 | Perceived Government rules and regulation influence OP |
| H3 | Organizational factors influence OP |
| H3.1 | Information security awareness influence OP |
| H3.2 | Information security policy and procedure influence OP |
| H3.3 | Information security risks, threat and vulnerability influence OP |
| H3.4 | Perceived Training programs influence OP |
| H3.5 | Perceived management support and commitment influence OP |
| H3.6 | Motivation of employee influence OP |
| H3.7 | Perceived Job roles and responsibilities influence OP |
| H4 | Technological factors influence information security culture |
| H4.1 | Perceived Technology advancement influence ISC |
| H4.2 | Information Security In-sourcing influence ISC |
| H5 | Organizational factors influence ISC |
| H5.1 | Information security awareness influence ISC |
| H5.2 | Information security policy and procedure influence ISC |
| H5.3 | Perceived training programs influence ISC |
| H5.4 | Perceived Information security threat, risk and vulnerabilities influence ISC |

| Table 5.32 | Continued |
|------------|---|
| H5.5 | Perceived top management support and commitment influence ISC |
| H5.6 | Motivation of employee influence ISC |
| H5.7 | Perceived job roles and responsibilities influence ISC |
| H6 | Environmental Factors influence ISC |
| H6.1 | International security standard influence ISC |
| H6.2 | Perceived government rules and regulation influence ISC |
| H7 | Information Security Culture Mediate between Technological factors and OP |
| H7.1 | Information security culture mediate the relationship between PTA and OP |
| H7.2 | Information security culture mediate the relationship between ISI and OP |
| H8 | Information security culture Mediate between Organizational factors and OP |
| H8.1 | Information security culture mediate the relationship between ISA and OP |
| H8.2 | Information security culture mediate the relationship between ISPP and OP |
| H8.3 | Information security culture mediate the relationship between PTP and OP |
| H8.4 | Information security culture mediates the relationship between PISTRV and OP |
| H8.5 | Information security culture mediates the relationship between PTMSC and OP |
| H6.6 | Information security culture mediates the relationship between MOE and OP |
| H8.7 | Information security culture mediates the relationship between PJRR and OP |
| H9 | Information Security Culture Mediates between Environmental factors and OP |
| H9.1 | Organizational culture mediates the relationship between ISS and OP |
| H9.2 | Organizational culture mediates the relationship between PGRR and OP |

In summary, this section enumerates the effect of the factor analysis conducted on the hypothesis statement. The next section will discuss the descriptive test of the variables.

5.8 Descriptive Statistics of Variables

The recognition of variables uniqueness could be discovered through descriptive statistics computation such as the mean, standard deviation, minimum and maximum values. The descriptive statistics techniques used in this study include mean and standard deviations. The mean score and standard deviation were computed for each variable. Also, the weighted items of all the metric latent variables in respect of 204 cases in this study as it applied in the previous studies on information security and accounting information system is computed (Alabede et al., 2011; Ismail, 2007). The interpretation of the mean scores was considered as a 50th percentile range of five point Likert scale was calculated as .3 , the mean score above is considered as high (Positive) and less than .3 were considered as low (Negative).

5.8.1 Descriptive Statistics of Technological Factors

In Table 5.33 below, the result of the descriptive statistics shows that the mean value for Technological advancement is within mean of (1.68-1.98) while information security insourcing is also within the range value of (1.81-2.05).

Table 5.33
Descriptive Statistics of Technological Factors

| Descriptive Statistics | | | | | |
|-------------------------------|-----|---------|---------|------|----------------|
| | N | Minimum | Maximum | Mean | Std. Deviation |
| PTA1 | 204 | 1 | 5 | 1.98 | .972 |
| PTA2 | 204 | 1 | 5 | 1.79 | .633 |
| PTA3 | 204 | 1 | 4 | 1.83 | .726 |
| PTA4 | 204 | 1 | 4 | 1.87 | .752 |
| PTA5 | 204 | 1 | 3 | 1.64 | .607 |
| PTA6 | 204 | 1 | 3 | 1.69 | .595 |
| ISI1 | 204 | 1 | 4 | 1.99 | .574 |
| ISI2 | 204 | 1 | 5 | 1.90 | .643 |
| ISI3 | 204 | 1 | 5 | 2.05 | .682 |
| ISI4 | 204 | 1 | 5 | 2.05 | .801 |
| ISI5 | 204 | 1 | 5 | 1.81 | .705 |

Valid N= 204
(listwise)

5.8.2 Descriptive Statistics for Organizational Factors

The mean range of all the items in organizational factors is within the value of 1.66 – 2.08. The results of the mean show low score. This means that the respondents' views of each item of an organizational factor is low (negative).

5.8.3 Descriptive Statistics for Environmental Factors

From Table 5.34 below, it can be seen that the respondents indicated a positive agreement with the items stated in the environmental factors.

Table 5.34

Descriptive Statistics of Environmental Factors

| | N | Minimum | Maximum | Mean | Std. Deviation |
|-------|-----|---------|---------|------|----------------|
| ISS1 | 204 | 1 | 5 | 1.78 | .592 |
| ISS2 | 204 | 1 | 5 | 1.84 | .647 |
| ISS3 | 204 | 1 | 4 | 1.87 | .610 |
| ISS4 | 204 | 1 | 4 | 1.88 | .625 |
| ISS5 | 204 | 1 | 4 | 1.92 | .669 |
| PGRR1 | 204 | 1 | 5 | 1.87 | .656 |
| PGRR2 | 204 | 1 | 5 | 1.88 | .587 |
| PGRR3 | 204 | 1 | 4 | 1.90 | .547 |

ValidN=204

(listwise)

N =204 (N represents the number of respondents)

5.8.4 Descriptive Statistics for Information Security Culture

Table 5.35 shows that the respondents agreed with the items stated in the information security culture.

Table 5.35

Descriptive Statistics of ISC

| | N | Minimum | Maximum | Mean | Std. Deviation |
|-------|-----|---------|---------|------|----------------|
| ISC1 | 204 | 1 | 5 | 1.79 | .775 |
| ISC2 | 204 | 1 | 4 | 1.83 | .580 |
| ISC3 | 204 | 1 | 5 | 1.89 | .626 |
| ISC4 | 204 | 1 | 5 | 1.92 | .732 |
| ISC5 | 204 | 1 | 5 | 2.22 | 1.009 |
| ISC6 | 204 | 1 | 5 | 1.97 | .705 |
| ISC7 | 204 | 1 | 5 | 1.83 | .737 |
| ISC8 | 204 | 1 | 4 | 1.71 | .643 |
| ISC9 | 204 | 1 | 5 | 2.01 | .756 |
| ISC10 | 204 | 1 | 5 | 2.27 | 1.052 |
| ISC11 | 204 | 1 | 5 | 2.52 | 1.151 |
| ISC12 | 204 | 1 | 5 | 2.50 | 1.125 |
| ISC13 | 204 | 1 | 5 | 2.50 | 1.143 |
| ISC14 | 204 | 1 | 5 | 2.19 | .944 |
| ISC15 | 204 | 1 | 5 | 2.36 | .995 |

Valid N=204

(listwise)

N =204 (N represents the number of respondents)

5.8.5 Descriptive Statistics for Organizational Performance

The response of the respondents to organizational performance with a mean value of 1.48- 1.79 and standard deviation values of .520 - .710 implied a negative (lower)

respondents' perception with the statement of the OP items in the questionnaires. Please, refer to Table 5.36 for details

Table 5.36
Descriptive Statistics of Organizational Performance

| | N | Minimum | Maximum | Mean | Std. Deviation |
|-----|-----|---------|---------|------|----------------|
| Op1 | 204 | 1 | 3 | 1.48 | .520 |
| Op2 | 204 | 1 | 4 | 1.56 | .571 |
| OP3 | 204 | 1 | 5 | 1.62 | .628 |
| Op4 | 204 | 1 | 5 | 1.79 | .716 |
| OP5 | 204 | 1 | 4 | 1.66 | .642 |
| OP6 | 204 | 1 | 4 | 1.71 | .710 |
| Op7 | 204 | 1 | 5 | 1.65 | .661 |
| OP8 | 204 | 1 | 3 | 1.52 | .539 |

Valid N=204

(listwise)

N =204 (N represents the number of respondents)

To recapitulate, the mean of the variables falls within the stipulated range. The next section will discuss correlation analysis of the study.

5.9 Correlation Analysis

The correlation in this study was computed by using multiple regressions. Distinctly, Pearson correlation was employed to check the direct relationship among the variables. Pearson correlation measure how variables are ranked using coefficient of "R" measures the linear relationship. Where $r = 0.10$ to 0.29 is regarded to be a small strength of the

relationship, $r = 0.30- 0.49$ is medium, good and high in the strength of the relationship and, $r = 0.50$ to 1 is assumed to be large or very high in the relationship.

Nevertheless, this study employ the rule of thumb of Guilford (1973) as shown in Table 5.37. Also, hierarchical regression was also used to test for the indirect mediating effect of information security culture on the relationship between the organizational performance and the TOE factors.

Table 5:37
Guilford Rule of Thumb (1973)

| R | Degree of relationship / Correlation |
|---------|--------------------------------------|
| < 0. 20 | Very weak correlation |
| < 0. 40 | Weak correlation |
| < 0. 70 | Moderate Correlation |
| < 0.90 | Strong correlation |
| > 0.90 | Very strong correlation |

This study employs the Guilford rule of thumb (1973) above as a guide in correlation analysis. Thus, the overall result provides that organizational performance is correlated with all the other variables. Result of correlation analysis is illustrated in Table 5.39

Table 5.38

Correlations Analysis Summary between Variables

| Variable | PTA | ISS | PGRR | ISA | ISPP | PTP | P ISRTV | PTMSC | MOE | PJRR | OP | ISC | | |
|----------|--------|--------|--------|--------|--------|--------|---------|--------|------|--------|--------|------|------|---|
| PTA | 1 | | | | | | | | | | | | | |
| ISS | .107* | 1 | | | | | | | | | | | | |
| PGRR | .151* | .383** | 1 | | | | | | | | | | | |
| ISA | .004 | .406** | .685** | 1 | | | | | | | | | | |
| ISPP | .323** | .473** | .503** | .669** | 1 | | | | | | | | | |
| PTP | .486** | .373** | .582** | .180* | .327** | 1 | | | | | | | | |
| PISTRV | .200** | .229** | .200** | .120* | .289** | .436** | 1 | | | | | | | |
| IST | .254** | .154* | .154* | .163 | .077 | .230** | .440** | .366** | 1 | | | | | |
| PTMSC | .063 | .145* | .149* | .225** | .112 | .235** | .223** | .283** | | 1 | | | | |
| MOE | .024 | .039 | .010 | -.025 | .168* | .088 | .109 | .155* | .043 | | 1 | | | |
| PJRR | .143 | .163* | .193 | .019 | .264** | .224** | .296** | .245** | .056 | .162* | | 1 | | |
| OP | .280** | .153 | .137 | .042 | .251** | .246** | .026 | .117 | .010 | .125 | .138 | .048 | 1 | |
| ISC | .162** | .184** | .149 | -.105 | .379** | .174* | .124 | .162* | .104 | .276** | .293** | .068 | .122 | 1 |

** Correlation is significant at 0.01(2-tailed), * Correlation is significant at 0.05 level (2 tailed).

5. 10 Multiple Regression Analysis

As it has been discussed in chapter three that multiple regression analysis is the most widely used techniques in social sciences to examine the relationship between a single dependent variable and several independent variables (Hair et al; 2010; Tabachnick &

Fidell, 2001). The greatest value in research is the ability to identify the dimension of variables in the relationship of empirical research (Hair et al; 2010; 2006; Bryman & Cramer, 2001).

Using factor analysis in the extraction method of the principal component factoring with the rotation method of Varimax and Kaiser Normalization is to analyze organizational performance, technological, organizational and environmental factors as well as the information security culture (Coakes & Ong, 2011). Therefore, Hypotheses H₁- H₆ were tested using multiple regression analysis while H₇- H₉ were also tested using hierarchical regression to know the mediating effects of information security culture on the relationship between organizational performance and TOE factors.

There are four steps involved in testing mediation as stipulated by Ramayah (2011), Baron and Kenny (1986). These steps are: (1) TOE factors (IVs) statistically significantly related to organizational performance (DV), (2) TOE factors is significantly related to information security culture (MV), (3) when TOE factors and information security culture is regressed against organizational performance, information security culture is significant (Ramayah, 2011; Baron & Kenny, 1986), and (4) after the three steps, if the beta value of TOE factors decreases / increases, if it is still significant hence, partial mediation/full mediation occurs such framework is considered significantly mediated (Hair et al., 2011, 2010; Baron and Kenny, 1986). The assumption for statistical data has been discussed succinctly in chapter three.

5.11 Testing for the Framework using Multiple Regression Analysis

Multiple regressions were computed to investigate the relationship between organizational performance and TOE factors, such as perceived technological advancement, information security in-sourcing, international security standard, perceived government rules and regulations, information security awareness, information security policy and procedure, perceived training programs, perceived information security risk, threat and vulnerabilities, perceived top management support and commitment, motivation of employee and perceived job roles and responsibilities.

In addition, multiple regressions enable many indicators to explain a single relationship. The p value must be significant to illustrate how a set of variables can predict an outcome. From Table 5.39, the model is significant at .000. Table 5.40 shows that TOE factors are significant with organizational performance (PTA β = 0.356, P value=.000, ISS β = 0.166, P value= 0.014, PTP β =0.158, p value =0.036, PISTRV β =0.268, p value= .000, ISA β = -.141, p value = 0.029, MOE β =.134, p value= 0.040, ISPP β =-.197, p value= 0.025, and PJRR β =-.123, p value= 0.050 while PTMSC and PGGR were not statistically significant. Hence, this study employs 0.01, 0.05 and 0.1 (1%, 5% and 10%) at the acceptable significant level for this study. Thus, Table 5.39 - 5.40 illustrates the result.

Table 5.39

ANOVA(b) of TOE factors and OP

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|-------|------------|----------------|-----|-------------|-------|-------------------|
| 1 | Regression | 10.849 | 10 | 1.085 | 7.997 | .000 ^a |
| | Residual | 26.182 | 193 | .136 | | |
| | Total | 37.031 | 203 | | | |

a. Predictors: (Constant), MPJRR, MIPISTRV, MPISPP, MISA, MMOE, MPTA, MISS, MIPTP, MTMSC, MPGRR

b. Dependent Variable: MOP

Table 5.40

Coefficients(a) of TOE factors and OP

| Model | | Unstandardized Coefficients | | Std Coefficient | t | Sig. | Collinearity Statistics | |
|-------|-----------|-----------------------------|------------|-----------------|--------|------|-------------------------|-------|
| | | B | Std. Error | Beta | | | Tolerance | VIF |
| 1 | Constant) | .725 | .320 | | 2.269 | .024 | | |
| | MPTA | .303 | .056 | .356 | 5.448 | .000 | .858 | 1.166 |
| | MISS | .159 | .064 | .165 | 2.486 | .014 | .819 | 1.221 |
| | MIPTP | .172 | .081 | .158 | 2.111 | .036 | .657 | 1.523 |
| | MIPISTRV | -.256 | .068 | -.268 | -3.741 | .000 | .715 | 1.399 |
| | MISA | .152 | .069 | .141 | 2.198 | .029 | .894 | 1.119 |
| | MMOE | .158 | .076 | .134 | 2.069 | .040 | .869 | 1.151 |
| | MTMSC | .013 | .024 | .046 | .562 | .575 | .550 | 1.820 |
| | MPGRR | -.032 | .026 | -.109 | -1.219 | .224 | .461 | 2.171 |
| | MPISPP | .079 | .035 | .197 | 2.260 | .025 | .484 | 2.067 |
| | MPJRR | -.095 | .048 | -.123 | -1.973 | .050 | .936 | 1.068 |

a. Dependent Variable:

MOP

However, From Table 5.41, the model is significant at .000. Table 5.42 shows that TOE factors are significant with information security culture (PTA β = 0.323, P value=.000, ISS β = 0.120, P value= 0.013, PTP β =0.214, p value =0.004, PTMSC β =.176, p value= 0.032, and PGRR β =-.123, p value= 0.023 while MISA, PISTRV, MISPP, MOE and PJRR not statistically significant. Hence, this study employs 0.01, 0.05 and 0.1 (1%, 5% and 10%) at the acceptable significant level for this study. Thus, Table 5.39 - 5.40 illustrates the result.

Table 5.41
ANOVA(b) of ISC and TOE factors

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|-------|------------|----------------|-----|-------------|-------|-------------------|
| 1 | Regression | 19.944 | 10 | 1.994 | 8.224 | .000 ^a |
| | Residual | 46.807 | 193 | .243 | | |
| | Total | 66.751 | 203 | | | |

a. Predictors: (Constant), MPJRR, MIPISTRV, MPISPP, MISA, MMOF, MPTA, MISS, MIPTP, MTMSC, MPGRR

b. Dependent Variable: MISC

Table 5.42

Coefficients(a) of ISC and TOE Factors

| Model | | Unstandardized Coefficients | | Std coefficient | t | Sig. | Collinearity Statistics | |
|-------|--------------|-----------------------------|------------|-----------------|--------|------|-------------------------|-------|
| | | B | Std. Error | Beta | | | Tolerance | VIF |
| 1 | (Constant) | .161 | .427 | | .378 | .706 | | |
| | MPTA | .369 | .074 | .323 | 4.964 | .000 | .858 | 1.166 |
| | MISS | .154 | .086 | .120 | 1.800 | .013 | .819 | 1.221 |
| | MIPTP | .313 | .109 | .214 | 2.875 | .004 | .657 | 1.523 |
| | MIPIST RV | .083 | .092 | .064 | .901 | .369 | .715 | 1.399 |
| | MISA | -.055 | .092 | -.038 | -.596 | .552 | .894 | 1.119 |
| | MMOE | .063 | .102 | .040 | .616 | .539 | .869 | 1.151 |
| | MTMS C | .069 | .032 | .176 | 2.163 | .032 | .550 | 1.820 |
| | MPGR R | -.080 | .035 | -.204 | -2.291 | .023 | .461 | 2.171 |
| | MPISPP | .009 | .047 | .017 | .191 | .849 | .484 | 2.067 |
| | MPJRR | .063 | .064 | .061 | .983 | .327 | .936 | 1.068 |

a. Dependent Variable:
MISC

5.12 Hierarchical Multiple Regression Analysis

Hierarchical multiple regression analysis allows deduction from the result as to whether the mediating variable of information security culture strengthens the relationship (Baron & Kenny, 1986) between TOE factors and organizational performance. The hierarchical regression was carried out using 204 cases. This study computed hierarchical multiple regression analysis based on the four steps involved in testing mediation. Those steps are: (1) TOE factors (IVs) statistically significantly related to organizational performance (DV), (2) TOE factors is significantly related to information security culture (MV), (3) when TOE factors and information security culture was regressed against organizational

performance, information security culture found to be significant (Ramayah, 2011; Baron & Kenny, 1986), and (4) from third steps mentioned above, the beta value of TOE factors decreases but it was still significant, this signifies partial mediation. Thus, framework is significantly mediated (Hair et al., 2011, 2010; Baron and Kenny, 1986).

From Table 5.43 below, the model is significant at .024. Table 5.44 shows that ISC mediates the relationship between TOE factors and organizational performance. (PTA $\beta = .344$, P value=.000, ISS $\beta = .162$, P value= .018, PTP $\beta = .150$, p value =0.051, PISTRV $\beta = -.270$ p value= .000, ISA $\beta = .142$, p value = .028, MOE $\beta = .133$, p value= .043, ISPP $\beta = .196$, p value= .026 and PJRR $\beta = -.126$, p value= .047 and ISC $\beta = p$ value =.021 while PTMSC and PGRR were not significant. Hence, this study employs 0.01, 0.05 and 0.1 (1%, 5% and 10%) at the acceptable significant level for this study. Thus, Table 5.44 illustrates the result. The hierarchical regression result after computation is shown in Tables 5.43 -5.44

Table 5.43
ANOVA (c) on TOE factors, ISC, and OP

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|-------|------------|----------------|-----|-------------|-------|-------------------|
| 1 | Regression | 10.849 | 10 | 1.085 | 7.997 | .000 ^a |
| | Residual | 26.182 | 193 | .136 | | |
| | Total | 37.031 | 203 | | | |
| 2 | Regression | 10.882 | 11 | .989 | 7.264 | .000 ^b |
| | Residual | 26.149 | 192 | .136 | | |
| | Total | 37.031 | 203 | | | |

a. Predictors: (Constant), MPJRR, MIPISTRV, MPISPP, MISA, MMOE, MPTA, MISS, MIPTP, MTMSC, MPGRR

b. Predictors: (Constant), MPJRR, MIPISTRV, MPISPP, MISA, MMOE, MPTA, MISS, MIPTP, MTMSC, MPGRR, MISC

Table 5.44
Coefficients(a) on TOE factors, ISC, and OP

| Model | | Unstandardized Coefficients | | Std Coefficients | | Collinearity Statistics | | |
|-------|--------------|-----------------------------|------------|------------------|--------|-------------------------|------|-------|
| | | B | Std. Error | Beta | t | Sig. | Tol | VIF |
| 1 | (Constant) | .725 | .320 | | 2.269 | .024 | | |
| | MPTA | .303 | .056 | .356 | 5.448 | .000 | .858 | 1.166 |
| | MISS | .159 | .064 | .166 | 2.486 | .014 | .819 | 1.221 |
| | MIPTP | .172 | .081 | .158 | 2.111 | .036 | .657 | 1.523 |
| | MIPIST RV | -.256 | .068 | -.268 | -3.741 | .000 | .715 | 1.399 |
| | MISA | .152 | .069 | .141 | 2.198 | .029 | .894 | 1.119 |
| | MMOE | .158 | .076 | .134 | 2.069 | .040 | .869 | 1.151 |
| | MTMSC | .013 | .024 | .046 | .562 | .575 | .550 | 1.820 |
| | MPGRR | -.032 | .026 | -.109 | -1.219 | .224 | .461 | 2.171 |
| | MPISPP | .079 | .035 | .197 | 2.260 | .025 | .484 | 2.067 |
| | MPJRR | -.095 | .048 | -.123 | -1.973 | .050 | .936 | 1.068 |
| 2 | (Constant) | .721 | .320 | | 2.250 | .026 | | |
| | MPTA | .293 | .059 | .344 | 4.953 | .000 | .761 | 1.314 |
| | MISS | .155 | .065 | .162 | 2.396 | .018 | .805 | 1.242 |
| | MIPTP | .164 | .083 | .150 | 1.963 | .051 | .630 | 1.588 |
| | MIPIST RV | -.258 | .069 | -.270 | -3.758 | .000 | .712 | 1.405 |
| | MISA | .153 | .069 | .142 | 2.213 | .028 | .892 | 1.121 |
| | MMOE | .156 | .076 | .133 | 2.041 | .043 | .867 | 1.153 |
| | MTMSC | .012 | .024 | .040 | .478 | .633 | .537 | 1.864 |
| | MPGRR | -.030 | .026 | -.101 | -1.120 | .264 | .448 | 2.230 |
| | MPISPP | .079 | .035 | .196 | 2.248 | .026 | .484 | 2.067 |
| | MPJRR | -.097 | .048 | -.126 | -1.999 | .047 | .932 | 1.073 |
| | MISC | .027 | .054 | .036 | .496 | .021 | .701 | 1.426 |

a. Dependent Variable:
MOP

5.13 Research Hypotheses Test Result

As previously discussed, the research hypotheses $H_1 - H_6$ were tested using multiple regression analysis, whereas H_7-H_9 used hierarchical regression process. The proposed hypotheses were thirty six but were reduced to thirty four because of low alpha value of ISI and SO. This can be clearly seen in the summary result of the hypotheses in Table 5.45 below.

Table 5.45

The Summary of the Hypotheses Testing

| Code | Statement of Hypotheses | Remarks |
|-----------|--|------------------|
| H1 | Organizational Performance is influenced by Technological Factors | Supported |
| H1.1 | Perceived technology advancement is influence Organizational performance | Supported |
| H2 | OP in Nigerian banks is influenced by Environmental Factors | |
| H2.1 | International security standards influence OP | Supported |
| H2.2 | Perceived Government rules & regulations influence OP | N/S |
| H3 | Organizational Performance in Nigeria banks is influenced by Organizational Factors | |
| H3.1 | Information security awareness influence OP | Supported |
| H3.2 | Perceived training programs influence OP | Supported |
| H3.3 | Information security threat, risks& vulnerabilities influence OP | Supported |
| H3.4 | Information security policy and procedure influence OP | Supported |
| H3.5 | Perceived management support and commitment influence OP | N/S |
| H3.6 | Motivation of employee influence OP | Supported |
| H3.7 | Perceived job roles and responsibilities influence OP | Supported |

Table 5.45 Continued

| | |
|--|------------------|
| H4 Technological factors are Influenced by ISC | Supported |
| H4.1 Perceived technological advancement influence ISC | Supported |
| H4.2 International security standard influence ISC | Supported |
| H5 Environmental Factors influence ISC | |
| H5.1 Perceived government rules and regulation influence ISC | Supported |
| H6 Organizational Factors influence ISC | |
| H6.1 Information security awareness influence ISC | N/S |
| H6.2 Information security policy and procedure influence ISC | N/S |
| H6.3 Perceived training programs influence ISC | Supported |
| H6.4 Perceived information security threat, risk and vulnerability influence ISC | N/S |
| H6.5 Perceived top management support and commitment influence ISC | Supported |
| H6.6 Motivation of employees influences ISC | N/S |
| H6.7 Perceived job roles and responsibilities influence ISC | N/S |
| H7 Information Security Culture Mediates between OP and Technological factors | Supported |
| H7: 1. Perceived technology advancement and OP | Supported |
| H7.2 International security standard and OP | Supported |
| H8. ISC Mediate between Environmental Factors and OP | |
| H8.1 Perceived government rules and regulations and OP | N/S |
| H9 ISC Mediate between OP and Organizational Factors | |
| H9. 1 Information security awareness and OP | Supported |
| H9.2 Information security policy and procedure and OP | Supported |
| H9.3 Information security threat, risks & vulnerabilities and OP | Supported |
| H9.4 Perceived training programs and OP | Supported |
| H9.5 Perceived top management support and commitment and OP | N/S |
| H9.6 Motivation of employee and OP | Supported |
| H9.7 Perceived job roles and responsibility and OP | Supported |

N/S= Not Supported

5.14 Refining of the Framework

Having done a series of analysis and discovered there are changes, especially when considering the framework. Figure 5.2 below illustrates the revised framework. The next chapter will elaborate on the improved framework.

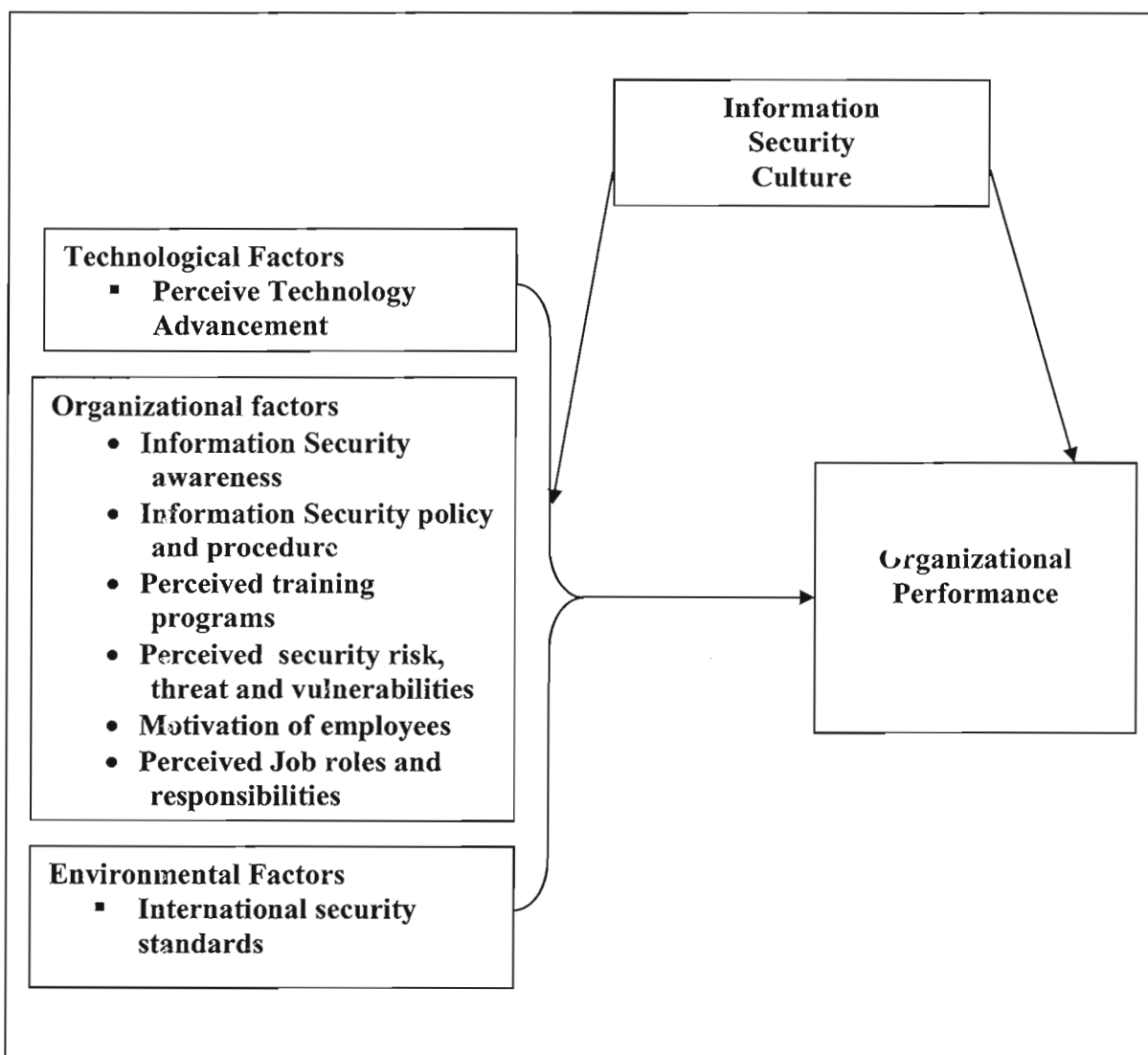


Fig. 5.2: Revised Theoretical Framework of ISC on Organizational Performance

5.15 Summary

This chapter presents the details of the various analyses computed on the data collection during the course of the research. In the descriptive statistics, perceived technology advancement, international security standard, perceived government rules and regulations has low mean while information security culture had a high overall mean score which means that the respondents had both negative and positive opinions about the variables.

The Cronbach's alpha from reliability results illustrate that 90% of the variables are above .7. Thus, the condition of internal consistency in measurement of items in this study is fulfilled. For factor analysis, items in each latent variable that does not fulfill the minimum requirement were deleted in order to meet the criteria under construct validity. With respect to multiple regressions analysis, three regressions were undertaken. The first regression measured the relationship between the dependent variable and independent variables in order to achieve the first objective of the study. The second aimed at evaluating the mediating effect of organizational performance and TOE factors. This third was designed to achieve the second objective of this study.

In addition, the findings from the multiple regression of TOE factors and organizational performance show that the models were significant and perceived technology advancement, information security standard, information security awareness, perceived training programs, information security policy and procedures, motivation of employee, perceived information security threats, risk and vulnerabilities, and perceived job roles and responsibilities has a strong positive relationship with organizational performance.

But, perceived government rule and regulations, and perceived top management support and commitment were not statistically significant. On the other hand, perceived technology advancement, information security standard, perceived top management support and commitment, motivation of employee and perceived government rules and regulations were statistically significant with information security culture.

Lastly, the result of the mediating effect shows that information security culture has significantly mediates the relationship between the TOE factors and organizational performance.

CHAPTER SIX

DISCUSSION ON FINDINGS

6.1 Introduction

The primary aim of this study is to examine the determinants of information security culture practices towards achieving organizational performance in the Nigerian banking sector using the technological, organizational and environmental factors. Furthermore, it examines the mediating effect of information security culture on the relationship between organizational performance and TOE factors. Based on the objectives of this study, the study answers the questions discussed in chapter 1. Thus, the study vividly discussed the findings of the variables tested in chapter five and implications to the practical setting. In collaboration with the findings of the study, Subsections 6.2- 6.4 elaborate the discussion in detail.

6.2 The Implication to the Practical Setting

The primary objective of this study is to examine the determinant of information security practices on organizational performance, and the establishment of information security culture in the Nigerian banking sector. It also examines the mediating effect of information security culture in the relationship between TOE factors (information security activities) and organizational performance. The regression results answer the research questions as represented in chapter five. In this chapter, the implication of the results to the practical setting is offered. This is dealt with in subsections 6.3.1 - 6.3.10 below.

6.3 Research Question 1: What are elements such as Technological, Organizational and Environmental Factors that influences Organizational Performance?

The test of hypotheses H_1 - H_6 indicates that the model is significant. The hypotheses support the relationship between perceived technology advancement, international security standard, information security awareness, perceived training program, perceived information security threat, risk and vulnerabilities, information security policy and procedure, motivation of employee, perceived job roles and responsibilities. The results show that those variables were statistically significant, while perceived government rule and regulations were not significant.

6.3.1 Relationship between Perceived Technology Advancement and Organizational Performance

The descriptive statistics indicate strong evidence that perceived technological advancement is an influencing factor of organizational performance in the Nigerian banks. The finding is consistent with Ehikamenor (2009), Orlikowski and Barley (2001), Sambamurthy (2000) and Boynton et al. (1994). This is because perceived technology advancement/ IT enable security compliance and regulation, and it is an organizational strategy for effectiveness. Thus, the use of computer enhances performance in the organization (Ehikamenor, 2009; Yam, 1998; Hoffman, 1998).

Furthermore, the use of computer or IT will support the organization in gaining competitive advantage. Secondly, the reduction of cost and time enables organizations to focus on new business. However, from the regression analysis, the result ($P=0.00$)

provides the evidence that perceived technology advancement plays major role in organizational performance effectiveness. Thus, H1.1 was accepted.

6.3.2 Relationship between International Security Standard and Organizational Performance

ISO 27001 stipulates policies and procedures in relation to organizational performance. These policies and procedures are the tools in reducing threat or security breaches. Onasanya (2010) opined that the compliance to certification with ISO, 27001 proves that the banks are complying with international standard in terms of technology, human and process (Omu, 2010). This is why First Bank of Nigeria is the only bank among the twenty four banks that got its certification while other banks are still struggling to conform to ISO 27001 (Omu, 2010; New Vista for banking Operation). These research findings however show that ISS was supported, although no empirical evidence from previous researches. Thus, H2.1 was accepted.

6.3.3 Relationship between Perceived Government Rules and Regulations and Organizational Performance

The empirical evidence from this study indicates that there is no strong relationship between organizational performance and perceived government rules and regulations. This may be due to the fact that the Nigerian banking system has not been fully incorporated into the international financial system or information security system (Akinsuyi (2009). Therefore, CBN and NDIC as the regulating bodies in Nigeria have enacted policies that will inculcate international standard such as Sarbanes- Oxley Acts, European Data Privacy Directive (EDPD) in order to enhance implementation of

information security standards. The result of this research indicates that government rule and regulations does not influence organizational performance.

6.3.4 Relationship between Information Security Awareness and Organizational Performance

The regression result computed establishes that there is a strong relationship between organizational performance and information security awareness. This is in agreement with Zakaria (2007) and Computer Security Act 1987. Their findings agree with the theoretical submission on the information security awareness. Thus, it shows that the employees will be familiar with information security within the organization and will be able to know how to prevail over it.

The finding in this study is in compliance with Computer Security Act 1987 that urged organizations and federal agencies to provide awareness to users of information system. In other words, creating awareness will enable employees to have knowledge of the involved risks and how to avert it. The finding of this study shows that information security awareness was supported. This is in agreement with a number of empirical studies on information security awareness such as situational information security awareness carried out in the USA by Chen, Medlin and Shaw (2008), Gatewood (2005), Wilson and Hash (2003). Thus, the empirical evidence from this study suggests that information security awareness is a determinant to establishing an information security culture among Nigerian banks. Thus, H3.1 was accepted.

6.3.5 Relationship between Information Security Policy and Procedure and Organizational Performance

Information security policy and procedure need to be followed as far as the issue of information security is concerned (Hone & Eloff, 2003). The regression result of this research proves that information security policy influence organizational performance in Nigeria. This illustrates that CBN and NDIC, as regulating bodies in Nigeria need to work immensely to enact laws on the development, maintenance and increase integrity on information system and ultimately, to combat the problem of security breaches in Nigeria (Domínguez, 2009; CBN Annual report, 2009; Akinsuyi, 2009).

6.3.6 Relationship between Perceived Information Security Risks, Threats and Vulnerability and Organizational Performance

The motive behind information security risk control is basically to avert unforeseen occurrence to information security, availability, integrity and confidentiality which can hinder organization to gain a competitive edge in this computer age (Brown & Heywood, 2006; Hong et al., 2003; Kankanhilli et al., 2003). The finding of this study shows that perceived information security threat, risk and vulnerability was statistically significant and H3.4 was accepted. The implication of this result shows that practitioners view risk as a threat that need to be given priority. Thus, CBN and NDIC must inculcate information security culture among the Nigerian banks.

However, Akinsuyi (2009) emphasized the need for top managers to keep watch on risk assessment. The regression result of information security risk support hypotheses (H3.4), this shows that perceived information security risk, threat and vulnerabilities influence

organizational performance. The above finding is consistent with Akinsuyi (2009), Mohammad and Suborna (2009) NIST (2003), Usamni (2008). In other words, Nigerian banks should realize the importance of confidentiality, integrity and availability of information within the organization.

6.3.7 Relationship between Perceived Training Programs and Organizational Performance

The regression result shows that perceived training program influence organizational performance in Nigeria. This suggests that the absence of security awareness is due to the employees that are not familiar with information security within the organization and do not know how to prevail over it (Zakaria, 2007). Computer Security Act provision of 1987 urge the organizations and federal agencies to provide awareness to users of information system. In other words, creating awareness will enable employees to have knowledge of the risks involve and how to avert it. The finding of this research was in agreement with the OECD guideline for the information system security. It is important that the empirical result shows that training program leads to information security culture participation within the organization if fully established (Qingxiong et al., 2009; ISO 27001).

6.3.8 Relationship between Perceived Top Management Support and Commitment and Organizational Performance

The finding provides evidence that perceived top management support and commitment does not influence organizational performance in Nigeria. This is consistent with Kajaya, Anuila, Varonen, Savola and Rönning (2006). Their study concluded that lack of

management support exist because of the belief that the top management and commitment does not need to be taught or preached to. In such phenomenon where top management fails to appreciate, the consequences of the organization's business activities may be daunting (Kajaya et al., 2006). Hence, top management needs to be encouraged and motivated when issue of information security arises.

6.3.9 Relationship between Motivation of Employees and Organizational Performance

The introduction of motivation of employee as a determinant of information security culture followed by expert suggestion is another interesting scenario during the process of this research. This study tried to consider the motivation of employees as part of the influencing factors of organizational performance. Employees need to be familiar with information security in order to know how to prevail over any threat or risk (Zakaria, 2007; Von Solms, 1999). The finding of this present study shows that motivation of employee was found to be significant with organizational performance among banks in Nigeria. It suggested then that there is a strong relationship between the two variables. Thus, in the context of Nigeria, bank officials should be acquainted with risks aversion and in turn organizational performance will be made possible.

6.3.10 The Relationship between Perceived Job Roles and Responsibilities and Organizational Performance

In this study, it was hypothesized that organizational performance is influenced by perceived job roles and responsibilities (PJRR). It plays a vital role on how information system task will be carried out within the organization. However, PJRR was introduced

as a variable and the finding shows that it was statistically significant. This shows that in the Nigerian banking sector, segregation of duties will lead to organizational performance. The previous researchers opined that job responsibilities enable easy allocation of employees' task (Toval et al., 2002; Bjorck, 2001 & Sami Abu-Zineh, 2006). Thus, it means that the nature of banking industry influence the management of Nigerian banks to establish an effective IS in the organization. Hence, hypothesis H5.7 was accepted.

6.4 Research Question 2: What is the Relationship between TOE Factors and Information Security Culture?

Introduction of the establishment of information security culture is of great value in this study. From the findings, the empirical evidences indicate that perceived technology advancement, international security standard, perceived training programs, perceived top management support and commitment and perceived government rules and regulations statistically significant to the establishment of information security culture. Information securities activities lead to information routines and in turn information security norms and ultimately information security culture (Zakaria, 2013) Thus, the establishment of information security culture are imperative and in turn, improve organizational performance.

6.5 Research Question 3: To Examine whether Information Security Culture Mediate the Relationship between TOE Factors and Organizational Performance

In order to achieve objective 3 of this study, information security culture was introduced as mediating variable. The empirical evidence provides that TOE factors such as PTA, ISS, PISTRV, ISA, ISPP MOE, PTP, and PJRR were significant. Nevertheless, the mediating effect of information security culture was conducted as suggested that information security culture could assist as a factor that could trigger success in organizational performance (Qingxiong et al., 2008). Other researchers were of the opinion that it can be employed as a mediating variable of organizational performance since it will strengthen or change the form of the relationship between a predictor and an outcome (Sekaran, 2003; Baron & Kenny, 1986). Thus, in this study it was hypothesized that information security culture mediates the relationship between organizational performance and TOE factors.

6.5.1 Information Security Culture Mediates the Relationship between Perceived Technology Advancement and Organizational Performance

This study illustrates that information security culture statistically mediates the relationship between perceived technology advancement and organizational performance. Thus, in the era where the technical know-how of IT is becoming a difficult phenomenon, reducing costs and improving activities will affect profitability (Parsons et al., 2012); Martins, 2012). There is a need for the establishment of information security culture that will propel performance. Previous researchers opined that adequate technology will reduce time to market and time to respond to the requirements of the business, new

legislation and individual liability and reliance on IT as a critical enabler of many compliance, regulatory, corporate governance effectiveness and organizational effectiveness capabilities (Ville, Kraemer & Gurbaxani, 2004; Kohli & Devaraj, 2003; Yam, 1998; Hoffman, 1998). Thus, this study indicates that ISC mediates between perceived technology advancement and organizational performance and H7.1 was accepted.

6.4.2 Information Security Culture Mediates the Relationship between International Security Standards and Organizational Performance

There are information security breaches and thus organizations were required to comply with ISO 27001: 2005 requirements in order to reduce the threat of successful information security breaches and inspire confidence in investors and users (Huang et al., 2010; Akinsuyi, 2009). This study shows that security culture enables compliance to international security standards thereby improve organizational performance. Thus, H9.1 was accepted.

6.4.3 Information Security Culture Mediates the Relationship between Perceived Government Rule and Regulations and Organizational Performance

The development of information security legislations in the Nigerian banking system is not fully integrated into the international financial system. Information security standards remain stagnant in some part of the country (NDIC 2009, CBN Annual Report, 2009, Akinsuyi, 2009). Hence, the collaboration of NDIC and CBN to combat the problem of information security breaches in Nigeria is paramount. This study introduced perceived

government rule and regulation as variable. Unfortunately, information security culture does not mediate between PJRR and OP. Thus, H9.2 was rejected.

Perceived government rules and regulations propel the willingness of the management and staff on security matters. This, in turn, forces the bank to establish good information security governance, internal control and security measures.

6.4.4 Information Security Culture Mediates the Relationship between Information Security Awareness and Organizational Performance

The previous researchers discovered that security awareness through training has been considered as a factor of ISC effectiveness (Von Solms, 2000; Dominguez, 2007). This study hypothesized that information security culture mediate between organizational performances and IS practices by the important role of information security culture in improving the relationship between organizational performance and ISA, which is found to be statistically significant. Hence, this hypothesis H9.2 was supported.

6.4.5 Information Security Culture Mediates the Relationship between Information Security Policy and Procedure and Organizational Performance

For the mediating effect of the study, evidence from regression analysis provides support for Hypothesis H8.2 where it is shown that information security culture significantly mediates the relationship between information security policy and organizational performance. This implies that organization provides policies and procedure to be followed by employees when issue of information security is concerned (Hone & Eloff, 2003). The finding in this study shows that information security policies were significant

in the banking industry in Nigeria. Therefore, security policies avails employees to be familiar with the rules and regulations guiding the protection of an organizational asset (information). Hence, the ISPP significant in this study was incoherent with Von Solms (1999).

6.4.6 Information Security Culture Mediates the Relationship between Perceived Information Security Threats, Risk and Vulnerability and Organizational Performance

Considering the perceived information security risk, threat and vulnerabilities , the result from the regression analysis on the hypothesis H8.3 shows that the respondents from the banking industry shows that their views are positively significant. This implies that information security, threat, risk and vulnerabilities is to avert unforeseen occurrence to information security availability, integrity and confidentiality and as well hinder organization to gain a competitive edge in this computer age (Brown & Heywood, 2006; Hong et al. 2003; Kankanhilli et al., 2003). The result further supports Von Solms (1999, 1998, 1997), which says that there should be an ‘inter- organizational reporting and investigating scheme’ in any given system. Hence, comprehensive risk analysis needs to be taken for effective security culture practices.

Moreover, the regression result on the hypothesis H8.3 indicates that information culture mediates the relationship between organizational performance and information security threat, risk and vulnerabilities. This shows the effect of information security culture on the establishment of culture within the organization. Akinsuyi (2007) emphasized the need for top managers to investigate risk assessment. Kwok & Dennis (1999) developed a

security model in their study for national Australian banks' risk analysis where cross references were stipulated. Also, it serves as auditing confirmatory tools in implanting organizational standards.

6.4.7 Information Security Culture Mediates the Relationship between Perceived Training Programs and Organizational Performance

Furthermore, absence of security awareness through perceived training programs indicates that employees will not be familiar with information security, neither will employees know how to prevail over security threats and risks within the organization. (Al-Awadi & Saidani, 2010; Zakaria, 2007; Von Solms, 1999). Thus, information security awareness enhances employees' approaches to information security.

The Computer Security Act of 1987 urged organizations and federal agencies to provide awareness to users of information system. In other words, creating training programs enable employees to have knowledge of the risks involved and how to avert it. Therefore, based on findings of this study, practitioners in Nigerian banking demonstrated that perceived training and is significantly relevant to the organizational performance. Although, there is no literature concerning the mediating effect of information security culture on the relationship between perceived training programs and organizational performance, but evidence from this study provides that information culture mediates the relationship between perceived training programs and organizational performance. Thus, the effect of information security culture will assist in the implementation of training programs that will improve performance in the banking sector.

6.4.8 Information Security Culture Mediates the Relationship between Perceived Top Management Support and Commitment and Organizational Performance

For the mediate effect of information culture on the perceived top management support and commitment, and organizational performance, the empirical evidence from regression results show that the information security culture does not mediate the relationship between top management and organizational performance. This is in inconsistency with Kajaya, Anuila, Varonen, Savola and Röning (2006). Their study concluded that there is lack of management support because of the belief that the top management does not need to be taught of information security. In such a phenomenon where top management fails to appreciate the establishment of information security culture towards organizational performance, the consequences of the organizational business activities may be daunted (Kajaya et al., 2006). Hence, top management in the Nigerian banking sector needs to be encouraged and motivated when the issue of information security arises.

6.4.9 Information Security Culture Mediates the Relationship between Motivation of Employee and Organizational Performance

This study introduced motivation of employees in the framework in the study as part of the determinant of organizational performance. The result highlight that information security culture mediate the relationship between organizational performance and motivation of employee. Employees within the organization setting need to be familiar with information security culture in order to know how to prevail over it as well manage

information system appropriately, Anything short of this will truncate security management that will improve OP (William, 2006; Von Solms, 1999; Zakaria, 2007).

The Computer Security Act of 1987 urged organizations and federal agencies to provide awareness to users of information system. In other words, creating awareness will enable employees to have knowledge of the risks involve and how to avert it. The finding of this study shows that motivation of employee is found to be significant. Thus, in the Nigeria context, bank officials should be acquainted with risks aversion through information security awareness and enact policy that will compel banks and information security culture in the organization.

6.4.10 Information Security Culture Mediates the Relationship between Perceived Job Roles and Responsibilities and Organizational Performance

This study introduced perceived job roles and responsibility and hypothesized that the relationship between organizational performance and perceived job responsibilities is mediated by information security culture. Perceived job roles and responsibilities are introduced in order to contribute to the body of knowledge in this study. It plays vital role in how information security activities are carried out within the organization. Thus, the results show that hypothesis H9.7 is statistically significant. This is to confirm that in the Nigerian banking sector, the role of job responsibilities is imperatives in establishing information security culture and in turn improve organizational performance. Previous researchers opined that job responsibilities enables easy allocation of employees' task (Toval et al., 2002; Bjorck, 2001 & Sami Abu-Zineh, 2006). Nevertheless, the result

indicates that information security culture mediate between organizational performance and perceived job roles and responsibilities. Thus, H9.7 is statistically supported and accepted.

6.6 Summary

This chapter elaborated the discussion of the findings on data obtained from the survey. The respondents' response was at 65.6% which is commendable. Also, the non response and the descriptive of the respondents profile and hypotheses testing were thoroughly discussed. In conclusion, the multiple regressions and the hierarchical regression for the mediating variable as well discussed in detail. The next chapter is dedicated for the conclusion of the study.

CHAPTER SEVEN

SUMMARY AND CONCLUSION

7.1 Introduction

This study examined the determinant of information security practices using TOE model and information security culture as a mediating variable. This chapter discusses the conclusions of the findings. Nevertheless, this chapter discusses the conclusions of the research, theoretical and managerial contributions of the study and the research limitations. Lastly, the study makes suggestions for future research in the area of information security culture.

7.2 Summary

This study examined the determinant of information security practices in the Nigerian banking sector. The banking practitioners' involvement in human factors failures, unethical and potential fraudulent activities in post consolidation reform within the banks is pervasive. Corporate governance and information security culture failed when management executives enriching their pockets at the detriments of the stakeholders insecure assets and resources (Elchangar, 2012; NCM, 2009; Owolabi, 2007; SOX, 2002). The Central Bank of Nigeria governor in 2005, in response to the downturn in the banking sector requested for banks' mergers and acquisition and information security culture that will produce a better performance (Sanusi, 2011). The results of the study

indicated that information security culture was not adequately established and thereby implementation was not properly achieved.

By and large, to assist Nigerian banks, this study developed two questions, firstly, what are the determining TOE factors that are capable of establishing an effective information security culture towards organizational performance. Secondly, does organizational culture mediate the relationship between organizational factors and organizational performance? To answer these two questions, a model and research hypotheses were formulated. The study employed questionnaires for data collection from the respondents to know their view on the establishment of information security culture in the Nigerian banking industry. The data collected was evaluated using SPSS 18. The researcher tested the relationship between information security cultures with TOE variables using multiple regression analysis.

Also, hierarchical regression was used to analyze the mediating effect of information security culture on TOE factors and organizational performance. The study suggested perceived technology advancement, international security standard, perceived government rules and regulations, information security awareness, information security policy, perceived information security threat, risk and vulnerabilities, perceived training programs, perceived top management support and commitment, motivation of employee, perceived job roles and responsibilities. The finding indicated that perceived technology advancement, perceived information security threat, risk and vulnerabilities information

security policy, motivation of employee, perceived training programs, perceived job responsibilities are factors that influence organizational performance while other variables were not statistically significant.

On the other hand, information security culture mediates the relationship between information security awareness, information security policy and procedure, perceived training programs, perceived information security threat, risks and vulnerability, motivation of employees; and perceived job roles and responsibilities and organizational performance while other variables were found not to be significant.

7.3 Research Contributions

Obviously, in a unique research of this nature, there are bounds for contributions to the body of knowledge, the managerial implication to the banking industry, policy makers especially the Central Bank Nigeria governing council, the shareholders as well as the stakeholders. This is dealt with in subsections 7.3.1 - 7.3.3.

7.3.1 Academia

The research findings of the factors influencing information security culture to the achievement of organizational performance in the Nigerian banking sector are visible in the body of knowledge, especially with reference to the field of Accounting Information System (AIS) The relationship of the TOE factors and information security culture will be an added advantage to the body of knowledge. Secondly, the possibility of expanding

TOE factors and information security culture in other areas is another value added to the field of AIS. Although, studies of such from developing countries like Nigeria to the best of the researcher's knowledge were very few where norms and value, culture and geographic phenomena are different from that of developed countries.

This research provides evidence of a strong positive association between information security culture practice and TOE factors. The indication is that the TOE factors have a considerable influence of information security practices on organizational performance. It serves as avenues for few literatures to be present in this perspective. Using information security culture as a mediator in this study has introduced a new dimension to the study of information security systems. It also provides security awareness to users in other industries such as insurance, engineering, agriculture and manufacturing companies. This research could be a precursor for new studies. In addition, the research will provide feedbacks on the effectiveness and establishment of information security culture. Thus, improve organizational performance. Additionally, the introduction of new variables during analysis of the data collected. Such variables like information security assessment and information security culture posited that organizational performance through establishment of information security can be measured by employees' rewards and compensations which have not been measured by previous researchers especially in the Nigerian context.

Also, this study introduces information security culture as a mediating variable as well. This offers empirical support that information security culture significantly mediates the

relationship between organizational performance and organizational factors. Organizational culture was found during data analysis. This is in agreement with previous scholars, who argued that information security is embedded in organizational culture and moreover, they are interrelated (Ramachandran et al., 2008; Zakaria, 2007; Andress & Fonseca, 2000; Vom Solms, 2000; Dhillon, 1997). In turn, the importance of information security culture cannot be underestimated.

7.3.2 Managerial Contributions

The empirical evidences indicate that this study have contributed significantly to the management practice in three ways namely: (1) the study unveil the fact that adequate information security practices could be transformed into activities, while activities becomes routine, routine become norm and eventually norms becomes culture, ultimately improve organizational performance. (2) Also, the study unveil the fact that adequate information security practices could be transformed to activities, while activities become routines, routine become norms and eventually norms become culture. Thus, these information security activities improve organizational performance.

The empirical evidence of this study indicates that information security activities are positively related to organizational performance . Hence, it is imperative for the managers in the organization to establish information security culture for better performance. In addition, the results of the findings present an avenue for the managers to employ information securities practices by creating a secure environment with adequate information security awareness, motivate employee and appropriate management support

and commitment to enhance organizational performance.

7.3.3 Practical Contributions

Information security governance (ISG) is used to determine the implementation of relevant TOE on establishing an information security culture. Secondly, the study used the appropriate TOE in evaluating information security culture within the organization. Thus, improve organizational objectives, and practices in the banking sector in securing information assets. The finding of this study revealed further that there is a positive relationship between perceived technology advancement and organizational performance. This means that practitioners in the banking sector will be able to gain competitive advantage in the global world (OECD, 2005).

Secondly, the empirical evidence of this study provides that PTA, ISS, ISA, PTP, ISTRV, ISPP, MOE and PJRR are the significant determinants of the organizational performance. This indicates that practitioners must endeavor to inculcate PTA, ISS, ISA, PTP, ISTRV, ISPP, MOE and PJRR. Hence, PTA, ISS, ISA, PTP, ISTRV, ISPP, MOE and PJRR are the tools of information security development which will propel a risk reduction in the organization.

The establishment of information security practices as activities - routine- norms and eventually become culture in the organizational policy and procedural schemes using PTA, ISS, ISA, PTP, ISTRV, ISPP, MOE and PJRR enables organizational performance attainment through information security practices within the organization. Due to the fact

that information security practices needs to be supported by top management, the mediating role of information security culture is becoming increasingly important in the study of information security practices. This will enable the practitioners to obtain empirical data on employers' insight of the status of information security culture. In other words, they will obtain information that could lead to focus and support of company leaders in information security activities.

7.4 Limitation of the Study

There is no study that is empirically tested that contributed to both theoretical and managerial aspect of information security practice without one or few limitations. Therefore, this study is not an exemption. The focus of this study, which is banking sector, indicates a limitation to this research. Other sectors such as insurance, manufacturing, agriculture sector, higher education, etc could provide a new avenue for validation. This study did not take into account of insurance sector in all the thirty six states of the federation due to the insecurity and threats of Boko-haram¹ activities during the time of the research. Also, the geographical location is another limitation that influences perception; there is a tendency for the respondents to view the establishment of information security culture practices as a factor that can enhance organizational performance in the Nigerian banking sector differently compared with other developed countries.

Boko-haram is the political distortions to the peace of the nation Nigeria

Lastly, measurement adopted may serve as another limitation. Thus, Hair et al. (2010) posited that the best way to get significant results in mediating effect will be through the use of Structural Equation Modeling (SEM) where large sample size is involved. Nevertheless, this study follows a rigorous process to achieve its objectives. Hence, the imperative of this study is without any doubt. The TOE factors inculcated in the model of this study are not exhausted. Thus, this study has not in detail exhausted the determinants of information security practices towards achieving organizational performance. It should be well documented that no single study can utilize all the factors for the establishment of information security culture that will gear organizational performance.

7.5 Suggestions for Future Study

This study examines the influencing TOE factors of information security practices that will foster improvement in the organizational performance of the Nigerian banking sector. Other future researchers could consider the following sectors:

- Insurance Sector
- Higher Education sector
- Manufacturing sector
- The influencing factors of information security practices in Small and Medium Enterprises.
- Comparative study of information security culture on organizational performance.

On the concluding note, the findings from this study indicate that international security standard, perceived government rules and regulations were not significant due to the geographical location of Nigeria which may influence the perception of respondents in the Nigerian banks (Eseh, 2011; Alabede, 2011). Hence other researchers could investigate these variables in a different geographical region for a better result.

7.6 Conclusion

This study provides empirical evidence on the determinants of information security culture practices that will enhance organizational performance among Nigerian banks. This study is basically designed to answer three questions: (1)“What are the technological, organizational and environmental factors that influence information security culture?” (2) What is the relationship between information security culture and organizational performance and (3) “Does information security culture mediate the relationship between ‘TOE factors and organizational performance.’ The findings of this study recommend that technological, organizational and environmental factors play a significant role in the establishment of information security culture within the banking sector. The result of the mediating variable stipulated that the introduction of information security culture strengthens the aptitude of the model in the establishment of information security culture among banks in Nigeria.

However, empirical evidence from the findings of this study provides that information security culture mediates the relationship between information security practices and organizational performance. Hence, information security model that inculcates information security culture as a mediating variable is thereby recommended to enhance a better regulation.

REFERENCES

- Abu- Musa, A. (2003). The perceived threats to the security of computerized accounting information system. *The Journal of American Academy of Business*, 1(2), 9-20.
- Abu-Zineh, S. (2006) Success Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies.
- Adeleye, B C, Annansingh, F and Nunes, M B. (2000). Risk management practices in IS outsourcing: An investigation into Commercial Banks in Nigeria. *International Journal of Information Management*, 24(2), 167-180.
- Aguinis, H. (1995). Statistical Power problems with Moderated Multiple Regression in Management Research. *Journal of Management*, 1995, Vol 21(6) pp. 1141-1158.
- Aggreliki Tsohou, Spiros Kokolakis, Maria Kenryda, and Evangelos Kiountouzis. (2008). Investigating information Security Awareness. 17, 207-208.
- Ajbaclv, A., Keramati & Razmi, J. (2007) Assessing the impact of IT on Firm Performance considering the role of interesting variables: Organizational Infrastructure & Business Processes re-engineering
- Aiello, M. (2008) Social Engineering. InL. J. J. Janczewski & A.M Colarik (Eds) *Cyber Warfare and Cyber Terroism* (pp 191-198) Hersey, P.A: IGI Global.
- Aiken, L.S and West, S.G. (1991). *Multiple regression: Testing and interpreting interactions*. Newbury Park, London: Sage.
- Aiken, L. S; West, S.G. (1991). *Multiple Regression: testing and Interpreting interactions* Sage publications, The international Professional Publishers Newbury Park- London New Delhi.

- Akinsuyi. (2009). The drawing of information security legislations: What Nigerian Corporations can do to prepare. Lagos- Nigeria.
- Alabede, J.O., Ariffin, Z. Z, Idris, M. (2012). Tax service Quality and Compliance Behavior in Nigeria. Do tax Payers's Financial Condition and risk Preference play any Moderating role? *European Journal of Economic Finance and Administrative Studies*.35, 90- 108.
- Alex, R.P (2010). Criminology and Criminal Justice Research: Methods – Quantitative Research Methods, Threats to Validity, Qualitative Research Methods, Future of Research Methods in Criminology and Criminal Justice. Retrieved from <http://law.jrank.org/pages/928/Criminology-Criminal-Justice-Research>.
- Al-Awadi, k. & Saidani, M. (2010). Justifying the need for data security. *Management Plan. Information Management & Computer Security*.Vol.18 (3) pp.173-184.
- Allison, P. (1999). Multiple Regression. A primer. 1: Pine Forge Press.
- Alnatheer, M. & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Proceedings of the 7th Australian Information Security Management Conference*, Perth, Western Australia.
- Alshawaf, A.H.,Ali, J.M.H & Hassan,M.H.(2005).A benchmarking framework for Information systems management issues in Kuwait. *Benchmarking: An International Journal*, Vol. 12(1), 30-44.

- Ashenden, D. (2008). Information security management: A human challenge?
Information Security Technical Report, 13, 195-201.
- Anderson, R.J (2008) Security Engineering. A Guide to Building Dependable Distributed Systems (2nd Ed.) new York: Wiley.
- Andress, M. (2000) Manage people to protect data . InfoWorld Vol.22 (46).
- Appari, Ajit & M. Johnson, Eric (2010) Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management, Vol. 6, No. 4.*
- Armstrong, J. & Overton, T.S. (1977). Estimating non-response bias in mail surveys. *Journal of Marketing Research*, 4, pp.396-402.
- Armstrong, C. & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: the influence of senior Leadership and IT infrastructures System Research 10(4), 304-327
- Babatunde, D. A. & Selamat, M.H. (2012a). Investigating information security and its Influencing factors in Nigerian bank Industry: A conceptual model. *International Journal of Social Science Economics and Arts*.Vol.2 (2).
- Babatunde, D. A. & Selamat, M.H. (2012b). Determining Factors Influencing Information Security Management in the Nigerian banking and Insurance Sector: A Literature Review. *Journal of Business and Economics*, USA.Vol.3 (6), December, 2012
- Babbie, E. R. (1990). Survey Research Methods, Wadsworth, Belmont Retrieved on 16th April,2012fromwww.cordaps.edu.pk/Download/QuantitativeMethodandSurveys.doc.

- Badamas, M. A (2008). Critical issues in the management of information systems in Nigeria: An empirical study. *International Journal of Business Information Systems*, 3(1) 63 - 72.
- Baron, R. M. & Kenny, D. A. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic and Statistical Consideration. *Journal of Personality and Social Psychology*. 51(6),1173-1182.
- Barlett, J. E., Kortlik, J. W. & Higgings, C.C. (2001). Organizational research: Determining appropriate sample size in survey research. *Journal of Information Technology, Learning and Performance*, 19(1), 43-50.
- Bartlett, M. (1954). A note on multiplying Factor for Various Chi-Square approximations *Journal of the Royal Statistical Society* 16 (series B), 256-298.
- Beech, N. (2008). Research Methods [Lecture notes]. Leeds Metropolitan University.
- Bennett, J. A. (2000). Focus on Research Methods Mediator and Moderator Variables in Nursing Research: Conceptual and Statistical Differences.
- Besnard, D. & Arief, B. (2004) Computer Security Impaired by legitimate Users. *Computer and Security* pp 253-264.
- Bjorck, F. (2001). Security Scandinavian Style: Interpreting the Practice of Managing Information Security in Organizations. (Doctoral dissertation, Stockholm University and Royal Institute of Technology, 2001).
- Blackwell, E. (1998). Building a solid foundation for intranet security. *Information Systems Management*. Spring 15(2): 26-34

- Boss, S. R., & Kirsch, L. J. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines," in International Conference on Information Systems, Montreal, 2007, pp. 1-18.
- Briney, A. (2001). 2001 Survey Information. *Information Security Magazine*, October, 34-37.
- Brotby, K. (2009) Information Security Governance: A practical Development and Implementation Approach. John Wiley & Sons Vol.53, 220.
- Bruce, L. (2003). Information security – key issues and developments. Retrieved from www.pwcglobal.com/jm/images/pdf/Information%20Security%20Risk.pdf.
- Bourque, L.H.,& Fielder, E.P.,(1994) how to conduct self-administered and mail survey London, SAGE Publications.
- British Standards Institute (1993), BS 7799: Code of Practice for Information Security Management (CoP), PD0003, British Standards Institute, UK.
- BS7799-1 (1999), Information Security Management – Part 1: Code of Practice for *Information Security Management*, British Standards Institute, London.
- BS7799-2 (1999), Information Security Management – Part 2: Specification for Information Security Management System, British Standards Institute, London.
- Bowden, J. (2000). Security policy: What it is and why the basic? DTI, The Business Managers guide to information security. Retrieved from <http://www.dti.gov.uk/2000>
- Brown, M., & Heywood, J. S. (2005). Performance appraisal systems: Determinant and change *British Journal of Industrial Relations*,. 43(4), 659-679.

- Bruno L.F. & Sousa, J.O. (2009). *Organization Culture: How to measure it*. Dom Cabral Foundation Nova Lima, Brazil .
- Brutis. (2006). National Population Commission. Nigeria.
- Brynjolfsson, E., Malone, T.W., Gurbaxi ,V., and Kambali, A. (1994). Does information technology lead to smaller firms?. *Management Science* 40(12), 1628-1644.
- Bryman, A. & Cramer, D. (2001). *Quantitative Data Analysis with SPSS Release 10 for Windows: A Guide for Social Scientists*. East Essex: Routledge.
- Buono, A.F., Bowiditch, J.L & Lewis, L.W (1985) When Culture Collides: The anatomy of a merger. *Human relations* 38 (5) , 477-500.
- Coakes, S. J & Ong, C.(2011) *Analysis without Anguish.SPSS version 18.0 for Windows*
- Caby, E. C., Pautke, R. W., and Redman, T. C. (1995). Strategies for improving data quality.*Data Quality*, 1(1), 4-12.
- Cameron, R. (1972). *The banking and economic development: Some lessons of the history*. New York: Oxford University Press.
- Cavana, R. Y., Delahaye, B. L, & Sekaran, U. (2001). *Applied business research: Qualitative and qualitative methods*. Singapore: Markono Print Media Limited.
- Cameron, R. (1972). *Banking and Economic Development: Some Lessons of History*. New York: Oxford University Press.
- Chan, M., Woon, I. & Kankanhalli, A. (2005) perception of IS at the workplace: Linking Information Security Climate to Complaint behavior, *Journal of information Privacy and Security* 1 (3), 18-42.

- Chang, S.H. & Ho, C.H. (2006). Organizational factors to the effectiveness of implementing Information Security Management. *Institute of Management & Data Science*, Vol. 106 (30), 345-361.
- Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management and Data Systems*, 107(3), 438-458.
- Chang, P.Y.K & Tam, K.Y. (1997). Factor adopting the open systems: An exploratory study. *MIS Quarterly*, 21(1), 1-21.
- Cohen, D. & Crabtree, B. (2006). Qualitative research guidelines project. Princeton NJ: Robert Wood Johnson Foundation. Retrieved from <http://www.qualres.org/h>.
- Cohen, J., Cohen, P; West S.G & Aiken,L.S. (2003). *Applied Multiple Regression/Correlation For the Behavioural Science* (3rd ed.) Lawrence Erlbaum Associates Publishers London.
- Cooper, D.R. & Schindler, P.S. (2003). *Business research Methods* (8th ed.) Boston: MA: McGraw-Hill.
- Connolly, P.J. (2002) Security start from within, *InfoWorld*, Vol. 22 (28).
- Cormack, A. (2001). Do We Need a Security Culture? *VINE*, 31(2), 8-10.
- Cortina, J. M. (1993). What is coefficient Alpha? An Examination of Theory and Application Vol.78(1). *Journal of Applied Psychology*.
- Cramer, D. (2003). *Advanced Quantitative Data Analysis*. Open University Press: Maidenhead Philadelphia.

- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16 (3), pp. 297-334.
- Cronbach, L. J. & Richard J. S. (2004). My Current Thoughts on Coefficient Alpha and Successor Procedures. *Educational and Psychological Measurement* 64(3) pp. 391-418.
- Chen C.C., Medlin, B.D & Shaw, R.S. (2008) A Cross-sectional Investigation of Situational Information Security Awareness programs.
- Churchill, G. A., Jr., & Brown, T. J. (2004). *Basic marketing research* (5th ed.). Sydney: South-Western College.
- David, (2002). Policy enforcement in the workplace, *Computers & Security* Vol. 21(6), pp.506-513.
- Deal, T. E. & Kennedy, A. A. (1982). *Corporate Cultures*. Addison-Wesley, MA.
- Devlin & Meyerson. (2001). Poor IT planning team organizational Structure especially in highly Complex Organization such as academic Institutions.
- De Guinea, A.O.; Kelley, H.; & Hunter, M.G. (2005). Information Systems Effectiveness in Small Business: Extending a Singaporean Model in Canada. *Journal of Global Information Management*, 13(3), 55-70.
- Deloitte (2007) 2007 Global Security Survey. The shifting Security Paradigm. Deloitte Touche Tohamatsu.
- DeLone, W. & McLean, E. (1992). Information system success: The quest for the dependent variable. *Information Systems Research*, 3(1), 60-95

- Denscombe, M. (1998) *The good research guide for small-scale social research projects*. 1st Ed. Buckingham, Open University Press
- Denscombe, M. (2003) *The good research guide for small-scale social research projects*. 4th Ed. Buckingham, Open University Press
- Denscombe, M. (2010) *The good research guide for small-scale social research projects*. 2nd Ed. Buckingham, Open University Press
- De Vaus, D. A. (1986) *Survey in Social research* (4 Ed.) London UCL Press Ltd, London.
- De Vaus, D. A. (2011) *Research Design in Social Research*. Sage Publication Ltd, London.
- Dhillon, G. & Torkzadeh, A. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, 293-314.
- Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security*; Vol.20, No.2, pp.165-172.
- Dhillon, G., & Backhose, J. (2001). Current directions in IS security research: towards socio organizational perspectives. *Information Systems Journal*, 11(2), 127-53.
- Dhillon, G., & Moores, S. (2001), Computer crimes: Theorizing about the enemy within. *Computers & Security*, 20 (8), pp.715-723.
- Dillman, D.A. (1978) *Mail and telephone survey. The total design method*. New York: John Wiley & Sons.

- Dhillon, G. (2007). Principles of information systems security. NJ: John Wiley & Sons.
- Dinev, T. & Hu, Q. (2007). The centrality of awareness in the formation of user behavior intentions towards preventives technologies in the context of voluntary use. *Journal of the AIS*, 8(7), 386-408.
- Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2001) Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia.
- Domínguez, C.M.F. (2009). Risk reduction by implementing security awareness programs in Puerto Rico metro area companies. (Doctoral dissertation, Universidad del Turabo Gurabo, Puerto Rico, 2009). Retrieved from ProQuest Database (UMI 3412026).
- Dwived, Y.K. (2007). Consume adoption and usage of broadband. IRM Press.
- Dwived, Y.K., Choude, J., & Brinkman, W. P. (2006). Development of a survey instrument to examine consumer adoption of broadband. *Industrial Management & Data Systems*, 106(5), 700-718.
- Easterby-Smith M., Thorpe R. & Lowe A. (1991). Management research: An introduction. London: Sage Publications Limited
- Ehikamenor, F.A, (2003.) Information technology in Nigerian banks: The limits of Expectations. *Information Technology for Development*, 10, 13–24. Retrieved from <http://itd.ist.unomaha.edu/Archives/44.pdf>.
- Elbanna, S. & Chidi, J. (2007) Influence on Strategic Decision Effectiveness, Development and test of an Integrative Model. *Strategic Management Journal* 28, 431-453

- Elchangar, H., Bouladour, B., Makoudi, M. & Regragui, B. (2012) information Security, 4th Wave, journal of Theoretical Applied information Technology. Vol 43 (1)
- Eloff, J. & Eloff, M. (2003). Information security management: A new paradigm. ACM, Proceedings of SAICSIT 2003, pp.130-136.
- Eloff, M., M., & Solms, S., H. (2000). Information Security management: A Hierarchical Approach for various frameworks. *Computer & Security*, 19(3), 243-256.
- Elky, S. (2006). An introduction to information System Risks Management. SANS, Institute.
- Ernst & Young (2007) 10th Annual Global Information Security Survey. Achieving a Balance of Risk and Performance. Ernst and Young.
- Emeka, R.O. (2009). A critical evaluation of the role of the Central Bank of Nigeria in ensuring corporate governance in Nigerian banks post consolidation. Retrieved from <http://ssrn.com/abstract=1509454> or <http://dx.doi.org/10.2139/ssrn.1509454>.
- Emery, J., Crump, C. & Bors, P. (2003). Reliability and Validity of Two Instruments Designed to Assess the Walking and Bicycling Suitability of Sidewalks and Road. Vol. 18(1). *American Journal of Health Promotion*.
- Eruh, O.L. (2011). The Moderating Effect of Location and Culture on the Relationship between Individual Determinants, External Factors and Firm Characteristics on Entrepreneurial Performance. UUM Thesis, Kedah-Malaysia.
- Farahm, F., Shamkant, B. N., Gunter P.S. & Philip H.E. (2003). Managing vulnerabilities of information systems to security incidents. ACM, 2003.

- Fauzi, H., & Idris, M. (2009). The relationship of CSR and financial performance: New evidence from Indonesian companies. *Issues in Social and Environmental Accounting*, 3 (1), 66-87.
- Fauzi, H., (2010). Corporate social performance and financial performance of Indonesian Firms. (Unpublished doctoral thesis). Universiti Utara Malaysia.
- Ferguson, A. (2005) Fostering email security awareness: The West point Carronade. *Edu Cause Quarterly* 28 (1) 54-57.
- Fill, C & Visser, E (2000). The outsourcing dilemma: A composite approach to the make or buy decision. *Management Decision*, 38(1), 43-50.
- Finne Thomas. (1998). A conceptual Framework for information security management. *Computer & Security Volume* (Issue), 303-307.
- Flynn, N.L. (2001). The E-policy handbook: Designing and implementing effective email, internet and software policies. New York, NY: American Association.
- Teong, S.Y. (1999). Effect of End User Personal and Systems Attributes on Computer Based Information System Success in Malaysian SMEs. *Journal of Small Business Management*, 37(3), 81-87.
- Frazier, P.A, Barron, K.E & Tix, A. (2004). Testing Moderator and Moediator Effect on Counselling Psychology Research. *Journal of Counselling Psychology* 51(1), 115-135. <http://dx.doi.org/10.1037/0022-0167.1.115>.
- Fried, L. (1994). Information Security and New Technology Potential Threats and Solutions. *Information Systems Management*, 11 (3): 57-63.

- Friedman J.N.,Goldman, R.D.,Srivasta, R., & Parkin, P.(2004) Development of a Clinical Dehydration Scale for Use in Children Between 1 And 36.Month of Age.
- Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of information security breaches. *Information Management and Computer Security*, 11(2), 74–83.
- Gay, C. E., & Essinger, J. (2000). *Inside Outsourcing: The Insider’s Guide to Managing Strategic Sourcing*. London: Nicholas Brealey Publishing.
- Gay, L.R.& Diehl, P. L. (1996). *Research methods for business and management*. (international ed.). Singapore; Prentice hall International Inc.
- Gebrasilase, T. & Lessa, L. (2011) Information security culture in public hospitals.The *African Journal of Information Systems, Volume 3, Issue 3, 2011*.
- Ghobadian, A. & Gallear, D. (1997). “TQM and organization size” *International Journal of Operations & Production Management, Vol. 17 (2)*, pp. 121-63.
- Glaser, F. & Pallas, B. (2007). Information security as organization internal control.
- Gragg, D. (2002) A multi- level defense against social engineering. White paper, SANA Institute.
- Grainger-Smith, N. & Oppenheim, C. (1994). The role of information systems and technology (IS/IT) in investment banks. *Journal of Information Science*, 20(5), 323–333.
- Gray, G.M & Ropeik, D. P (2002) Dealing with the danger of fears. The role of risk communication. *Health Affairs* 21, 106-116.
- Gonzalez, J. & Agata S. (2002). A framework for human factors in information security.

Paper presented at The 2002 WSEAS, International Conference on Information Security, Rio de Janeiro.

Gonzalez, R., Gasco, J. & Llopis J. (2009). Information systems outsourcing reasons in the largest Spanish Firms. *International Journal of information management*, 25(2), 117-136.

Gonzalez, R., Gasco, J. & Llopis J. (2006). Information systems outsourcing: a literature analysis. *Information and Management*, 43(7), 821-834

Gonzalez, R.; Gasco, J & Llopis, J. (2010). "Information Systems Outsourcing. Reasons and Risks: a new assessment. *Industrial Management & Data System* Vol. 110 (1), pp. 284-303.

Gonzalez, R.; Gasco, J & Llopis, J. (2005b) "Information Systems Outsourcing Risks: a Study of Large Firms", *Industrial Management & Data Systems*, Vol. 105 (1), pp. 45-62.

Goodhue, D.L. & Straub, D. W. (1991). security concerns of system users: a study of Perception of the adequacy of security. *Information & Management*. Vol. 20(1), 13-27.

Gupta, V.G, & Gupta, A. (2005). Outsourcing the IS function: Is it Necessary for your Organization?. *Information systems management*, 9(3), 44-50.

Gupta, A. & Hammond, R. (2005) Information security issues and decision for small business. *Information Management & computer security* 13(4), 297-310.

- Gupta, A. & Hammond, R. (2007). Information security management: factors that influence its adoption in small and mid-sized businesses. *Journal of Information Security System and Technology Management*, Vol. 4(30,2007,pp.375-397.
- Gibbs, J.L. & Kraemer, K. L., (2004). A Cross-country investigation of the determinants of the scope of e-commerce use: An institutional approach. *Electronic Market* 14(2), 124-137.
- Guildford, J. P. (1973). *Foundamental Statistics in Psychology and Education*, 5th edition
Newyork: McGraw-Hill.
- Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. (1998). *Multivariate Data Analysis: A global perspective. (7th ed.)*. USA: Pearson Education Inc.
- Hair, J.F., Black, W.C., Babin, B. J & Anderson, R. (2003). *Multivariate Data Analysis. (5th ed.)*. London: Prentice Hall.
- Hair, J.F., Black, W.C., Babin, B. J, Anderson, R. & Tatham, R.L (2006). *Multivariate Data Analysis. (5th ed.)*. London: Prentice Hall.
- Hair, J.F., Black, Mony, A. H., Samuel, P. & Page, M. (2007). *Research methods for business*. England: John Wiley & Sons limited.
- Hair, J.F., Black, W.C., Babin, B. J, Anderson, R.. (2010). *Multivariate Data Analysis. (7th ed.)*. Upper Saddle River, N.J: Pearson Prentice Hall.
- Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.

- Hellriegel, D., Slocum, J.W. & Woodman, R.W. (1998). *Organizational Behavior*. 8th Ed: South-Western College Publishing.
- Hinde, S. (2002). Security survey spring crop. *Computer & Security*, 21(4), 310-321.
<http://ujdigispace.uj.ac.za:8080/dspace/handle/10210/292>; viewed on Sept. 5, 2009
<http://www.is2.lse.ac.uk/asp/aspecis/20070041.pdf> (Accessed April 14, 2013).
- Hill, M. (1999). Technology investment in business banking. *Journal of Lending and Credit Risk Management*, 81(6) 30–35.
- Hoffman, T., (1998). Winning weapon. *Computerworld*, 1998, 17–20.
- Holmbeck, G. N. (1997). Toward Terminological, Conceptual, and Statistical Clarity in the study of Mediators and Moderators: Examples From the Child-Clinical and Pediatric Psychology Literatures, *Journal of Consulting and Clinical Psychology*, 95(4), 599-610.
- Hinson, G. (2003). Human factor in information security. 2003, ISecT Ltd.
- Hone, K. & Eloff, J.H.P (2002). Information security policy what do international information security standards say?. *Computers Security*, 21(5), 402-409.
- Hong Kwo-shing, Yen-Ping Chi, Louis R. Chao & Jih-Hsing Tang (2003). An integrated System theory of Information Security Management. *Information Management & Computer Security*, 11(5), 243-248.
- Hoffer, J.A. & Straub, D.W. (1989). The 9 to 5 underground: are you policing computer crimes?, *Sloan Management Review*, Vol. 30 No. 4, pp.35-43.
- Hong Kwo-shing, Yen-Ping Chi, Louis R. Chao & Jih-Hsing Tang (2003). An Integrated System theory of Information Security Management. *Information & Management Computer Security*, 11(5), 243-248.

- Hurt R.L (2008) *Accounting Information System: Basic Concepts and Current Issues*. Boston: McGraw-Hill, Inc.
- Hu, Q., Hart, P. & Cooke, D. (2006). The role of external influences in organizational Information security practices: An institutional perspective. *Journal of Strategic Information System*, 16(2), 153-172.
- Huang, D.,Rau, P.P & Salvendy , G. (2007) Survey of Factors Influencing People's Perception of Information Security. INJ (Ed.) *Human-Computer Interaction, Part Iv*. Heidelberg: Springer.
- Iacaovou, C. L, Benbasat, I, & Dexter, A. S., (1995). Electronic data Interchange and small organization adoption and impact of technology. *MIS Quarterly*, 19(4), 465-485.
- Igbaria, M.; Zinatelli, N.; Cragg, P. B., & Cavaye, A.L. (1997). Personal computing acceptance factors in small firms: A structural equation model. *MIS Quarterly*, 21(3), 279-305.
- Ighomwenghian, K., (2010). Daily Independence Newspaper, Lagos- Nigeria.
- Im, G., & Baskerville, R. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *The Database for Advances in Information Systems*, 36(4), 68-79.
- Ismail N. A (2008). Information technology governance, funding and structure: A case analysis of Public University in Malaysia. Information Reading Room. *SANS Institute*, 25(3), 145-160.

- Ismail, N.A. & King, M. (2006). The alignment of accounting and information systems in SMEs in Malaysia. *Journal of Global Information Technology Management*, 9(3), 24-42.
- Ismail, N.A. & King, M. (2007). Factors influencing the alignment of accounting information systems in small and medium sized Malaysian manufacturing firms. *Journal of Information Systems and Small Business*, 1(1/2), 1-19.
- Ismail, N.A. (2009). Factors influencing AIS effectiveness among SMEs: Evidence from Malaysia. *The Electronic Journal of Information Systems in Developing Countries*, 38: 10, 1-19.
- ISO (2005) ISO/IEC17799 Information Technology Security Technology- Code of Practice for ISM. Second Edition 2005-06-15. Reference ISO/IEC 17799-1: 2005 (E) Pg 1-115.
- IT News Africa, (2009) ATM Removal to banking Hall Premises.
- James, L. R. & Brett, J. M. (1984). Mediators, moderators, and tests for mediation, *Journal of Applied Psychology*, 69, 307-321..
- Jarvenpaa, S.L. & Ives, B. (1991). Executive involvement and participation in Management Information Technology. *MIS Quarterly*, 15(2), 205-227.
- Juma'h, A., & Wood, W. (2000). Outsourcing implications on companies' profitability: A sample of UK companies. *Work Study*, 49(7), 265-274.
- Judd, C.M. & Kenny, D.A. (1981). Process analysis: Estimating mediation in treatment evaluations, *Evaluation Review*, 5 602-619.

- Kabay, M. E. (1996). *The NCSA guide to enterprise security*. New York, NY: McGraw Hill.
- Kabiru, J. R. (2012). A Framework of Business Process Re-engineering Factors and Organizational Performance of Nigerian Banks. *Asian Social Science Journal*, Vol 8,(4).Canadian center of science and Education.
- Kassarjian, H.H. (1977) Content analysis in Consumer Research. *Journal of Consumer Research*, 4,8-10.
- Kankanhalli, A., Teo, H-H., Tan, B.C., & Wei, K-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139-154.
- Kap-Willam, S. (2009) Employees- a Company's Greatest Asset. Retrieved from Business Management Suite 101 on 24 July, 2012
- Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). "Information systems security policies: A contextual perspective. *Computers & Security*, 24, 246-260.
- Karyda, M., Kiountouzis, E. & Kokolakis, S. (2004). Information system security policies contextual perspective. *Computer & Science*, Volume(Issue), 246-260.
- Kankanhalli Atreyi, Hock-hai Teo, Bernard C.Y.Tan, & Kwok-kee Wei. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, Volume(Issue), 139-154.
- Kaiser, H. (1974). An Index of factorial Simplicity *Psychometrika* 39(31-36).
<http://dx.doi.org/10.1007/BF02291575>.

- Kenny, M.J. (2001). Security Management Standard - ISO. *BT Technology Journal*, 19(3), 132-136.
- Kaiser, H. (1974). An index of factorial simplicity", *Psychometrika*, Vol. (39), 31-6.
- Kearns, G.S. & Lederer, A.L.(2004). The impact of industry contextual factors on IT focus and the use of IT for competitive advantage. *Information & Management* Vol.41(7),899-919.
- Krause, M. & Tipton, H. F. 2002. Handbook of Information Security CRC Management Press LLC, ISBN: 0849399475.
- Kraemer, S. & Carayon, P. (2005). Computer and information security culture: findings from two studies. Proceedings of the 49th Annual Meeting of the Human Factor and Ergonomics Society. Orlando, Florida: Human Factors and Ergonomics Society. Retrieved from <http://cis.engr.wisc.edu/docs/skhfes2005.pdf>.
- Krejcie, R. V.& Morgan, D. V. (1970). Determining Sample Size for Research Activities Educational and Psychological Measurement 1970, 30, 507-610.
- Koacich, G. (1998). Establishing an information systems security organization (ISSO). *Computer & Security*, 17, 600-612
- Knapp, J. K., Marshall, E. T., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.
- Knapp, K. J., Marshall, T.E., Rainer, R.K. & Morrow, D.W. (2004). Top Ranked Information Security Issues. Paper presented at the 2004 International Information Systems Security Certification Consortium (ISC).

- .Krause, M. & Tipton, H. F, (2002). Handbook of Information Security CRC Management Press LLC, ISBN: 0849399475
- Kruger, H.A., & Kearney, W.D.(2006). A prototype for assessing information security Awareness *Computers & security*, 25, 289–296.
- Kuan, K.L.Y. & Chau, P.Y.K. (2001). A perception-based model for EDI adoption on small business using a technology-organization- environment framework. *Information and Management*, 38(8), 507-512.
- Kwok, Lam-for & Dennis, L. (1999). Information Security Management and Modeling information. *Management & Computer Security*, Volume (Issue), 30-39.
- Lacity, M., Hirschheim, R. & Willcocks, L. (1994) “Realizing Outsourcing, Expectation, Credible Outcomes”, *Information Systems Management*, Incredible Vol. 11 (4), pp. 7-18.
- Lankford and Parsa (1999), Outsourcing A Primer, *Management Decision*, 37/4, pp.310: 316.
- Lau, Oliver. (1998). The ten commandments of security. *Computer & Security*, 17(Issue), 119-123.
- Lederer, A.L. & Gardner, V. (1992). The process of strategic information planning. *Journal of Strategic Information system*, 1(2), 76-83.
- Leidner, D. & Kayworth, T. (2006). Review: A review of culture in information systems research: towards a theory of information technology culture conflict. *MIS Quarterly*, 30(2), 357-399.

- Lee, J., & Lee, Y.(2002).“A holistic model of computer abuse within organizations,
Information Management & computer security (10:2/3), 2002, pp. 57- 63.
- Lee, S. M., Lee, S. G., & Yoo, S.(2003) “An integrative model of computer abuse based
on social control and general deterrence theories,” *Information & Management*
(41:6), 2003, pp. 707-718.
- Leidner, D.E. & Kayworth, T. (2006): Review: A review of culture in information
systems Research: Toward a theory of information technology culture conflict, *MIS*
Quarterly Vol.30, (2) pp. 357-399.
- Liang, H., Saraf, H. Hu,Q, & Xue, Y. (2007). Assimilation of Enterprise Systems: The
effect of Institutional Pressure and Mediating Role of Top Management. *MIS*
Quarterly. 31(1), 51-87.
- Lippert, S. K. (2001). An exploratory study into the relevance of trust in the context of
information systems technology. (Doctorial dissertation, The George Washington
University, Washington, D.C., 2001).
- Lippert, S.K. & Govindarajulu, C. (2006). Technology-organization-environment
antecedents to web services adoption. *Communication of IIMA*, 6(1), 146-158.
- Loh, L. & Venkatraman, N. (1992). Determinants of information technology
outsourcing: a cross sectional analysis. *Journal of Management Information*
Systems, 9(1), 7-24.
- Loh, L. (1994). An organizational- economic blueprint for information technology
outsourcing: concepts and evidence. ICIS 1994 Proceedings, 73-89. Retrieved from
<http://aisel.aisnet.org/icis1994/7/>

- Martins, A. (2000). The influence of organizational culture on creativity and innovation in a University library. M.Inf. Dissertation. Pretoria: University of South Africa.
- Matins A. & Eloff, J. (2001) Social and Ethical Aspects of Information Security.
- Martins, O. & Odunfa, A. (2012) At the 50th Information Value Chain Forum in Lagos.
- Malhotra, N. K., Hall, J., Shaw, M., & Oppenheim, P. (2006). *Marketing research: An Applied orientation* (3rd ed.). Frenchs Forest: Prentice Hall.
- Matteson, M.T, Ivancevich, J.M & Smith, S.V. (1984). Relation of type of behavior to performance and satisfaction among sales personnel. *Journal of Vocational Behaviour*,25,203-214.
- Maslow, A.H. (1997). *Motivation and Personality*, Harper & Row, New York, NY.
- MacKinnon, D. P., Warsi, G., & Dwyer, J. H. (1995), A simulation study of mediated effect measures. *Multivariate Behavioral Research*, 30(1), 41-62.
- MacKinnon, D.P., Lockwood, C.M., Hoffman, J.M., West, S.G., & Sheet, V. (2002). A comparison of methods to test the significance of mediating Analysis. *Annual Review of Psychology Methods*,7 (1), pp83-104.
- MacKinnon, D.P., Fairchild, A.J., & Fritz, M.S, (2007). *Mediating Analysis*. *Annual Review of Psychology* ,Vol.58. pp.593-694.
- Milkovich, G.T., & Newman, J. M. (1999). *Compensation*. New York: Irwin/McGraw-Hill.
- Mitchell, R.C., Marcella, R. & Baxter, G. (1999). *Corporate Information Security Management*. *New Library World*, 100 (1150), 213-227.

- Mitchell Ruth C., Rita Marcella & Craeme Baxter. (1999). *Corporate Information Security Management*, New Library World, 1999 pp 213-227.
- Mobley, W.H., Wang, L. & Fang, K. (2005). Organizational culture: Measuring and developing it in your organization. *The LINK*, Summer, 11-20.
- Mouratidis, H., Jahankhani, H., & Nkhoma, M. Z. (2008). Management versus security specialists: An empirical study on security related perceptions. *Information Management & Computer Security*, 16 (2), 187-205.
- Muhammad, M.A. (2009). The Combine Effect of Market Orientation and Owner/ Manager's Innovation and Business Performance of Small and medium Sized Manufacturing Firms in Pakistan Sintok, Kedah, Malaysia: PhD Thesis, UUM.
- Myllyot, T, R. (1995). *Computer outsourcing: Managing transfer of information systems*. Eaglewood Cliffs, N.J: Prentice Hall.
- McIvor, R. (2000). A practical framework for understanding the outsourcing process supply chain management. *An International Journal*, 5(1), 22-36.
- McKelvie, S.J. (1978). Graphic rating scale- How many categories? *British Journal of Psychology*, 69,185-502.
- Mckelvie, P.L. (1989). Accounting Systems: Past, Present and Future, *The Accounting System Journal* 1(1), 1-3.
- Meyers, L. Gamst, G. & Guarino, A., (2006). *Applied multivariate research : design and interpretation*. London: SAGE Publication.
- Miller, H. (1996). The multiple dimensions of information quality. *Information systems Management*, 13(2), 79-83.

- Miskell, J.R & Miskell, V.(1994) *Motivation at work*, Irwin,Burr Ridge II.
- Muller, D.; Judd, C.M. & Yzerbyt, V. Y. (2005). When Moderation is Mediated and Mediation is Moderated. *Journal of Personality and Social Psychology* 2005, Vol 89 (6) pp.852-863.
- Nakatani & Chang, (2005). Poor IT planning team organizational Structure especially in highly Complex Organization such as academic Institutions.
- Neil, J. (2009). *Exploring Research*. Seventh edition. New Jersey: Pearson Education International, Inc.
- Ngo, L., Zhou, W. & Warren, M. (2005) Understanding transition towards organizational culture change. *Proceedings of the 3rd Australian Information Security Management Conference*, Perth Australia.
- Nickels, W.G, McHugh, J.M &McHugh S.M (2002) *Understanding Business* 6th Edition. Boston: McGraw-Hill, Inc
- Nigerian Stock Exchange. (2010). Nigerian Stock Exchange. Retrieved on 20/03/2011 from www.nigerianstockexchange.com/.
- Nigeria, Central Bank. (2001). *Banking Supervision Annual Report*.
- Nigerian Tribune, (2011) Case on ATM Fraud.
- Nigeria, Deposit Insurance Corporation. (2002). *Annual Report and Statement of Accounts*.
- Norusis, M. J. (1999). *Guide to Data Analysis*. New Jersey: Prentice Hall.

- Noradilah, M. N., N. M. Talib, M.A., & Yaacob, S.N. (2009). Personality, Loneliness and Mental Health Among Undergraduates at Malaysian Universities. *EuroJournals Publishing, Inc.* Vol. 36 (2) pp.258-298. <http://www.eurojournals.com/ejsr.htm>.
- Nosworthy, J. D. (2000). Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? *Computers & Security*, 19, 337 – 347
- Nunnally, J. (1978), *Psychometric Theory*, 2nd ed., McGraw-Hill, New York, NY.
- Odunfunwa, M.O. (2008) Impact of Information Technology on Banking Industry *Information System Research* 12 (1).
- Ogunleye, G. A. (1999). A review of banking activities and its regulatory framework in Nigeria: The past, present and future. *NDIC Quarterly*, 9(4).
- Orchesky, C. (2003). Beyond technology - the human factor in business systems. *Journal of Business Strategy*, 24(4), 43-47.
- Owolabi, E.A. (2007). Corruption and financial crimes. Nigeria: Genesis.
- Pallant, J. (2007) *SPSS Survival Manual: A step by step guide to data analysis using SPSS for Windows (Version 15) 3rd Edition*. Australia: Allan & Unwin.
- Parker, D.B. (2002). Motivating the workforce to support security objectives: A long-Term view.
- Parker, D.B. (1984), "The Many Faces of Data Vulnerability," *IEEE Spectrum*, (May), pp. 46-49.
- Parsons, K. McCormac, A., Butavicious, M. & Ferguson, L. (2010) *Human Factors and Information Security: Individual, Culture and Security Environment*, Command, Control, Communication and Intelligence Division. DSTO Defense Science and Technology-Organization. Australia.

- Pfleeger, C.P. (1989). *Security in computing*. Englewood Cliffs, NJ: Prentice Hall.
- Peters, T. & Waterman, R. (1982). *In Search of Excellence*. Harper and Row, Sydney.
- Peltier, T. R.(2003). Preparing for ISO 17799. *Security Management Practices*.pp 21-28 .
- Peltier, T. R. (2005). Implementing an information security awareness program. *Security Management Practices*, (May/June), 37-49.
- Pironti, J. P. (2005). Key elements of information security program. *Information Systems Control Journal*, 2005 vol.1.
- Porter, M. & Millar, V. (1985). How information gives you competitive advantage. *Harvard Business Review*. July-August: 149 – 160.
- Qingxiong Ma, Johnston, A. C., & Pearson, J. M. (2008). Implementation security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, 16(3), 251-270.
- Qingxiong Ma, Schmidt, M.B., Herbenger, G.R. & Pearson, J. M. (2009). Data security issue. Information accessibility product. Review of business publisher: St John's University, *College of business Administration*.ISSN 00346454. Vol. 30 (1).
- Ramayah, T. (2011). *Developing and Testing Mediators and Mediators in Malaysia* Research School of Management, Univeristi Sains Malaysia, Penang.
- Reyes Gonzalea, Jose Gasco, & Juan Llopis.(2009). Outsourcing and information 110 (3), 325-350.
- Rahman, I. (2008). The Role of Information Technology on Banking Industry: Theory and Empirics, *Nigeria Time Book Review*, July 12 (2008).

- Peltier, T. R. 2003. Preparing for ISO 17799. Security Management Practices.pp 21-28 .
- Porter, M. & Millar, V. 1985. How information gives you a competitive advantage.
Harvard Business Review. July-August: 149 – 160.
- Ramayah, T. (2010). Developing and Testing Moderators and Mediators in Management Research. School of Management, Universiti Sains Malaysai, Minden, 11800, Penang.
- Richardson, R. (2008). CSI Computer Crime & Security Survey. Retrieved from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>
- Rotvold, Glenda (2008). How to create a Security Culture in Your Organization
- Ruighaver, A.B., Maynard, S.B., Chang, S. (2007) Organizational security culture:
- Saint-German, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*, Arma International.Vol.39 (4), 60-66.
- Samuel, Mark. (2002). Good securities policies should be second Nature. Computing, (Elsevier Science Limited).
- Sanusi, L.S. (2010, February 26). The Nigerian banking industry: What went wrong and the way forward. Lecture delivered at the Convocation Square, Bayero University, Kano, Nigeria.
- Sanusi, L.S. (2011). Banks in Nigeria and National Economic Development: A Critical review. BIS Central Bankers' Speeches, 1-6. Retrieved from <http://www.bis.org/review/r110323b.pdf>.

- Santos, J.A.R. (1999). Cronbach's Alpha: A Tool for Assessing the Reliability of Scales
Texas A&M University. Vol. 37(2), Extension Journal. Tools of the Trade2TOT3.
Retrieved from www.joe.org/joe/1999april/tt3.php on the April 18th, 2012.
- Saunders M., Lewis P. & Thornhill A. (2007). *Research Methods for Business Students*.
5th Ed. Financial Times Prentice Hall.
- Scalet, S. D. (2005). Five Steps to an Effective Strategic Plan July, 2005 Vol.4
(8). www.csoonline.com
- Schlinger, T. & Teufel, S. (2002). Information security culture: the socio-cultural
dimension in information security management. In Ghonaimy, M.A., El-Haddi, M.T.
and Asian, H.K. (eds). *Security in the Information Society: Vision & Perspectives*.
USA: Kluwer Academic, 193-201.
- Schlienger, T. & Teufel, S. (2003) 'Information Security Culture - From Analysis to
Change.' *Proceedings of ISSA 2003*, Johannesburg, South Africa, 9-11 July 2003.
- Schein, E. H. (1992): *Organizational Culture and Leadership*, 2d, San Francisco: Jossey
Bass.
- Schumpeter, J. A. (1934). *The Theory of Economic Development*. Cambridge: Harvard
University Press.
- Scott, J.E (2007) An e-Transformation Study Using the Technology–Organization
Environment Framework. 20th Bled eConference e Mergence: Merging and
Emerging Technologies, Processes, and Institutions June 4 -6, 2007; Bled, Slovenia.
- Senge, P. M. (1990). *The Fifth Discipline: The Art and Practice of the Learning
Organization*. New York, USA: Doubleday Currency.

- Sekaran,U. (2001). *Research Methods for Business: A skill-building approach*. NYC: John Willey & Sons, INC.
- Sekaran,U. Bougie, R. (2010). *Research Methods for Business 5th (ed): A skill-building Approach*. NYC: John Willey & Sons, Publication INC.
- Selamat, M.H., Dwivedi, Y. K., Abd Wahab, M. S., Samsudin, M.A., Williams, M.D., and Lal, B. (2008). Factors Affecting Malaysian Accountants' Broadband Adoption and use Behavior. Paper presented at the 14th Americas Conference on Information Systems (AMCIS,2008), Toronto, Ontario.
- Shahri, I. & Rahim, A.B (2012) Security Effectiveness in Health Information System. Through Improving human factor by Education and Training. *Australian Journal of Basic and Applied Science* 6 (12) 226-233.
- Sharma, R. & Yetton, P. (2006). The contingent Effects of Management Support and task Interdependence on Successful information Systems implementation. *MIS Quarterly*, 27(4), 533-555.
- Shadish, W. R. & Sweeney, R. B. (1991). Mediators and moderators in meta analysis: There's a reason we don't let dodo birds tell us which psychotherapies should have.
- Sheridan, J.C. & Clara, O. (2011). *Analysis Without Anguish SPSS version 18.0 for Windows*. Jon Wiley & sons Australia, Ltd.
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1), pp. 31-41.
- Sindhuja Parakkattu, & Anand S. Kunnathur. (2010). A framework for research in information security management.

- Silverman, D. (2001). *Interpreting qualitative data; methods for analyzing talk, text and interaction*. 2nd Ed. London, Sage Publication Ltd.
- Siponen, M.T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The Database for Advances in Information Systems*, 38(1), 60-81.
- Siponen, M. T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization*, 15 (2005) 339–375.
- Somoye, R. (2008). The performance of commercial banks in post-consolidation period in Nigeria: An empirical review. *European Journal of Economics, Finance and Administrative Science*, Volume(14), 62 – 72.
- Soludo, C. (2004, July 4). Consolidating the Nigerian banking industry to meet the development challenges of the 21st century. Presented at the meeting of the Bankers Committee, CBN Head Quarter, Abuja.
- Soludo, C. (2009, March 30). Banking in Nigeria at a time of global financial crisis. Presented at Special Interactive Session Eko. Hotel & Suites, Victoria Island, Lagos.
- Straub, D. W., & Nance, W. D.(1990) “Discovering and disciplining computer abuse in organizations: a field study,” *MIS Quarterly* (14:1), 1990, pp. 45-60.
- Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for positivist research communication. *Association for Information Systems*, 13(24), 380-427.
- Straub, D. W. & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly* 22(4): 441 - 469.

- Swanson, D. (2000). Secure Strategies. Retrieved at February 4, 2011 from <http://infosecuritymag.techtarget.com/articles/october00/features3.html>
- Tabachnick, B.G. & Fidell, L.S. (2001). Using multivariate statistics. (4th ed.). London: A Pearson Education Company.
- Tabachnick, B.G. & Fidell, L.S. (2007). Using Multivariate Statistics (5th ed.) (2) Pearson International Edition.
- Ta- Wei David Wong, Jackie Rees & Karthik Kannan. (2008). Reading the disclosure with new eyes: bridging the gap between information system disclosure and incidents.
- Tarimo, C. N., Bakari, J. K, Yngström, L., & Kowalski, S. (2006) A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security - The Case of Tanzania Available at:<http://www.citaseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.2850.pdf> (Accessed April 15, 2013)
- Thong, J.Y.L., Yap, C.S., & Raman, K.S. (1994). Engagement of External Expertise in Information Systems Implementation, *Journal of Management Information Systems*, 11(2), 209-231.
- Thong, J.Y.L., Yap, C.S. & Raman, K.S. (1996). Top Management Support, External Expertise and Information Systems Implementation in Small Businesses. *Information Systems Research*, 7(2), 248-267.
- Thong, J.Y.L. (1999). An Intergrated Model of Information Systems Adoption in Small Business. *Journal of Management information Systems* 15(4), 187- 214.

- Thomas, A. & Lindsay, D. (2003). Organizational culture at a South African food service company. *South African Journal of Business Management*, 34(4), 45-52.
- Tornatzky, L. G. & Fleischer, M. (1990). The process of technology innovation. Lexington: Lexington Books.
- Toval Ambrosio, Joaquin Nicolas, Begona Moros, & Fernando Garcia (2002). Requirement reuse for improving *Information Systems Security*: A practitioner's approach, requirements engineering.
- Uchendu, O. A. (1998) A Concentration in the Commercial Banking Industry in Nigeria. *Economic and Financial Review*, 40 (3), Central Bank of Nigeria.
- Von Solms, R. (1999). Information security management: Why Standards are important *Information Management & Computer Security*. 7, (1) pp. 50-57.
- Von Solms, R. (1996). Information security management: The second wave. *Information Computer and Security*, 15, 281-288.
- Von Solms, R. (1998a). Information security management: Why information security is so important. *Information Management and Computer Security*, pp. 174-177.
- Von Solms, R. (1998b). Information security management: Guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*, pp. 221-223.
- Von Solms, R. (1998c). Information security management: The code of practice for information security Management (BS 7799). *Information Management & Computer Security*, pp. 224-225.

- Von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security*, 50-57.
- Von Solms, B. & Von Solms, R. (2004). The 10 deadly sins of *information security management*. *Computer & Security* 23, 371-376..
- Von Solms, B. (2000). Information security – The third wave?. *Computers and Security*. 19(7),November: 615-620.
- Von Solms, B. (2000). Information security – The Fourth wave?. *Computers and Security*. 25 (165), 165-168.
- Van Muijen, J.J, & Koopman, P. (1999). Organizational Culture: The Focus Questionnaire, *European Journal of Word and Organizational Psychology*, 8(4), 551-568.
- Wang, R. Y., & Strong, D.M. (1996). Beyond accuracy: what data quality means to data consumers. *Journal of Management Information Systems*, 24(4), 5-34
- Wang, J.J, & Yang, D.L. (2007). Using a hybrid multi-criteria decision aid. *Computers & Operations Research*, 34(12), 3691-3700.
- Wang, H. J & Zhao, J.L. (2011) “Constraint-Center workforce change analytics” *Decision Support Systems* 13, 3. 562-575.
- Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4-19.

- Williams, P. A. (2009) What Does Security Culture Look Like For Small Organizations?
7th Australian Information Security Management Conference, Perth, Western
 Australia.
- Williams, P. (2007). Executive and Board Roles in Information Security. *Information
 Systems Control Journal*, vol.2007(8), pp.11-14.
- Willison, R.(2006)“Understanding the Perpetration of Employee Computer Crime in the
 Organizational Context,” *Information and organization* (16:4), 2006, pp. 304-324.
- Wilson, M. & Hash, J. (2003) National Institute of Standards and Technology. *NIST
 Special Publication 800-50*.
- Wood, C.C., (2008) The Importance of Defining and Documenting Information Security
 Roles and Responsibilities. *Information Shield*.
- Wright, C. (2004). Top Three Potential Risks with Outsourcing Information Systems.
Information Systems Control Journal, 5,
- Wright, M. (1999). Third generation risk management practices. *Computers & Security*,
 (2), 9-12.
- Wright, M. A. (1994). Protecting information: effective security controls. *Review of
 Business*, 16 (2): 4 – 9.
- Wright, M.A. (1998). The need for information security education. *Computer Fraud &
 Security*, (8), 14-17.
- Wulgaert, T. (2005). Security Awareness – Best Practices to Serve Your Enterprise:
 Rolling.

- Yam, J. (1998). The impact of technology on financial development in East Asia. *Journal of International Affairs*, 51(2), 539–555.
- Yin, R.K. (1989). *Case Study Research: design and methods* (Vol.5) Newbury Park,CA, Sage Publication.
- Zakaria, O. (2013) *Information Security Culture: A Human Firewall Approach*, Lambert Publishing Germany.
- Zakaria, O. (2004) *Understanding Challenges of Information Security Culture: A Methodological Issues: in Proceedings of the 2nd Australia Information Security Management Conference Perth Australia.*
- Zakaria, O. (2005) *Information Security Culture and Leadership. 4th European Conference on Information Warfare and Security .Cardiff, Wales.*
- Zakaria, O. (2007). *Investigating information security culture challenges in a public sector organization: a Malaysian case (Unpublished PhD Thesis)*
- Zedeck, S. (1971). Problems with the use of moderators variables. *Psychology Bulletin*, 26(4) 295-310.
- Zhao, J. L. & Chang, H. K. (2005). Web services and process management: A union of convenience or a new area of research. *Decision Support Systems*, 40(1),1-8.
- Zhu, K. & Kraemer, K.L. (2005). Post-adoption variations in usage and value of business by organizations cross-country evidence from the Retail Industry. *Information Systems Research*, 16(1), 61-84.

Zhu, K., Kraemer, K.L., ; Xu, S. & Dedrick, J. (2004). Information technology payoff in e-business environment: An international perspective on value creation of e- business in the financial services industry. *Journal of Management Information systems*, 21(1), 17-56.

Zhu, K., Kraemer, K.L., & Xu, S. (2003). E-Business adoption by European Firms across country assessment of the facilitators and inhibitors. *European Journal of Information Systems* 12(4), 251-268.

Zikmund, W.G. (2003). *Business Researcher Methods* (7ed.), U.S.A.: Thomas South – Western, INC.

Zikmund, W.G., Badin, B.J., Carr, J.C. & Griffin, M. (2010). *Business Researcher Methods* (8ed.), U.S.A.: Thomas South – Western, INC.