



UNIVERSITY OF
KWAZULU-NATAL

INYUVESI
YAKWAZULU-NATALI

**THREE-DIMENSIONAL SECURITY FRAMEWORK FOR
BYOD ENABLED BANKING INSTITUTIONS IN NIGERIA**

By
Ofusori Lizzy Oluwatoyin
214584651

**A thesis submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy**

**School of Management, IT and Governance
College of Law and Management Studies**

Supervisor: Dr. Prabhakar Rontala Subramaniam
January 2019

DECLARATION

I, Ofusori Lizzy Oluwatoyin, declare that

- (i) The research reported in this thesis, except where otherwise indicated, is my original research.
- (ii) This thesis has not been submitted for any degree or examination at any other university.
- (iii) This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
- (iv) This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
 - a) their words have been re-written but the general information attributed to them has been referenced;
 - b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.
- (v) Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.
- (vi) This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signature:



Date: 3rd January, 2019

DEDICATION

The research work is dedicated to the Almighty God for the wisdom, knowledge and strength to commence and conclude this study.

I also dedicate this research to my mother, Mrs. J.A Ofusori, for her moral support and encouragement.

Finally, to the memory of my father, the late Elder Michael Aiyedogbon Ofusori, may he continue to rest in the bosom of God till we meet to part no more.

ACKNOWLEDGEMENTS

I would like to acknowledge and appreciate the people who have supported and encouraged me throughout the period of my study. My profound gratitude goes to:

Dr. Prabhakar Rontala Subramaniam for his supervision. He kept the study on the right track from the beginning till the end. Through constructive criticisms and encouraging comments, he has indeed made me a better researcher.

The Acting Deputy Vice-Chancellor and Head of College-Law and Management Studies, Professor Brian McArthur and the Acting College Dean of Research, Professor Harold Ngalawa for funding my travel for data collection, conference and also for language editing. I am indeed grateful.

The Acting Dean and Head of School-Management, IT and Governance, Professor Stephen Mutula and the Academic Leader of Research and Higher Degree, Professor Isabel Martins for their support.

I also acknowledge the priceless contributions of the Academic Leader of Information Systems and Technology, Professor Irene Govender and the Administrators of the Higher Degree, School of Management, IT and Governance, - Ms Angela Pearce and Mrs Nadia Ally for their encouragement all through my study.

To my lovely mother, Mrs Janet Adelodun Ofusori, who played a vital role in kick-starting this journey. I appreciate the invaluable sacrifices, support, and prayers that she offered me throughout the period of this study.

I remained indebted to my siblings and their wives: Engr. and Dr. (Mrs) Temidayo Ofusori, Dr. and Dr. (Mrs) David Ofusori, Mr. Femi Ofusori and Mr. Benjamin Yusuf who have been very supportive all through this journey. I am indeed very grateful.

My gratitude also goes to everyone that has contributed in various ways to the success of this study: Prof Dele Oluwade, Dr. Paul Kariuki, Dr. Jude Adeleke, Dr. John Chaka,

Mr. Torkuma Kuha, Mr Muyiwa Oladipo, Mr. Mohammed Abdullahi Minin, Miss Funke Kayode, Miss Madeshola Adelakun, Miss Londiwe Ndwandwe and Mrs. Olaitan Okunola.

I also appreciate the University of KwaZulu-Natal, for keeping to its vision as the premier university of African scholarship through providing the enabling environment for research to flourish.

To God I give honour and glory.

ABSTRACT

Bring your own device (BYOD) has become a trend in the present day, giving employees the freedom to bring personal mobile devices to access corporate networks. In Nigeria, most banking institutions are increasingly allowing their employees the flexibility to utilize mobile devices for work-related activities. However, as they do so, the risk of corporate data being exposed to threats increases. Hence, the study considered developing a security framework for mitigating BYOD security challenges. The study was guided by organizational, socio-technical and mobility theories in developing a conceptual framework.

The study was conducted in two phases, the threat identification and the framework evaluation, using a mixed-methods approach. The main research strategies used for the threat identification were a questionnaire and interviews while closed and open-ended questions were used for the framework evaluation. A sample consisted of 380 banking employees from four banks were involved in the study. In addition, the study conducted in-depth interviews with twelve management officials from the participating banks. As for the framework evaluation, the study sampled twelve respondents to assess the developed security framework for viability as far as mitigating security threats emanating from BYOD in the banking sector is concerned. The sample consisted of eight executive managers of the bank and four academic experts in information security.

Quantitative data was analysed using SPSS version 21 while qualitative data was thematically analysed. Findings from the threat identification revealed that banking institutions must develop security systems that not only identify threats associated with technical, social and mobility domains but also provide adequate mitigation of the threats. For the framework evaluation, the findings revealed that the security framework is appropriate in mitigating BYOD security threats.

Based on the findings of the study, the developed security framework will help banks in Nigeria to mitigate against BYOD security threats. Furthermore, this security framework will contribute towards the generation of new knowledge in the field of information security as far as BYODs are concerned. The study recommends ongoing training for banks' employees as it relates to mitigation of security threats posed by mobile devices.

DERIVED PUBLICATION

Ofusori, L. O., Dlamini, N. N. J., & Prabhakar, R. S. (2018). Optimized three-dimensional security framework to mitigate risks arising From BYOD-enabled business environment. In *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 205-233). IGI Global

TABLE OF CONTENTS

DECLARATION	i
DEDICATION	ii
ACKNOWLEDGEMENTS	iii
ABSTRACT	v
DERIVED PUBLICATION.....	vi
TABLE OF CONTENTS.....	vii
LIST OF TABLES	xiv
LIST OF FIGURES	xvii
LIST OF ABBREVIATIONS	xviii
CHAPTER 1: INTRODUCTION	1
1.1 Introduction.....	1
1.2 Background	3
1.3 Problem statement.....	5
1.4 Research questions.....	5
1.5 Research objectives.....	6
1.6 Research rationale	6
1.7 Significance of the study.....	7
1.8 Structure of thesis.....	8
1.8.1 Chapter One: Introduction.....	8
1.8.2 Chapter Two: Literature review	8
1.8.3 Chapter Three: Conceptual model.....	8
1.8.4 Chapter Four: Research methodology	8
1.8.5 Chapter Five: Data analysis and interpretation of results.....	9
1.8.6 Chapter Six: Discussion of findings.....	9
1.8.7 Chapter Seven: Three-dimensional (3-D) security framework for BYOD enabled banking institutions in Nigeria.....	9

1.8.8 Chapter Eight: Evaluation of 3-D security framework for BYOD enabled banking institutions in Nigeria.....	9
1.8.9 Chapter Nine: Summary of findings, discussions and recommendations	9
1.9 Summary	10
CHAPTER 2: LITERATURE REVIEW	11
2.1 Introduction.....	11
2.2 Evolution of BYOD	11
2.2.1 Risk arising from organizations’ BYOD practices	12
2.2.2 Risk arising from BYOD individual practices	13
2.3 BYOD security threats vs cyber security threats	15
2.4 Existing security threats	15
2.4.1 Technical threats	16
2.4.2 Social threats	19
2.4.3 Mobility threats	21
2.5 Existing security measures	23
2.5.1 Mitigating technical threats.....	23
2.5.2 Mitigating social threats.....	26
2.5.3 Mitigating mobility threats.....	27
2.6 Vulnerability in BYOD environment.....	28
2.7 Related security frameworks.....	29
2.7.1 ISO/IEC 27000 series.....	29
2.7.2 PCI DSS	29
2.7.3 COBIT.....	30
2.7.4 NIST SP 800 Series.....	30
2.7.5 CISCO SCF (Security control framework)	30
2.7.6 IBM security framework.....	31
2.8 Challenges in securing BYOD environment.....	31
2.9 Summary	32
CHAPTER 3: CONCEPTUAL MODEL.....	34

3.1 Introduction.....	34
3.2 Related theoretical models	34
3.2.1 Protection motivation theory.....	34
3.2.2 Technology threat avoidance theory	35
3.2.3 Security risk perception model.....	35
3.2.4 Organization theories	36
3.2.5 Social-technical theory.....	37
3.2.6 Mobilities theory	39
3.3 Conceptual model	40
3.4 Summary	42
CHAPTER 4: RESEARCH METHODOLOGY	44
4.1 Introduction.....	44
4.2 Research philosophies.....	45
4.3 Research approach	46
4.4 Research choices	47
4.5 Research strategy	49
4.6 Research design.....	51
4.7 Research time horizon.....	51
4.8 Sample design	52
4.8.1 Study site.....	52
4.8.2 Target population	53
4.8.3 Sampling and sampling techniques	53
4.9 Research instrument.....	57
4.9.1 Questionnaire design.....	58
4.9.2 Interview design.....	60
4.9.3 Data collection procedure	61
4.10 Data quality control.....	62
4.10.1 Reliability.....	62
4.10.2 Validity.....	63

4.11 Ethical consideration.....	64
4.12 Limitations of the research methodology.....	65
4.13 Summary	65
CHAPTER 5: DATA ANALYSIS AND INTERPRETATION OF RESULTS.....	67
5.1 Introduction.....	67
5.2 The response rate	67
5.3 Overview of data analytical techniques	68
5.4 Data analysis: Quantitative data.....	70
5.4.1 Demographic data	70
5.4.2 General practices.....	72
5.4.3 Technical practices.....	73
5.4.4 Social practices.....	85
5.4.5 Mobility practices.....	94
5.4.6 Security threats experienced	110
5.5 Data analysis: Qualitative data.....	112
5.5.1 ICT Department personnel interview	113
5.5.1.1 Technical practice	113
5.5.1.2 Social practice	116
5.5.1.3 Mobility practice	118
5.5.2 Executive managers' interview	120
5.5.2.1 Technical.....	121
5.5.2.2. Social.....	123
5.5.2.3. Mobility.....	125
5.6 Summary	127
CHAPTER 6: DISCUSSION OF FINDINGS	128
6.1 Introduction.....	128
6.2. Technical security threats.....	128
6.2.1 Quantitative findings.....	129
6.2.2 Qualitative findings: ICT department personnel.....	131

6.2.3 Qualitative findings: Executive managers.....	131
6.2.4 Overview of technical security threats	132
6.3 Social security threats	133
6.3.1 Quantitative findings.....	133
6.3.2 Qualitative findings: ICT department personnel.....	135
6.3.3 Qualitative findings: Executive managers.....	136
6.3.4 Overview of social security threats	137
6.4 Mobility security threats	138
6.4.1 Quantitative findings.....	138
6.4.2 Qualitative findings: ICT department personnel.....	139
6.4.3 Qualitative findings: Executive manager	140
6.4.4 Overview of mobility security threats.....	141
6.5 Summary	141
CHAPTER SEVEN: THREE-DIMENSIONAL (3-D) SECURITY FRAMEWORK FOR BYOD ENABLED BANKING INSTITUTIONS IN NIGERIA.....	143
7.1 Introduction.....	143
7.2 Security threats classification.....	144
7.3 Threats based on individual practices	149
7.4 Threats based on organization practices	151
7.5 Solutions for threats arising from individual practices	153
7.6 Solution for threats arising from organization practices	157
7.7 Activities guiding device management	166
7.7.1 Device acquisition	166
7.7.2 Device monitoring.....	168
7.7.3 Device maintenance	169
7.7.4 Device disposal	169
7.8 Three-dimensional (3-D) security framework.....	170
7.9 Summary	173
CHAPTER 8: EVALUATION OF THREE-DIMENSIONAL (3-D) SECURITY FRAMEWORK FOR BYOD ENABLED BANKING INSTITUTIONS IN NIGERIA	174

8.1 Introduction.....	174
8.2 Descriptive analysis	175
8.2.1 Appropriateness.....	175
8.2.2 Adequacy	177
8.2.3 Feasibility.....	180
8.2.4 Flexibility	183
8.2.5 Intention to use.....	186
8.3 Thematic analysis.....	189
8.3.1 Recommendations for threats and solutions not considered in the framework.....	189
8.3.3 Implementation comments	192
8.3.4 General comments.....	193
8.4 Summary	196
CHAPTER 9: SUMMARY OF FINDINGS, DISCUSSIONS AND RECOMMENDATIONS	
.....	197
9.1 Introduction.....	197
9.2 Findings from the literature.....	197
9.3 Findings from threat identification.....	199
9.3.1 General practices.....	200
9.3.2 Technical security threats.....	200
9.3.3 Social security threats	201
9.3.4 Mobility security threats	202
9.3.5 The influence of technical, social and mobility security.....	203
9.3.6 Existing security measures.....	203
9.4 Findings from the framework evaluation	204
9.5 Contribution to body of knowledge	204
9.6 Limitations of the study	205
9.7 Recommendations.....	207
9.7.1 Recommendations for employees	207
9.7.2 Recommendations for ICT department personnel.....	208

9.7.3 Recommendations for executive managers.....	210
9.7.4 Recommendation for future research.....	211
9.8 Summary.....	212
REFERENCES.....	213
APPENDIX A: ETHICAL CLEARANCE APPROVAL LETTER.....	235
APPENDIX B: QUESTIONNAIRE FOR THREAT IDENTIFICATION.....	236
APPENDIX C: INTERVIEW FOR ICT DEPARTMENT PERSONNEL (THREAT IDENTIFICATION).....	248
APPENDIX D: INTERVIEW FOR EXECUTIVE MANAGERS (THREAT IDENTIFICATION).....	251
APPENDIX E: EVALUATION QUESTIONNAIRE.....	255
APPENDIX F: STATISTICIAN LETTER.....	259
APPENDIX G: DECLARATION OF EDITING AND TRANSLATION SERVICES.....	260

LIST OF TABLES

Table 4.1: Banks administered questionnaires.....	55
Table 4.2: List of ICT department personnel and executive managers for the interview (Threat identification).....	56
Table 4.3: List of participants for closed and open-ended questions (Framework evaluation) ..	56
Table 5.1: Demographic data.....	71
Table 5.1: Demographic data (Contd...)	72
Table 5.2: Chi-square goodness of fit test for device usage.....	73
Table 5.3: Cross-tab of respondents managing credential with smartphone and data leakage ...	75
Table 5.4: Chi-square test of independence for respondents managing credentials with smartphone and data leakage.....	75
Table 5.5: Cross-tab of respondents updating mobile device on public network and unauthorized modification of confidential information.....	76
Table 5.6: A chi-square test of independence for updating mobile devices on public networks and unauthorized modification of confidential information.....	77
Table 5.7: Cross-tab of respondents saving work document from laptop to a free cloud storage and Data leakage.....	78
Table 5.8: A chi-square test of independence for respondents saving work document from laptop to a free cloud storage and data leakage.....	78
Table 5.9: Crosstab of respondents not using password authentication and unauthorized access to social interactive network.....	80
Table 5.10: A chi-square test of independence for not using password authentication and unauthorized access to social interactive network.....	80
Table 5.11: Cross-tab of respondents for not using anti-virus and software keeps making copies of itself on the device.....	81
Table 5.12: A chi-square test of independence for not using anti-virus and software keeps making copies of itself on your/one's device.....	82
Table 5.13: Cross-tab of respondents for firewall and unauthorized access to social interactive network.....	82
Table 5.14: A chi-square test of independence for not using firewall and unauthorized access to social interactive network.....	83
Table 5.15: Cross-tab of respondents for hardware token and unknown number in the dialing list.....	84
Table 5.16: A chi-square test of independence for not using hardware token and unknown number in the dialing list.....	84

Table 5.17: Cross-tab of respondents for clicking on links and data leakage	86
Table 5.18: A chi-square test of independence for clicking on links and data leakage.	86
Table 5.19: Cross-tab of respondents for clicking on advertisement and malicious messages...	87
Table 5.20: A chi-square test of independence for clicking on advertisement and malicious messages.....	88
Table 5.21: Cross-tab of respondents for clicking on videos/audios and access request to device resources.....	89
Table 5.22: A chi-square test of independence for clicking on videos/audios and access request to device resources	89
Table 5.23: Cross-tab of respondents for attaching customer bank statement and unauthorized modification of confidential information	90
Table 5.24: A chi-square test of independence for attaching customer bank statement and unauthorized modification of confidential information	91
Table 5.25: Cross-tab of respondents for sharing password with colleagues and data leakage ..	92
Table 5.26: A chi-square test of independence for sharing password with colleagues and data leakage	92
Table 5.27: Cross-tab of respondents for sharing password with family/friends and data leakage	93
Table 5.28: A chi-square test of independence for sharing password with family/friends and data leakage	94
Table 5.29: Cross-tab of respondents for permanently deleting data from the recycle bin and unauthorized modification of confidential information	96
Table 5.30: A chi-square test of independence for permanently deleting data from the recycle bin and unauthorized modification of confidential information	96
Table 5.31: Cross-tab of respondents for not formatting the storage devices to get rid of critical information and data leakage	97
Table 5.32: A chi-square test of independence for not formatting the storage devices to get rid of critical and data leakage	98
Table 5.33: Cross-tab of respondents for not replacing the hard drive of the device to get rid of the critical information and data leakage	99
Table 5.34: A chi-square test of independence for not replacing the hard drive of the device to get rid of the critical information and data leakage.....	100
Table 5.35: Cross-tab of respondents for resetting the device to factory default settings to get rid of critical information and data leakage.....	101
Table 5.36: A chi-square test of independence for not resetting the devices to factory default settings to get rid of the critical information and data leakage	101

Table 5.37: Cross-tab of respondents for disposing of obsolete or faulty devices and unauthorized modification of confidential information	103
Table 5.38: A chi-square test of independence for disposing obsolete/ faulty device and unauthorized modification of confidential information	103
Table 5.39: Cross-tab of respondents for disposing of obsolete or faulty devices by giving them to family/friends and data leakage	104
Table 5.40: A chi-square test of independence for disposing of obsolete or faulty devices by giving them to family/friends and data leakage	105
Table 5.41: Cross-tab of respondents for throwing away faulty device and unauthorized modification of confidential information	106
Table 5.42: A chi-square test of independence for throwing away faulty device and unauthorized modification of confidential information	106
Table 5.43: Cross-tab of respondents for sharing device with colleagues and software keeps making copies of itself on the device.....	108
Table 5.44: A chi-square test of independence for sharing mobile device with colleagues and software keeps making copies of itself on one's device	108
Table 5.45: Cross-tab of respondents for sharing device with family/friends and personal information on one's mobile device were used without one's knowledge	109
Table 5.46: A chi-square test of independence for sharing mobile device with family/friends and personal information on your mobile device were used without your knowledge.....	110
Table 5. 47: Binomial test to determine significant proportion of security threats experienced	111
Table 5.48: Categories and themes that emerged in the qualitative analysis for IT personnel .	113
Table 5.49: Categories and themes that emerged in the qualitative analysis for executive managers	121
Table: 8.1: Categories and themes that emerged in the open-ended questions	189

LIST OF FIGURES

Figure 3.1: Socio-technical system (Bostrom & Heinen, 1977)	38
.....	40
Figure 3.2: Dimension of mobility (Basole, 2004)	40
Figure 3.3: Conceptual model (Source: Author’s own)	41
Figure 4.1: Research onion (Saunders et al., 2011, p. 108)	44
Figure 4.2: Research ‘onion’ adopted for the study	66
Figure 5.1: Bar graph distribution of type of mobile device and purpose of usage	73
Figure 7.1: Broad classification of threats	145
Figure 7.2: Threats based on individual practices.....	151
Figure 7.3: Threats-based organization practices.....	153
Figure 7.4: Solution for threats based on individual practices	157
Figure 7.5: Solution for threats based on organization practices	163
Figure 7.6: Summarized threats and solutions: Individual practices.....	164
Figure 7.7: Summarized threats and solutions: Organization practices	165
Figure 7.8: Activities guiding device management.....	167
Figure 7.9: Three-dimensional (3-D) security framework	172
.....	175
Figure 8.1: The framework is aligned with the policies and strategies of the bank	175
Figure 8.2: The framework enhances the effectiveness of the bank’s data security	176
Figure 8.3: The framework could contribute towards the efficiency of the bank operations ...	177
Figure 8.4: The framework could address all the technical threats identified	178
Figure 8.5: The framework could address all the social threats identified.....	179
Figure 8.6: The framework could address all the mobility threats identified	180
Figure 8.7: The framework could be cost-effective	181
Figure 8.8: The framework could be implemented within a short period of time	182
Figure 8.9: The framework could be implemented with the available resources of the bank...	183
Figure 8.10: The framework could be easily adopted with changing policies	184
Figure 8.11: The framework could be adopted for mitigating security threats within different branches of the bank	185
Figure 8.12: The framework could be adopted for mitigating security threats across different banks	186
Figure 8.13: The bank’s willingness to implement the framework.....	187
Figure 8.14: The bank willingness to adopt the framework.....	188
Figure 8.15: Use of framework by bank employees’ could be easy	188
Figure 8.16: Three-dimensional (3-D) security framework (Revised).....	195

LIST OF ABBREVIATIONS

ATM: Automated teller machine

BYOD: Bring your own device

BYOT: Bring your own technology

BYOIoT: Bring your own internet of things

CBN: Central Bank of Nigeria

COBIT: Control objectives for information and related technology

DDoS: Distributed denial of service

DoS: Denial of service

GPS: Global Positioning System

GSM: Global System for Mobile communications

IBM: International Business Machines

ICT: Information and communication technology

ISO: International Standards Organization

IT: Information technology

IP: Internet Protocol

IoT: Internet of Things

LTE: Long-term Evolution

LTE-A: Long-term Evolution Advanced

MANET: Mobile ad hoc network

MMS: Multimedia services

NIST: National Institute of Standards and Technology

PC: Personal computer

PCI DSS: Payment Card Industry Data Security Standard

PDA: Personal digital assistant

PIN: Personal identification number

PMT: Protection motivation theory

SMS: Short messages services

SOA: Service-oriented approach

TTAT: Technology threat avoidance theory

UKZN: University of KwaZulu-Natal

USB: Universal Serial Bus

WLAN: Wireless local area network

CHAPTER 1: INTRODUCTION

1.1 Introduction

Globally, mobile technologies are a useful tool of communication, which are now becoming an integral part of everyday life (Bello, Armarego & Murray, 2015). As these technologies become prevalent, they are also becoming popular in workplaces. Most employees prefer to use their personal mobile devices for work because of the several benefits associated with it. Foremost among the benefits is convenience; with mobile devices, employees literally have access to everything they need in their palmtop: contacts, schedules, e-mail, search engines, access to corporate data and applications (Uz, 2014). These mobile devices are also used to make calls, check e-mail, browse the internet, perform financial transactions, and for other similar activities that a user would perform on a personal computer (Astani, Ready & Tessema, 2013). More importantly, mobile devices help the employee to stay connected to their co-workers and customers anywhere in the globe. With the help of such devices, employees are also able to respond to work-related e-mails away from the office and attend conference meetings via Skype or other applications (Nunoo, 2013).

Conversely, using a personal mobile device for work has given rise to a trend called Bring Your Own Device (Twinomurinzi & Mawela, 2014). Bring Your Own Device (BYOD) sometimes known as Bring Your Own Technology (BYOT) is gaining popularity among the employee in all sectors, including the banking sector (Mark, 2014). BYOD refers to a trend whereby employees are given the liberty to bring their mobile devices (e.g. smartphone, laptops and tablets) to access organizational network (Disterer & Kleiner, 2013). In this present age of technology, BYOD trend enables easy communication and quick access to information (Nunoo, 2013). There are several benefits associated with the BYOD phenomenon: Firstly, it lowers corporate cost whereby organizations do not have purchase mobile devices for the employees (Dunnett, 2012). Secondly, employees are naturally familiar with their own mobile devices, hence it requires less technical training (Bello et al., 2015). Thirdly, employees can now perform work duties outside the organizational premises because they are no longer confined to work within the organizational premises and this has increased their productivity and efficiency (Garba, Armarego, Murray & Kenworthy, 2015). Fourthly, it increases employees' engagement

during working hours as well as after working hours (Bello et al, 2015). Lastly, BYOD increases employees' job satisfaction and happiness (Bello et al, 2015).

However, despite these enormous benefits, Mphahlele (2016) argues that these benefits are not without their risks. These risks come in the form of security concerns for the devices. Foremost among the concerns is how the organizational information on the device will be protected (Bello et al., 2015). Protecting such information becomes a major challenge as these mobile devices are carried everywhere by the employees. Other concerns are the risk of mingling personal and organizational data, sharing devices with non-employees, and software licensing issues (Olalere, Abdullah, Mahmood & Abdullah, 2015). According to De las Cuevas, Mora, Merelo, Castilo, Garcia-Sanchez and Fernandez-Ares (2015), once employees use their personal mobile devices for work purpose, it becomes challenging to separate an organization's data from personal data. Furthermore, the issue of data integrity is raised as organization information is transferred from the organization's network to employees' mobile devices. Similarly, employees are concerned with the issue of data privacy and that their personal information is at the disposal of their employer (Deasy, Meyer, Newell, Emil, Winsner, Furodet and Strudel, 2018). Privacy invasion arises when an employer tries to access employees' devices and such action can result in a lawsuit when not handled properly (Lebek, Degirmenci & Breitner, 2013).

According to Twinomurinzi and Mawela (2014), the ICT departments are now finding it difficult to secure personally owned devices because it is out of their control and also impossible to review employees' mobile devices manually since these are their personal devices. Uz (2014) also identifies file-sharing sites as a security concern for an organization's classified data because it allows employees to save and access files from the cloud wherever they are. However, such file-sharing services can be compromised thus leading to security breach of corporate information. Astani et al. (2013) identified other security issues such as data theft or leakage, malware, software bugs and lack of control over what is on employee devices. Olalere et al. (2015) claim that the major security risk that organizations could face by implementing BYOD is lost or stolen mobile devices because it leads to data leakage. Thus, it is important to have a well secured and scalable BYOD strategy that will manage any security risks introduced by employees' mobile devices (Thielens, 2013). However, Disterer and Kleiner (2013) argue that there

is little research into the phenomenon of risks associated with the exposure to uncontrolled data sharing through BYODs in the banking sector, especially in developing countries, including Nigeria. This represents a gap in the literature, and it gives an opportunity for this case study to address.

Hence this study presents an overview of the BYOD trend and pertinent features influencing its adoption as a standard. Moreover, it presents the security threats confronting individual and organizations practices together with the mitigating strategies that are being adopted in curbing the threats. In addition, the study presents the difference between cyber threats and BYOD security threats. Furthermore, a security model is conceptualised to explain the difference amongst threats that constantly affect individuals and the organization as they relate to BYOD. This framework will help prioritize security awareness to be able ensure data integrity.

1.2 Background

In a developing country such as Nigeria with a population of over 150 million people, the banking sector is privileged with an opportunity to attract a significant number of diverse clienteles in the country (Adeniran, 2008). Despite this enormous population, only 20 per cent of Nigerians have bank accounts (National Bureau of Statistics, 2017). One of the major reasons why most Nigerians do not have bank accounts is unemployment (International Labour Organization, 2012). According to the National Bureau of Statistics (2012), the unemployment rate was 24 per cent as at 2012 but as at 2017, the unemployment rate has increased to 25.2 per cent (National Bureau of Statistics, 2017). This rate of unemployment poses significant threats to all sectors of the economy, including the banking sector. The majority of the unemployed people are well educated and technologically knowledgeable, spending much of their time and energy online for a range of activities such as buying and selling of goods (Adeniran, 2008). However, some of these unemployed people engage in cybercrimes and become conduits of criminal acts that threaten banking operations. Presently, Nigeria is a leading target and source of malicious Internet activities and this is spreading across the West African sub-region (Aribake, 2015). According to Ojeka, Ben-Caleb, and Ekpe (2017), these malicious Internet activities are on the increase because of the significant rise of mobile communication and the drive from the Central Bank of Nigeria towards a cashless

economy. Cybercrimes in the Nigerian banking sector are a major source of threat that diminishes the effectiveness of the sector on a large scale (Ehimen & Bola, 2010). In some instances, these crimes are committed by banking employees using their own mobile devices because they have adequate knowledge of the banks' software systems and they can manipulate these to their advantage (Greitzer, Strozer, Cohen, Moore, Mundie and Cowley, 2014). In another instance, employees lack adequate security awareness of BYOD, leaving businesses vulnerable to online attacks or cyber-crime (Ribadu, 2007).

Serianu (2016) asserts that over 34 per cent of Nigerian banks that adopt the BYOD phenomenon do not have a best practice policy for BYOD, thus making this device vulnerable to security threats and attacks. Likewise in other African countries such as Swaziland, Ghana, Kenya and Mozambique there are no policies that have been implemented that specifically regulate the use of personal devices in the work environment (Madzima, Dube, & Mashwama, 2013). As a result, the banking sector lack adequate planning, technical support and inadequate infrastructure to tackle BYOD security threats (Madzima et al., 2013). Similarly, Bello et al. (2015) affirm that most African banking institutions that allow their employees to bring and use their personally owned mobile devices for work purposes do not have policies for data protection issues, specifically security and privacy. Conversely, in South Africa, there are policies and a regulatory framework that have been incorporated to support the use of technology (Gustav & Kabanda, 2016). However, "the continuous changes in government regulation regarding the use of data; and the lack of conducive ICT infrastructure were deemed as hinderances to BYOD" (Gustav & Kabanda, 2016).

It is worth mentioning that as a result of the type of classified information contained and processed in the banking sector, it is essential to consider risk management in the development of a BYOD policy (Wang, Wei & Vangury, 2014). However, only minimal studies have been carried out to comprehend the phenomenon of risks associated with the uncontrolled exposure of data sharing through BYODs in the banking sector in developing countries, including Nigeria (Disterer & Kleiner, 2013; Ojeka et al., 2017). Thus, this study examines the security concerns being raised through BYODs in the Nigerian banking sector, reviews the existing security measures and their drawbacks,

analyses the level of security threat awareness and develops a security framework that supports BYOD and could assist the banking sector in policy development.

1.3 Problem statement

Globally, BYOD trend has enabled an increase in information sharing, eliminating geographical constraints. However, with this increase in information sharing that transcends geographical boundaries, security threats have also increased and have become a major concern (Aribake, 2015). While Bello et al. (2015) maintains that there is high rate of security threats due to the large number employees bringing their mobile devices to access organizational networks, Lindström and Hanken (2018) emphasize that the major concerns associated with these security threats is the extent of vulnerability to which they expose the banking institution as far as access to classified organizational information is concerned, a phenomenon that can lead to the loss of important clientele data. In addition, despite the increased rate of these security threats such as phishing, policy violation and lost or stolen devices, a large number of employees are not fully aware of the vulnerability and the challenges that BYOD brings to information security in their organizations (Ojeka et al., 2017). Furthermore, measures to help curb these security threats and vulnerabilities do not respond to same level of increase of the security threats. Lindström and Hanken (2018) argue that the implication of enabling a BYOD environment implies handling the security concerns that comes with the use of personal devices for work purpose. Ojeka et al. (2017) highlight the importance of protecting critical information on BYODs which is to improve the organization well-being. However, recent empirical research has shown that only minimal studies have been carried out to understand the phenomenon of risks associated with the uncontrolled exposure of data sharing through BYODs in the Nigeria banking sector (Ojeka et al., 2017). Thus, this research aims to answer the following main research question:

How can the security threats associated with BYOD practices in the Nigerian banking sector be mitigated?

1.4 Research questions

To clearly understand and address the problem in focus, the main question/problem has been further broken down into the following research questions:

1. What are the security threats associated with the technical system in the banking sector of Nigeria?
2. What are the security threats associated with the social system in the banking sector of Nigeria?
3. What are the security threats associated with the mobility system in the banking sector of Nigeria?
4. How does the security threat regarding the technical, social and mobility systems influence the banking sector of Nigeria?
5. How do the recommended security measures help to mitigate the security threats?

1.5 Research objectives

The objectives of this research are the following:

1. To identify the security threats associated with the technical system in the banking sector of Nigeria;
2. To investigate the security threat associated with the social system in the banking sector of Nigeria;
3. To understand the security threats associated with the mobility system in the banking sector of Nigeria;
4. To examine the influence of the security threats to the technical, social and mobility systems in the banking sector of Nigeria; and
5. To evaluate the recommended security measures that help to mitigate the security threat.

1.6 Research rationale

Nigeria has been regarded as one of the leading countries in Africa in terms of its economic contribution to the continent and population (Okonjo-Iweala & Osafo-Kwaako, 2007). The Ministry of Communication Technology (2012) has also stated that one of its goals is to "...sustain socioeconomic development critical to Nigeria's vision of becoming a top 20 economy by the year 2020". Hence, if sustaining socioeconomic development is critical to Nigeria's vision of being among the world's top 20 economies by the year 2020, then the banking sector is a major sector that must be given ultimate priority. This is because the banking sector is a major sector responsible for the growth and development of the overall economy as well as for other sectors of the economy

(Alade, 2013; Sanusi, 2012; Soludo, 2004). However, cybercrimes in Nigeria are a major source of threats that diminish the effectiveness of the sector on a large scale, especially in the banking sector (Ehimen & Bola, 2010). Using personal devices for work purpose has given birth to the trend BYOD (Twinomurinzi & Mawela, 2014). This implies that there are possibilities for an unlimited number of employees to be connected by mobile devices (Greitzer et al., 2014). These possibilities will be further multiplied in the Fourth Industrial Revolution.

Furthermore, Moavenzadeh (2016) a member of the Management Committee of the World Economic Forum and head of mobility industries, raised the following concerns about the fourth industrial revolution. Firstly, the fast-paced technology have exerted pressure on available security control, leaving most organizations vulnerable to security related risks. Secondly, how will the technology world collaborate to build regulatory frameworks and standards that promote growth and adoption of new technologies? According to Schwab (2016), the fourth industrial revolution profoundly affects the nature of security in businesses. Lastly, the regulators have to adapt to the fast-changing environment as a result of rapid pace of change in innovation. Hence, regulators have to deal with vulnerabilities and security threats arising from a BYOD-enabled environment in the Fourth Industrial Revolution.

1.7 Significance of the study

Several studies have developed various security frameworks such as ISO, NIST, Cobit, CISCO and IBM (ISACA, 2011; ISO, 2005; NIST, 2012), but these security frameworks are completely inadequate for dealing with the current security threats arising from a BYOD-enabled environment because they do not sufficiently consider the influence of the Fourth Industrial Revolution in accommodating these security threats. This study fulfils the limitations by developing a security framework that addresses the diverse technology and also considers the technical, social and mobility aspect for a BYOD-enabled environment, particularly the Nigerian banking sector in the Fourth Industrial Revolution. Furthermore, this research is of significance as it provides primary empirical information about security threats associated with the uncontrolled exposure of data sharing through BYOD devices in the Nigerian banking sector. It also aims to contribute to the current theoretical perspectives concerning the use of such devices, therefore

contributing to the existing body of knowledge regarding security threats for banks. Finally, this study provides a basis through which banks in developing countries can enhance their security while supporting their employees in using their personal devices in executing their duties as employees of the bank.

1.8 Structure of thesis

The entire thesis consists of nine chapters as follows:

1.8.1 Chapter One: Introduction

The chapter introduces the problem statement by introducing the research background, research objectives, research questions, research rationale, and the significance of the study. This helps to understand the relevance of the research and also to place it in a correct perspective.

1.8.2 Chapter Two: Literature review

This chapter reviews the threats, solutions and identifies the vulnerabilities in a BYOD-enabled environment. The chapter also reviews the existing security measures and related security frameworks.

1.8.3 Chapter Three: Conceptual model

This chapter models the detailed description of the conceptual framework that forms the basis of the research work and shows its relevance to the research. These theories include organization theory, social-technical theory and mobilities theory. This forms the foundation on which the proposed security framework was built.

1.8.4 Chapter Four: Research methodology

Chapter four discusses the research methodology adopted for this study. The research philosophy, research approach, research strategy, research design, research time horizon, research methodology and research instrument are dealt with. This chapter also describes the data quality control, ethical considerations as well as limitations of the study's methodology.

1.8.5 Chapter Five: Data analysis and interpretation of results

Chapter five analyzes the quantitative and qualitative data collected from the field study in relation to the security threats associated with the technical, social and mobility system of the Nigerian banking sector. These results are represented in bar graphs, tables and figures. The quantitative data were analyzed using statistical software packages, namely IBM SPSS Amos version 21. The tests used in the analysis are descriptive statistics, chi-square and binomial tests while the qualitative results were represented using thematic analysis.

1.8.6 Chapter Six: Discussion of findings

Chapter six discusses the findings of the study. The findings are discussed based on the empirical evidence presented in chapters five, thus expanding the frontiers of knowledge on threats associated with the technical, social and mobility systems of the Nigerian banking sector.

1.8.7 Chapter Seven: Three-dimensional (3-D) security framework for BYOD enabled banking institutions in Nigeria

Chapter seven presents a three-dimensional (3-D) security framework for BYOD enabled banking institutions in Nigeria based on the results and findings of the data analysis.

1.8.8 Chapter Eight: Evaluation of 3-D security framework for BYOD enabled banking institutions in Nigeria

Chapter eight evaluates the 3-D security framework for BYOD enabled banking institutions in Nigeria. These results are represented in bar graphs and tables. The quantitative data (closed-ended questions) are analyzed using descriptive analysis while the qualitative data (open-ended questions) are represented using thematic analysis.

1.8.9 Chapter Nine: Summary of findings, discussions and recommendations

Chapter nine summarises the findings from the literature as well as the findings from the two phases (threat identification and framework evaluation) of the study. The limitations of the study and its contribution to knowledge and research are also presented. Lastly, conclusions and recommendations for further studies are made in the chapter.

1.9 Summary

This chapter introduced the trends of BYOD with regard to the banking sector. As more financial institutions adopt the BYOD phenomenon, the risk of corporate data being exposed increases and becomes a security problem that must be addressed frequently (Bello et al., 2015).

The chapter also provided background information on the emergence of cybercrime in the Nigerian banking sector and how mobile devices are susceptible to security threats. This is in line with the literature that attests that "...cybercriminals take advantage of the fact that almost everyone uses a mobile device and as such make it easy to spread threats through the pervasive technology" (Wada & Odulaja, 2012). However, Ojeka et al. (2017) claim that there have been insufficient studies carried out to understand the phenomenon of risks associated with the uncontrolled exposure of data sharing through BYODs, especially in the Nigerian banking sector. This forms the basis for the problem statement, research questions and objectives.

In addition, the chapter discussed the research rationale and significance of this study which includes providing primary empirical information about security threats associated with BYOD in Nigerian banking sector. Lastly, the chapter discussed the structure of the thesis.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Rice (2017) defines literature review as an objective critical survey of scholarly articles, books and any other sources relevant to a particular problem, theory or area of study and by so doing, provides a critical evaluation and summary of these work in relation to the research area or problem being investigated. In other words, it gives an evaluation report of information found in the literature that is related to a particular area of research. Thus, the literature review for this study focus on the BYOD concept, specifically with regard to vulnerabilities and threats against portable mobile devices used by employees for work purposes. According to Tung (2017), "...the increase in the use of mobile devices has significantly increased the total number of interconnected devices to 13.19 billion in 2017 and it is expected to grow to 25 billion by the year 2020". These interconnected devices will keep expanding, thus making it easier for cybercriminals to propagate threats on large scale. Similarly, harnessing this connectivity for productive use becomes a major challenge as this will affect data security, privacy and integrity although Ofusori, Dlamini and Prabhakar (2018) assert that "...there are some BYOD security measures, but they all have limitations when applied on a BYOD environment". Hence, this chapter reviews the literature to identify the knowledge gap and substantiate the need for the research. To begin with, a brief background is given on the evolution of BYOD.

2.2 Evolution of BYOD

Vignesh and Asha ((2015) as cited in Ofusori et al., 2018) argue that "...the infiltration of personally owned mobile devices like smartphones, laptops and tablets gave birth to Bring Your Own Device (BYOD) phenomenon, where personal gadgets started entering the workspace". According to Copeland and Crespi (2012), there is a new consumerization paradigm shift in the technological world where individuals do not only bring their personal devices but also use web applications for official work. Zahadat, Blessner, Blackburn, and Olson (2015) assert that "BYOD is a trend that has been around for some time, firstly characterised by individuals bringing their own personal devices to the workplace and installing preferred programs to accomplish tasks assigned to them". Broomhead (2013) redefined this trend using statements such as "the rise of mobility and marginalization of the PC" and the "move-and-do culture". The ICT departments made

some effort to stop the infiltration of these employee-owned devices from entering the organizations, but they were unsuccessful (Zahadat et al., 2015).

Hence, ICT departments had to increase their security measures and adjust their budgets to cater for employees' own devices being brought to the organization (Vignesh & Asha, 2015). Gartner (as cited in Ofusori et al., 2018), "...considers the use of mobile devices in the workplace to be among the ten most important strategic trends". Broomhead (2013, p.207) echoed Gartner by stating that "...BYOD has become disruptive in the sense that employees always want to bring personal devices to the organization and want to connect to everything". Copeland and Crespi (2012, p. 187) outline three major steps that have been taken by most organizations in the adoption of BYOD. "Firstly, organizations started encouraging personal devices and connecting them to corporate internet servers. Secondly, organizations started connecting personal devices to corporate applications. Lastly, organizations stopped providing laptops and phones to employees, thereby adopting the option of BYOD strategy". According to Bello et al., (2015), BYOD became a fascinating trend in most organizations, including the banking sector. The banking sector interprets BYOD as a strategy that can contribute to the cost-efficiency of the business, create a competitive advantage and increase productivity (Mphahlele, 2016). However, owing to the type of classified information and transaction that are processed in the bank, risk management is a major aspect that must be tackled. Furthermore, individual and organization practices have to be re-defined and policies have to be drawn up to provide guidelines that accommodate the BYOD trend in the banking sector in developing countries which include Nigeria (Bello et al., 2015).

2.2.1 Risk arising from organizations' BYOD practices

The adoption of BYOD in organizations lead to increased productivity, increased job satisfaction and lower ICT costs (Astani et al., 2014; Lee et al., 2013; Smith & Forman, 2014). However, Osterman Research (2012) argues that every organization that allows a personal device to be used within its environment must also address the risks that come along with it. According to Bello et al (2015), there are some organizations that give out smartphones and laptops to employees to be used for work purpose as well as allowing them to bring in their personal devices. However, among the organizations that allow employees to bring personal devices, 94 per cent face the challenge of a stolen or lost device, 93 per cent raise a concern regarding adopting BYOD policies while 66 per cent

admit to having careless employees (Dimensional Research, 2014). In addition, Osterman Research (2012) reveals that there are organizations that allow employees to use their mobile device from home or public places for work purpose. The implication is that the corporate information on the device becomes exposed to unprotected public networks (Bello et al., 2015). Furthermore, Olalere et al. (2015) affirm that although some organizations have established BYOD policies, they do not ensure that their employees comply with this policy. In presenting another view, Shumate and Ketel (2014) argue that despite the fact that some organization carry out training to ensure employees' compliance, they do not provide appropriate security information training on ways in which employees can use their mobile devices (Tu, Turel, Yuan & Archer, 2015). The implication of this is that an organization's information becomes vulnerable to risks such as data leakage, phishing, malware attack and keylogger attack (Tu et al., 2015). Shumate and Ketel (2014) opine that an organization requires a well-structured policy for BYOD as well as security training for employees. This may include safe device operation (establish password, avoid lending the device to third party), public networks restriction (access must be restricted), measures to store organizations information (data must be encrypted, information must not be stored in the cloud) and lost or stolen device protocols to follow (report immediately to the organization).

From the review of organization practices, it appears that most of these practices create security risks, but the organization still adopts BYOD practices because of the profound benefits (Nunoo, 2013). This has gradually led to individual practices as employees now enjoy the benefits of connecting their personal devices to corporate networks.

2.2.2 Risk arising from BYOD individual practices

Bello et al. (2015) argue that most employees take advantage of BYOD by connecting their devices to networks specifically for personal purpose. However, such action makes it difficult to distinguish organizational data from personal data (Bello et al., 2015). Similarly Gartner (2015) reveals that 75 per cent of employees have their mobile devices configured to automatically connect to a wireless network. However, such action can make employees' mobile devices vulnerable to various security threats which can lead to data leakage (Bello et al., 2015). Furthermore, Bello et al. (2015) affirm that most employees are in the habit of connecting their personal mobile device to unregulated public networks. According to Wakefield (2014), public networks such as WiFi hotspots

are very attractive to mobile device users because they are unrestricted and are common in public places such as hotel, malls and restaurants. Nevertheless, the implication of this is that the integrity and confidentiality of information is exposed when employees use WiFi hotspots (Arregui, Maynard & Ahmad, 2016). In addition, Uz (2014) argues that most employees are in the habit of using cloud storage services owing to inadequate memory storage on the device and also because it enables employees to save, copy and access files wherever they are. However, such cloud services may pose a security risk to an organization's information (Uz, 2014).

Dimensional Research (2013) revealed another practice exercised by employees which is accessing social media platforms from their mobile device for work-related purposes. The exponential growth of social networking sites (e.g. Blogs, LinkedIn, and YouTube) offers employees the opportunity to engage in a daily conversation with many customers around the world. However, when employees access social media platforms for work-related purposes either through their mobile devices or computer, they risk endangering the corporate data on their devices by unknowingly acquiring malware, viruses, and spyware (Chanda & Zaorski, 2013; Uz, 2014). Hackers coax unsuspecting employees to click a link or download a free application that secretly spread spyware, which in turn penetrates the employees' devices (Dimensional Research, 2013). Furthermore, an empirical study by Bello et al. (2015) demonstrated that employees share passwords with colleagues, friends and family without realising how this can cause a security breach. According to Notoatmodjo and Thomborson (2009), the highest volume of security breaches come from employees' carelessly misusing data as a result of shared passwords. Similarly, a study conducted by Chris (2016) reveals that employees share mobile devices with friends and family. However, when these shared devices are used by colleagues, friends or family either to check e-mail, social media or do other personal work, they may come across some confidential information (e.g. customers' details, bank accounts or personal identification numbers) which can be retrieved without the knowledge of the device owner and then used maliciously (Chris, 2016). In another instance the borrowed mobile device can be used to access a malicious WiFi unintentionally and this can open doors for hackers to spoof out confidential information (Dimensional Research, 2013).

From the aforementioned security risks encountered, "...this practice would have been stopped but most organizations have adopted this practice because of the profound

benefits they derived from BYOD” (Bello et al., 2015, p.1279). Hence it is of utmost importance to take proactive security measures to avert BYOD associated risks.

2.3 BYOD security threats vs cyber security threats

According to Olasanmi (2010), a cyber-threat refers to any mischievous way of gaining access to a computer network. El-Moussa (2018) describes cyber threats as any type of malicious code (e.g. malware) that moves from one network to another, trying to gain illegal access to a device without the user’s knowledge with the aim of performing a malicious act. The recent security threat called “WannaCry ransomware” is a typical example of cyber threats (Ehrenfeld, 2017). WannaCry ransomware is one of the most dangerous ransoms that has the capability to spread across an organization’s network by exploiting a critical vulnerability in computers as well as mobile devices (Ehrenfeld, 2017). It automatically encrypts every file and demands ransom once it gains access to the device (El-Moussa, 2018).

On the other hand, Sipior, Bierstaker, Chung and Lee (2017) describe BYOD security threats as those threats associated with the movement of mobile devices from one place to another. These security threats include lost or stolen devices, sharing of devices and e-waste. However, El-Moussa (2018) argues that while these devices can be connected to the Internet, the malicious code on the network can also be resident in the device. Wada and Odulaja (as cited in Ofusori et al., 2018), also claim that “...cybercriminals take advantage of the fact that almost everyone uses a mobile device and as such make it easy to spread threats through the pervasive technology”. In addition, Sipior et al. (2017, p.10) confirm that “...cyberspace is witnessing the advent of a complete range of mobile devices and applications that have made it susceptible to security threats from all types of miscreants”. From these arguments, it can be inferred that BYOD security threats also include cyber threats because once the mobile devices are connected to the Internet, they become vulnerable to cyber threats.

2.4 Existing security threats

Organizations are often confronted with inherent security threats while trying to increase production and boost service delivery through the use of information communication technology (ICT), hence frustrating the advancement of its progress (Ehimen & Bola,

2010). Conversely, the Nigerian banking sector seems to have an endless list of these security threats, but this section focuses on threats that have relevance to BYOD. In addition, since it has been established in section 2.3 that BYOD security threats also encompasses cyber security threats, this study therefore categorized security threats resulting from BYOD under the technical, social and mobility domains.

2.4.1 Technical threats

Ofusori et al. (2018, p. 223) refer to technical threats as “...threats emanating from the technical knowledge in the use of mobile device as well as threats emanating from BYOD hardware and software technology used for work related purpose”. This technology supports the operation of an organization that enables communication and workflow (Bello et al., 2015). The following security threats are considered as the major technical threats related to BYOD in the Nigerian banking sector.

Phishing

Phishing can be defined as a fraudulent act against any form of legitimate businesses (Wang et al., 2014). Phishing can be used to steal the identity and classified information of unsuspecting consumers (Wang et al., 2014). A phishing attack is a form of deception from hackers with the aim of collecting confidential information or forcing mobile device users to send confidential information about themselves (Ngoqo & Flowerday, 2015). It can be used to persuade BYOD users to download malicious applications onto their mobile device with the aim of obtaining the location of the device as well as the data (Pratt Jr & Jones, 2013). Other strategic methods of deception can be invitations to register personal details on a website or e-mail messages sent from someone known by the recipients requesting them to respond with confidential information. This is a type of crime that is basically used to steal confidential information such as credit card numbers, banking passwords, bank account details, financial status, corporate secrets and other valuable information (Goverdhan & Sammulal, 2013).

Keystroke logging

Keystroke logging can be defined as the use of a software program to record typed characters made by a computer user in order to fraudulently gain access to confidential information which includes password (Ladakis, Koromilas, Vasiliadis, Polychronakis & Ioannidis, 2013). For BYOD users, when a malicious attachment is downloaded or

software is installed on the device, it runs a hidden keylogger program on their mobile device without the knowledge of the user. This is used to capture information which is transmitted to a cyber-criminal website (Pratt Jr & Jones, 2013). According to Tuli and Sahu (2013), keyloggers cannot easily be detected and there is no effective anti-software that helps unravel their malicious act. In other words, they can run on mobile devices for a long period of time without being detected.

Rogue device

Golde, Redon and Borgaonkar (as cited in Ofusori et al., 2018) define a rogue device “...as an unauthorized connection of mobile devices to the network which pose a security threat to the organization”. Rogue device can be used to commit a security breach or disrupt network operations in order to steal classified corporate information with the aim of harming the organization’s reputation (Ofusori et al., 2018). According to Arregui et al. (2016), preventing the illegal connection of a mobile device to the network has been a major challenge in allowing BYODs into the organization. BYODs are more susceptible to be used as rogue devices if appropriate security measures are not put in place.

Jailbreaking

Jailbreaking, sometimes called rooting, allows users to install third-party applications that are unavailable in official vendor stores, to modify the operating system and to perform other operation that would normally be restricted or that the manufacturer would not have allowed (Rogers, 2012). As a result of this flexibility, most mobile device users root their devices in order to enjoy the freedom of downloading preferred software (e.g. security applications or advanced backup). However, the information security of the organization may be affected if these devices are used in a BYOD-enabled environment (Arregui et al., 2016). According to Nazar, Seeger, and Baier (2011), when users root their mobile devices, it opens the device up to security risks that can compromise sensitive data on their mobile devices. Hackers have been known to develop applications that look innocent but actually steal data (Rogers, 2012). Once a malicious code has root access, it can do almost anything from deleting critical files to retrieving account information (Rogers, 2012).

Data interception

According to Evripidis (as cited in Ofusori et al., 2018, p. 223), "...data interception refers to the obstruction of data transmission to and from the device, and remotely altering the messages". With BYOD implementation, data interception may cause a serious threat to various networks (Bello et al., 2015). It becomes a serious concern when personal information can easily be intercepted while using the mobile device (Wu, 2009). Such action can lead to the risk of the data being accessed, edited, or destroyed. Bello et al. (2015, p. 1280) affirm that "...attackers will capture and alter data packets between devices when mobile devices connect to unsecure WiFi networks; this is referred to as man-in-the-middle attack".

Network exploit

Mobile systems that operate on local or cellular networks (e.g. Bluetooth or WiFi) usually encounter software flaws (Pratt Jr & Jones, 2013). Network exploits seize the opportunity of such flaws to launch spyware attacks on mobile devices because it is easy to propagate threats using these ubiquitous devices and they succeed most times without users' interference (Pratt Jr & Jones, 2013). In other instances, the network exploits analyse a particular mobile device, and then spread malware on it with the aim of accessing, destroying, modifying, and extracting confidential information (Bello et al., 2015). According to Needham and Lampson (2008, 385), "...network exploits makes use of special tools to find users on a WiFi network and hijack the users' information which is then used to impersonate a user online".

Unregulated public networks

Unregulated public networks are networks that can easily be accessed by anyone or the general public and through these, can connect to the Internet (Bello et al., 2015). With the emergence of BYOD, most mobile device users can update applications or software from any network (e.g. public network). However, public networks are most susceptible to attacks such as WiFi eavesdropping. According to Needham and Lampson (2008), most of the unintentional threat is that of insecure wireless network usage. Unsecured wireless networks either at an airport, hotel or coffee shop can easily put sensitive information in jeopardy (Du & Zhang, 2006). Hackers can disguise in such untrusted networks to infiltrate into any system connected and obtain sensitive information (Balachandran, Voelker & Bahl, 2005).

2.4.2 Social threats

According to Ofusori et al., (2018, p. 225), "...social security threats are threats that represent users' attitudes and awareness levels in using mobile devices". They also refer to the act of communication among mobile device users (Bello et al., 2015). It is essential that organizations recognize the effect of these threats on their security system because Bello et al. (2015) claim that due to the invisibility of these security threats they are normally not well addressed.

Malicious insider threat

Malicious insider threats occur when someone in a trusted position intentionally abuses the trust for private gain (Bowen, Salem, Hershkop, Keromytis & Stolfo, 2009). A malicious insider can either be a former staff member, consultant, contractor, a trusted partner or a current employee of the organization taking advantage of the knowledge they have about organization operations to compromise information security (Mathew, Upadhyaya, Ha & Ngo, 2008). With BYOD, it is easier to achieve malicious insider threats since employees have access to organisational resources anywhere and at any time. A BYOD user with malicious intent can possibly carry out malware attacks, phishing, and data interception (Bello et al., 2015). Furthermore, malicious insiders can easily steal a co-worker's device without the organisation's knowledge (Bello et al., 2015).

User policy violations

User policy violation occurs when a user intentionally or unintentionally goes contrary to the stipulated policy of using a mobile device (Chanda & Zaorski, 2013). In a BYOD context, individuals can deliberately or ignorantly disable antivirus or firewall applications on their mobile devices in order to increase speed and performance. In addition, they can access unsecured websites to download documents that might contain malware, which in turn exposes the device to vulnerabilities and threats since the firewall and antivirus have been disabled. Most organizations are continuously facing challenges of ensuring their employees comply with user policies (Vance, Siponen & Pahlila, 2012). Bello et al. (2015, p. 1281) noted that "...no matter how well developed and structured organizational policies are, they are rendered useless if not used adequately by employees".

Data privacy violation

According to Aula (2010), data privacy violation occurs when the confidential information of an individual or an organization is shared with a third party without the consent of the owner. Data privacy violation becomes easier with the implementation of BYOD in most organization. Most BYOD employees interact with colleagues or friends through social network platforms such as LinkedIn, Facebook and WhatsApp (Aula, 2010; Chanda & Zaorski, 2013). Unfortunately, some of the organization's or personal information that is disclosed on social networking site can be stolen by an experienced hacker who buys and sells it with aim of committing security breaches (Aula, 2010). Empirical studies have shown that these hackers use social networking sites to manipulate employees into divulging information that leads to more valuable information (such as banks' information, usernames and passwords) or provides access to a bank's computer and mobile device (APWG, 2013; Dimensional Research, 2013). In a similar way, an employee's profile on social media that indicates he/she works in the bank can become a focus of hackers who try to reconstruct or hack an e-mail address and send him/her hyperlinks so that when the link is clicked, it activates some crime ware that infiltrates the e-mail box to extract sensitive information (Balogun & Obe, 2010).

Data ownership violation

Data ownership violation occurs when organization information is being saved or backed up on file-sharing sites such as Google Drive, Dropbox and iCloud, (Uz, 2014). The ownership of data has been entrusted to a third-party service. In the BYOD context, most mobile device users save personal or work documents on file-sharing sites for easy retrieval anywhere and at any time (Mphahlele, 2016). However, Uz (2014) expressed concern over the security of corporate data in file-sharing sites. The implication is that corporate data are out of the employees' control and can be accessed by an unauthorized third party, thus resulting in data leakage (Uz, 2014). Furthermore, this information can be hijacked while uploading. Studies have also indicated that some employees use these services on the organization network without the knowledge of the organization (Balachandran et al., 2005; Uz, 2014).

Disgruntled employees

Disgruntled employees are employees who are not happy with what is happening in the organization (CERT insider threat, 2015). They can be unhappy for having been

dismissed from work, they could be upset for been scolded by their manager or co-employee, and they could be dissatisfied with their current wages. Whichever way, an unhappy employee can be a threat to any organization (CERT insider threat, 2015). In the BYOD context, a disgruntled employee can decide to steal a mobile device belonging to a co-worker with whom he/she has a conflict and log on with his/her credentials (which must have been obtained through a shared password), visiting questionable websites (Gregory, 2011). Thereby, a disgruntled employee may intend to implicate the co-employee by using technology, violating and reporting the person to human resources. An employee usually becomes disgruntled if an expectation is not met or owing to an unfortunate situation e.g. not been promoted (Gregory, 2011).

2.4.3 Mobility threats

Mobility threats refer to those threats associated with device location (Ofusori et al., 2018). “These devices are either connected to secured and unsecured networks where the security policies differ” as cited in Ofusori et al. (2018, p. 224). In addition, a mobility threat also refers to methods used to prepare and dispose of mobile devices. The following security threats are considered for mobility threats as they relate to BYOD, namely lost or stolen devices, e-waste, sharing of the mobile device, unauthorized location tracking, and WiFi eavesdropping.

Lost/Stolen device

According to Karen (2015), lost and stolen devices are the primary concern for allowing BYOD into an organization. Mobile devices are much more vulnerable to be stolen or lost than desktop computers (Tu et al., 2015). Karen (2015) argues that there are over 65 per cent of cases of data breaches which occur owing to a missing device. However, not every device owner understands how and when to remotely wipe off personal or corporate information on the lost or stolen device to avoid security breaches. Although Juniper Network (2011) affirms that the portability of these devices allows people to stay connected while on transit, it can also lead to the incidence of theft or loss.

E-waste

An improperly disposed of mobile device that contains a wealth of useful information such as passwords and customer data can cause a security breach if it falls into the wrong hands (UCSC, 2015). In the context of BYOD, Arregui et al. (2016) assert that mobile

devices are much more susceptible to data leakage if the appropriate security precautions are not taken before disposal. For example, if an employee sells a laptop that contains sensitive information or passes it to someone else without wiping off the information, there is a high risk of exposing data. There are several reports of laptops that contained sensitive data where the information has been retrieved despite the fact that this information had been deleted before selling it (Keys, 2013). A study has shown that deleting information is not effective as such information can still be retrieved (Walters, 2012). Further studies have also revealed that if the recycle bin is “empty”, the information is still there and can be retrieved (Keys, 2013; Walters, 2012). This has caused several security breaches that cause harm to the organization’s system and the customer’s information (Gartner, 2014).

Sharing mobile devices

Most employees lend out their mobile devices that contain sensitive information to family, friends or colleagues without realizing the adverse effects (Karen, 2015). According to Arregui et al. (2016), BYOD users are ignorant of the security risks that may arise from sharing mobile devices with a third party. For instance, when these devices are lent out to friends either to check e-mail, social media or do other personal work, they may come across some confidential information such as bank accounts or a personal identification number (Bunn, 2016). This information can be retrieved and used maliciously without the knowledge of the device owner. In another example, the borrowed mobile device can be used to access malicious WiFi unintentionally and this can open the door for hackers to spoof out confidential information (Mphahlele, 2016).

WiFi eavesdropping

According to Ojeka et al. (2017, p. 341), eavesdropping is the “...unauthorized real-time interception of a private communication such as an instant message, phone call or video conference”. With BYOD, employees can access the Internet via WiFi at any location, and at any time. However, accessing the Internet on WiFi networks at any locations is not secure because cyber-criminals can take advantage of the wireless hotspot to remotely modify messages (Du & Zhang, 2006). “The hackers often create a hotspot with a device and such device is used to compromise a legitimate WiFi network in order to steal the user’s information and in turn hack into the banks’ database or commit online fraud” (Balachandran et al., 2005, p. 266).

2.5 Existing security measures

According to Ofusori et al. (2018), “...there are various types of security measures available to address BYOD security threats and many more are being developed”. These include password authentication (Sree, 2008), encryption (Gharibi, 2012) and firewalls (Kahate, 2013), to mention but a few. However, these existing security measures are insufficient as mobile devices often create diverse sets of security threats that require special or additional control. Hence, it is essential to review some of the existing security measures available and their effectiveness.

2.5.1 Mitigating technical threats

Mitigating technical threats on BYODs requires some technical security measures. Supporting this claim, Shumate and Ketel (2014) argue that before granting mobile device access to an organization’s network, certain security characteristics must be established on the device. Shazmeen and Prasad (2012) also affirm that some security measures must be adopted to reduce the possibility of a security incident. Hence, the following existing security measures for mitigating technical threats on BYODs are discussed.

Password authentication

The use of a password has been instrumental towards protecting confidential information on mobile devices (Acar, Belenkiy & K p c , 2013). The user ID, together with passwords, provides essential protection of information (Ometov, Bezzateev, M kitalo, Andreev, Mikkonen, & Koucheryavy, 2018). This helps to identify the rogue device in a BYOD-enabled environment. According to Ometov et al. (2018), a well-structured multifactor authentication method (e.g. the combination of username/password with personal biometric characteristics or smart card) is more dependable and robust against any external intrusion. However, their usefulness is highly reliant on the enforcement of passwords (Acar et al., 2013).

Encryption

Data encryption helps to prevent data loss in case of phishing, WiFi eavesdropping, data interception and stolen or lost devices in a BYOD-enabled environment (Gharibi, 2012). There are two major categories of cryptographic techniques used for data encryption, namely symmetric key encryption and asymmetric key encryption (Gui-Hong, Hua &

Gui-Zhi, 2010). Symmetric key cryptography, also known as secret key cryptography, is a kind of encryption in which both sender and receiver of a message share a single common key that is used to encrypt and decrypt the message (Gui-Hong et al., 2010; Yadav, 2010). On the other hand, asymmetric key cryptography, also known as public key cryptography, is a method that requires the use of a pair of different keys: a public key and a private key (Gui-Hong et al., 2010). These two keys are complementary to each other but are not interchangeable (Gharibi, 2012). The public key is kept secret and the private key is only known to the owner. The private key remains on the user's personal device and cannot be transferred via the Internet (Yadav, 2010). Hence, a message can be encrypted using either of the keys but can only be decrypted using the other key in the pair. This technique is easy to do one-way but difficult to reverse because of the mathematical function and its algorithm (Gharibi, 2012).

Firewall

A firewall is a software program utilized to protect business resources from external intrusion meant to destroy any electronic devices (Friedman & Hoffman, 2008). According to Clark (2013, p. 59), a "...firewall can be referred to as a security system that controls access to a protected network". It assesses all messages passing through the Internet with the aim of blocking unwanted messages (Kahate, 2013). Thus, for mobile devices firewalls block unauthorized access to mobile communication. However, "...while firewalls can play an important role in detecting the malware, it can, however, be compromised by an unauthorized intruder" (Kahate, 2013, p. 440).

Anti-virus/malware

Anti-virus/malware software is a signature-based software utilized to detect, protect and act against external intrusion into computer devices (Friedman & Hoffman, 2008). Srinivasan (2007) contends that documents must be verified by antivirus software or malware before downloading them. Moreover, their sources must be established to ensure they come from a reliable or trusted source and this necessitates an enterprise to install strong antivirus software to guarantee the security of their systems. However, Friedman and Hoffman (2008, p. 165) identified the following challenges associated with signature-based detection: "...first it can only detect known malware, that is unknown malware cannot be detected. Secondly, the authors of malware create self-modifying malware that alters its own signature every time. Lastly, encryption can disguise the signature of a

malware program”. Hence, antivirus software detection is not a completely reliable form of protection.

Anti-phishing

Anti-phishing is a tool used alongside a browser, an added feature for protecting systems or mobile devices (James & Philip, 2012). They can be used to intercept phishing e-mails and have been proven to be very effective (Gharibi, 2012). Although this approach of intercepting phishing e-mails is also associated with anti-spam, “however, the effectiveness of anti-spam techniques mostly depends on many critical factors such as regular filter training and the availability of anti-spam tools and are currently not used by the majority of Internet users” (Gharibi, 2012, p. 3).

Hardware token

A hardware token is sometimes referred to as a security token. It enables ‘two-factor authentication’ in that the two-factor authentication is based on two important elements e.g. a password and a hardware token (Lorch, Basney & Kafura, 2004). However, despite the use of two-factor authentication, studies have shown that the security features can be bypassed or defeated by a knowledgeable attacker in order to gain access to private data (Goyal, Ishai, Sahai, Venkatesan & Wadia, 2010; Grand, 2000). It can also be compromised when it is stolen or lost.

Encrypted cookies

Encrypted cookies are commonly used to prevent hackers from viewing cookies’ content (Alawatugoda, Stebila & Boyd, 2015). For instance, in a situation where a hacker gains access to a mobile device or computer system and scans for cookies, encrypted cookies deny or prevent the hacker from gaining access to the contents of the cookie. Encrypted cookies are specifically used on an online banking system as additional security for the customer (Atallah & Hopper, 2010). While cookies have been considered to be very useful, some studies argue that they can be abused to impersonate a user privacy and in most cases reveal confidential information (Queiroz & De Queiroz, 2010; Reisman, Englehardt, Eubank, Zimmerman & Narayanan, 2014).

Windows Defender

Windows Defender, formerly known as Microsoft Anti-spyware, was developed by Microsoft Windows to detect and eliminate malware or spyware (Thurrott, 2009). It includes some real-time security agents that monitor several areas of Windows which enables downloaded files to be scanned to ensure that malicious software is not accidentally downloaded (Xie, Han, Tian & Parvin, 2011). However, Thurrott (2009) argues that Windows Defender does not integrate with Firefox or other web browsers and thus cannot be a reliable security measure in the banking sector.

2.5.2 Mitigating social threats

To mitigate social security threats (e.g. malicious insider, user policy violation, data privacy violation, a disgruntled employee) there are some security measures used in most organizations, especially the banking sector, to mitigate these security threats. Some of these include training on acceptable use of ICT policy (Mulligan & Gordon, 2002), training on information security (Enisa, 2014) and enforcement of security policy (Herath & Rao, 2009), to mention but a few. This existing security measure relates to the organization's policies, principles, and values that define the practices of individuals (Ofusori et al, 2018). These social security measures are discussed further in this section.

Training on acceptable use of ICT policy

Acceptable use of policy is set of rules designed by an organization stipulating the practices and constraints that every employee must abide with in order to gain access to the organization's network (Downer & Bhattacharya, 2015). While it is important for employees to abide with the stipulated ICT policy, it is also essential for the organization to give adequate training on the implication of not abiding by the rules (Broughton, Higgins, Hicks & Cox, 2009). This is to guide against user policy violation and data privacy violation. However, there are still some employees that do not get acquainted with this policy (Mulligan & Gordon, 2002).

Training on information security

Relevant information security training is given to employees and executive management to assist in compliance with the terms of policy (Bulgurcu, Cavusoglu & Benbasat, 2010). Nevertheless, some employees still remain nonchalant by carelessly ignoring this security

training and awareness which has led to several security threats, including sharing password and data ownership violation (Enisa, 2014; Yeh & Chang, 2007).

Enforcement of security policies

To prevent any form of data leakage, most organizations enforce security policy on their employees. “Employees are forced to comply with the terms of the policy and where it is confirmed that an employee has violated the policy, such employee is disciplined or reprimanded” (Herath & Rao, 2009, p.113). However, despite the policy enforcement, there are still some recurring security threats which include malicious insiders and disgruntled employees (Bulgurcu et al., 2010).

2.5.3 Mitigating mobility threats

To mitigate mobility security threats such as lost or stolen devices, sharing of mobile devices and e-waste, there some security measures used in most organizations, especially the banking sector, to mitigate these threats. Some of these include mobile device management (Wang et al., 2014), an intrusion detection system (Amer & Hamilton, 2010) and a tracking device (Val, Sam & Jim, 2014). These solutions are further discussed as follows.

Mobile device management

Mobile Device Management (MDM) is used in managing BYODs as an enforcement of security policies in devices that use them as applications (Wang et al., 2014). However, there are two major challenges associated with MDM. “Firstly, it does not separate individual and corporate space on the devices (Wang et al., 2014, p. 83). Secondly, the security policies administered by MDM are on the entire device due to lack of space isolation device” (Wang et al., 2014, p. 83). Hence, employees will no longer enjoy the flexibilities attached with personal space once MDM is used.

Intrusion detection system

An intrusion detection system (IDS) is applied to identify pre-mortem and post-mortem security threats (Amer & Hamilton, 2010). It has a monitoring component that helps to arrest network packets flowing through IDS as well as determining any unwarranted and malicious movement (Scheidell, 2009). IDS sends a malicious signal whenever a

malicious activity is detected and automatically barricades the network transmission coming from the attacker's Internet protocol (Scheidell, 2009).

Tracking device

The ever-increasing ubiquity of mobile technologies has made it easier for employees to move about with their mobile devices and also to respond to official messages while travelling (Val et al., 2014). However, this has also contributed to the high rate of lost or stolen devices. Nevertheless, the banking sector can track and wipe off confidential information on the device with the help of a pre-installed security feature, a global positioning system (GPS) or by using third-party applications (Lee, Park, Chung & Blakeney, 2012; Val et al., 2014). However, Lee et al. (2012) have argued that some mobile devices do not support the use of a GPS and not all banks have a pre-installed security feature on the employees' mobile devices. Thus, there is every possibility that security breaches may occur when a mobile device goes missing.

2.6 Vulnerability in BYOD environment

Despite the numerous existing security measures adopted in a BYOD environment, there are various gaps identified with these security measures. Firstly, in the case of password authentication, González, Tapiador and Garnacho (2008) revealed that although the use of digital signatures could be an effective method for authentication, such methods have significant flaws and are highly reliant on the enforcement of passwords security. In addition, despite the use of two-factor authentication, studies have shown that the security features can be bypassed or defeated by a knowledgeable attacker to gain access to private data (Gui-Hong et al., 2010). Secondly, data encryption with private and public keys is difficult to reverse because of the mathematical function and its algorithm (Gharibi, 2012). Thirdly, Kahate (2013) reveals that a firewall can easily be compromised by an unauthorized intruder. Fourthly, not all employees become acquainted with ICT policy and some have remained nonchalant by carelessly ignoring security training which has led to several security threats (Bulgurcu et al., 2010). Lastly, Lee et al. (2012) argue that some mobile devices do not support the use of a GPS and not all banks have pre-installed security features on the employees' mobile devices. Thus, there is every possibility that security breaches may occur when a mobile device goes missing.

2.7 Related security frameworks

According to Granneman (as cited in Ofusori et al, 2018), "...security frameworks refer to a series of documented processes that are used to define procedures and policies around the ongoing and implementation of information security controls in an organization". These frameworks come in various degrees of complexity and are used to build an information security program to reduce vulnerabilities and manage risks.

2.7.1 ISO/IEC 27000 series

The International Standards Organization (ISO) 27000 is a series of standards on information security (Granneman, 2013). The use of this standard has enhanced information systems protection processes. However, while this framework can be used to establish, implement, monitor and improve the information security management system (ISMS) of an organization, its adoption for security management is minimal because organizations see it as both procedurally and technically challenging (Dobson & Hietala, 2011). In addition, Al-Ahmad and Mohammad (2013) maintain that ISO/IEC 27000 was not designed for the purpose of information security assessment. Hence, it is not suitable for mitigating BYOD security threats.

2.7.2 PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) helps in protecting the cardholder's data as well as maintaining a secure network (Council Payment Card Industry, 2010). According to Al-Ahmad and Mohammad, (2012), it is compulsory for individuals that stores or transmits credit or debit card data to comply with the requirements for PCI. This helps organizations to safeguard consumer data, manage information security risks and reduces losses resulting from fraud (Council Payment Card Industry, 2010). However, Ofusori et al., (2018) argues that PCI DSS is unable to provide protection on BYODs due to its incapability to mitigate against security breaches. Therefore, it does not guarantee the security consciousness that a banking system would depend on for its operations. For instance, every bank would be interested in ensuring that its clientele is protected from any form of losses as a result of fraud or any other malpractices that jeopardize their personal banking information. Hence, PCI DSS does not fit into the objectives of this study.

2.7.3 COBIT

Control Objectives for Information and related Technology (COBIT) developed by the Information Systems Audit & Control Association (ISACA) is a mechanism that establishes information technology control and governance framework for business operations (ISACA, 2011). COBIT can be used to create IT policies, improve IT processes and increase organization effectiveness (Al-Ahmad & Mohammad, 2013; Barlette & Fomin, 2010). In addition, Parvizi, Oghbaei and Khayami (2013) maintains that COBIT can be used to meet an organization's compliance needs as well as to conduct an audit. However, while COBIT is appreciated as a mechanism that provides a necessary framework for IT governance (Tambotoh, & Latuperissa, 2014), it does not take into consideration the methodologies for information security (Ofusori et al., 2018). This makes COBIT framework inadequate in mitigating BYOD security threats.

2.7.4 NIST SP 800 Series

National Institute of Standards and Technology (NIST) Special Publication 800 series is a security framework that assesses the security controls of information systems whilst assessing the risk threshold posed to business operations as a result of exposure to security threats (NIST, 2012). Even though this framework has versatile purposes as far as protection of business operations is concerned (Stouffer, Falco, & Scarfone, 2008; Ross, 2011), it falls short of providing adequate protection to an IT system thereby exposing the entire system to security risks (Ofusori et al., 2018). Hence, this framework is inadequate to address BYOD security threats.

2.7.5 CISCO SCF (Security control framework)

CISCO security control framework is basically designed for assessing the technical risk in infrastructure architecture (Ofusori et al., 2018). The framework consists of a set rules for assessing the design of an information systems to ensure effective operation (Al-Ahmad & Mohammad, 2012). These rules outline the needed requirements to perform an assessment on the security architecture (Al-Ahmad & Mohammad, 2012). However, while CISCO SCF aimed at using appropriate control sets for specific business environments, it does not have an inherent security mitigation mechanism for protecting business operations from security threats (Ofusori, et al., 2018). Hence, it is inadequate as a security framework for mitigating BYOD security threats.

2.7.6 IBM security framework

International Business Machines (IBM) security framework is used to mitigate against business risks associated with data breaches and data losses (Ofusori et al., 2018). It addresses security challenges that relates to physical infrastructure, security governance, network, server and endpoint, people and identity, data and information, application and process, risk management and compliance (Buecker, Borrett, Lorenz & Powers, 2010). However, this security framework, only focuses on the ‘what’ not the ‘how’ and therefore limited to only interpreting user requirements into business solutions, not into specific IT components or solutions (Ofusori et al., 2018). Hence, it is not suitable to be used in a BYOD context to mitigate security threats.

2.8 Challenges in securing BYOD environment

There are several challenges associated with securing the BYOD environment and this creates more concern (Downer & Bhattacharya, 2015, p. 4). However, this study considered the following six major challenges.

Firstly, it is difficult for organizations to distinguish between the organization’s data and private data because the data is mixed (Mphahlele, 2016). While Romer (2014) suggests enforcing the usage of two different mobile devices (i.e. one corporate and one personal) as a way to separate organization data from private data, this strategy was resisted by the employee because it is not convenient.

Secondly, it is difficult to determine how data is accessed and controlled when organizational information is being accessed with personal devices as well as public network connection (Astani et al., 2013). Downer and Bhattacharya (2015) also claim that it can be challenging to limit how many employees’ mobile devices can gain access to certain information at one time and also setting time limits.

Thirdly, monitoring data on devices is complicated as the organization loses sight of the device once it is transferred from the organization’s network to an external network, which may lead to data leakage (Lindström & Hanken, 2018). Furthermore, when an employee stops working with the organization, he/she still keeps the device where the data is stored. However, the organization may not be able to employ certain monitoring tools to wipe data remotely from the device because this may cause conflict with privacy laws since it is considered a personal device (Downer & Bhattacharya, 2015).

Fourthly, it is difficult to implement security measures to protect all devices' hardware and software as well as maintaining secure and stable connections for all devices connected to the network (Downer & Bhattacharya, 2015). This is because extra resources are needed to maintain the required level of security (Lindström & Hanken, 2018). Downer and Bhattacharya (2015) claim that in order to meet these needs, the responsibilities of the security personnel will also increase. In addition, it also requires more time and commitment from the security personnel.

Fifthly, most organizations find it difficult to control and protect the transfer of organization data from mobile devices to public cloud and this has created a security loophole (Downer & Bhattacharya, 2015). This security loophole is heightened when the employee enables the 'remember password' feature on the cloud storage and mobile devices which are out of the organization's control.

Lastly, the local government laws and regulations may limit the levels of organizational control over enforcing security compliance on employee-owned devices (Downer & Bhattacharya, 2015). According to Downer and Bhattacharya (2015), every global organization may need to adjust their BYOD policies to align with the local laws of each country in which they are based. This makes it more difficult streamlining employee contracts.

2.9 Summary

While recommendations towards enforcing the existing security measures and frameworks as a way of addressing BYOD security threats are laudable, these security measures have their shortcomings (section 2.6) and do not sufficiently take into consideration the significant impact of the Fourth Industrial Revolution to accommodate these security threats. In addition, based on the frameworks reviewed, the identified shortcomings are a deterrent to the Fourth Industrial Revolution. "With the Fourth Industrial Revolution, the possibilities of billions of people connected by mobile devices, with unprecedented storage capacity, processing power, and access to knowledge, are unlimited" (Schwab, 2016). These possibilities will continuously increase owing to the emergence of BYOD, and this will further increase the likelihood of the loss of data as well as data contamination (Schwab, 2016). This implies that the organizations have less control over every new device brought into the organization (Twinomurinzi & Mawela, 2014). According to Bello et al. (2015), the major challenge has always been how to

prevent and secure data from being compromised or misused on mobile devices. Hence, a security framework is urgently needed. However, in order to develop a security framework, it is important to first of all understand the theories that guide the use of BYOD in any organization. In chapter three the study will review the relevant theories as they relate to BYOD.

CHAPTER 3: CONCEPTUAL MODEL

3.1 Introduction

This chapter reviews related theories with the aim of conceptualizing an integrated security model. According to Saunders, Lewis and Thornhill (2011), a theory is an established scientific framework that explains various variables (constructs) surrounding a given phenomenon and their interrelationship. A theory may be presented in a research study in the form of a rationale, discussion or an argument which assists to explain any phenomena that occur in any part of the world (Creswell, 2013). Furthermore, a theory may be used in a mixed-method research, either inductively or deductively. By implication, a theory serves as the bedrock upon which the research is built. Hence, this chapter reveals the various related theories used in studies of information systems from which substantial factors supporting an integrated model for BYOD security were identified. The chapter concludes with a discussion of adaptable theories relating to the need for an integrated security model.

3.2 Related theoretical models

There are several theoretical models in information systems literature that suggests important factors which are useful for an integrated model. These theories provide better comprehension and enhanced visualisation of an integrated security model. Hence, this section discusses the theories that are relevant to the research study which helps to form the foundation upon which the model is built.

3.2.1 Protection motivation theory

Catherine (2010) describes protection motivation theory (PMT) as an explanatory theory that is used in predicting behaviour. This theory was developed by Rogers (1975) and it is used to provide a better understanding of the effects of fear appeals and how people cope with them. This is an extension of cognitive processing and expectancy-value theory (Maddux & Rogers, 1983). PMT has been applied in different studies but especially in personal health contexts (Catherine, 2010). Maddux and Rogers (1983) point out two main aspects of this theory, namely threat appraisal and coping appraisal. “Threat appraisal relates to users' assessment of the level of risk that results from having a careless manner in contracting the disease (perceived vulnerability) and the seriousness (perceived

severity)” (Catherine, 2010, p. 625). Coping appraisal refers to how the user manages the risk (Woon, Tan & Low, 2005). The self-efficacy is an important aspect of coping appraisal. It refers to users' behaviour towards minimizing the risk (Ifinedo, 2012). PMT has been widely used in health sciences, but only a handful of researchers in the field of information technology have tested the theory (Ifinedo, 2012). While Putri and Hovav (2014) applied PMT to investigate employees' compliance with information security policy, Dang-Pham and Pittayachawan (2015) used PMT to examine the students' attitude regarding malware threats in a BYOD-enabled university. However, PMT was not used in this study because this study does not intend to measure individual attitudes towards compliance to information security, but to identify security threats associated with a BYOD-enabled environment in order to develop a security framework to curb these security threats. Hence, PMT was not suitable for this study.

3.2.2 Technology threat avoidance theory

Technology threat avoidance theory (TTAT) was proposed by Liang and Xue (2009) in order to explain the behaviour of individual IT users that engage in threat avoidance behaviours. TTAT explains how and why individual IT users try to avoid the threat of malicious information technologies (Arachchilage & Love, 2014). While most studies examined IT security at organizational level, TTAT examined IT security at an individual level. This theory was developed to synthesize literature from different areas of study which include risk analysis, information systems, psychology and health care (Liang & Xue, 2009). TTAT has been found to be useful in explaining user avoidance behaviour through the cybernetic theory and coping theory. For instance, Arachchilage and Love (2014) used TTAT to investigate users' self-efficacy to avoid phishing threats. However, TTAT was not used in this study because this study does not intend to measure the factors influencing threats avoidance in a BYOD-enabled environment but to explore individual and organization practices in identifying BYOD security threats with the aim of developing a security framework for the banking sector. Hence, TTAT was not appropriate for this study.

3.2.3 Security risk perception model

The security risk perception model was first introduced by Alexandrou and Chen (2015) to examine the adoption of mobile devices in medical institutions. This theory was used

to gain a better understanding on how healthcare practitioners perceive the risks associated with mobile devices as they relate to BYOD (Alexandrou & Chen, 2014). This theory postulates that each healthcare practitioner has specific security beliefs that could indirectly impact their behavioural intentions to use the devices. This compels the healthcare practitioner to adopt security controls while using the device (Alexandrou & Chen, 2014). Furthermore, Alexandrou and Chen (2014) explore the various factors influencing each healthcare practitioner's security risk perception on mobile devices and their intention to comply with security controls. In this regard, there is a Health Insurance Portability and Accountability Act (HIPAA) with which the healthcare practitioners are expected to comply. The HIPAA emphasizes the importance of protecting the confidentiality of individuals' medical records. However, it is important to note that the key focus of this study is to develop a security framework for the banking sector which can only be achieved by identifying the security threats associated with a BYOD-enabled environment. Hence, the security risk perception model was not used for this study because it is mostly used for explaining users' perceptions and adoption and does not meet with the objectives of this study.

3.2.4 Organization theories

Organization theories originate from organizational practices and they explain how individuals and groups of people behave in differing organizational arrangements (Yang, Liu & Wang, 2013). It captures the diversities of organizational structure and operating processes (Robbins, 1990). Furthermore, organization theories are knowledge systems which study and explain organizational group behaviour and individual behaviour (Czarniawska, 1999). While some studies have used organization theories to focus on individual and small groups within the context of an organization, other studies have used organization theory to deal with macro-level analyses of organization-wide concepts, intergroup relationships, and organization environment interactions (Yang et al., 2013). This theory contends that in those instances where organizational policy is flouted or abused by employees, it exposes the organization to potential security threats that make the organization vulnerable (Yang et al., 2013). In this regard, organization theory helps to understand the linkages between individual and organization practices in exploring BYOD security threats in the organization. This theory links such practices to security concerns that may impair the organization security system capacity to detect such harmful

security threats. Hence, this study adopts organization theories in investigating organization and individual practices in the context of a BYOD-enabled environment.

However, Yang et al. (2013) argue that organization theories only focus on how groups and individuals behave in differing organizational arrangements but do not capture how technology influences this behaviour or practices. Hence, organization theory has to be used along with other theories that incorporate technology. Thus, to fully understand how technology influences individual and organization practices while using mobile devices at work, it is important to review other theories that explain this interrelationship.

3.2.5 Social-technical theory

According to Bostrom and Heinen (1977), the socio-technical design principle was formulated by Cherns (1976). The socio-technical theory implies that organizations are made up of people and technology coming together to create an environment for the success or failure of the organization (Figure 3.1). Socio-technical theory explains mobile devices as productive working tools that are important in any social system so that they are not regarded as purely technical artefacts and the organization as a separate social entity. Urry (2012) holds the same view which suggests that using mobile devices as working tools can increase productivity if they are used as socio-technical tools with the right training and education, the right controls and the right mobile policies put in place (Nunoo, 2013). However, some employees use this device as though it was either a purely social artefact or a purely technical artefact (Nunoo, 2013). They do not seem to understand it as a socio-technical tool that can increase both the social and technical aspects of their working lives if managed as a socio-technical artefact (Akbari & Land, 2011).

Hence, this study has noted the unique contribution of socio-technical theory and will be adopting the social and technical constructs for the following reasons; firstly, to explain how the reciprocal interrelationship between technology and people creates an environment for either the success or failure of the organization; secondly, to explain the theoretical constructs for the social aspect resulting from interactions among people and technical aspects resulting from the technology used in the organization. The social construct will also be used to identify the security threats associated with employees' interaction, knowledge skills, attitudes, values and organization policies as they relate to

BYOD practices. In addition, the technical construct will be used to identify the security threats associated with the technical knowledge regarding the use of mobile device as well as from BYOD hardware and software technology used for work purposes. Lastly, socio-technical theory will be used to explain how the work system and its environment also lead to joint optimization.

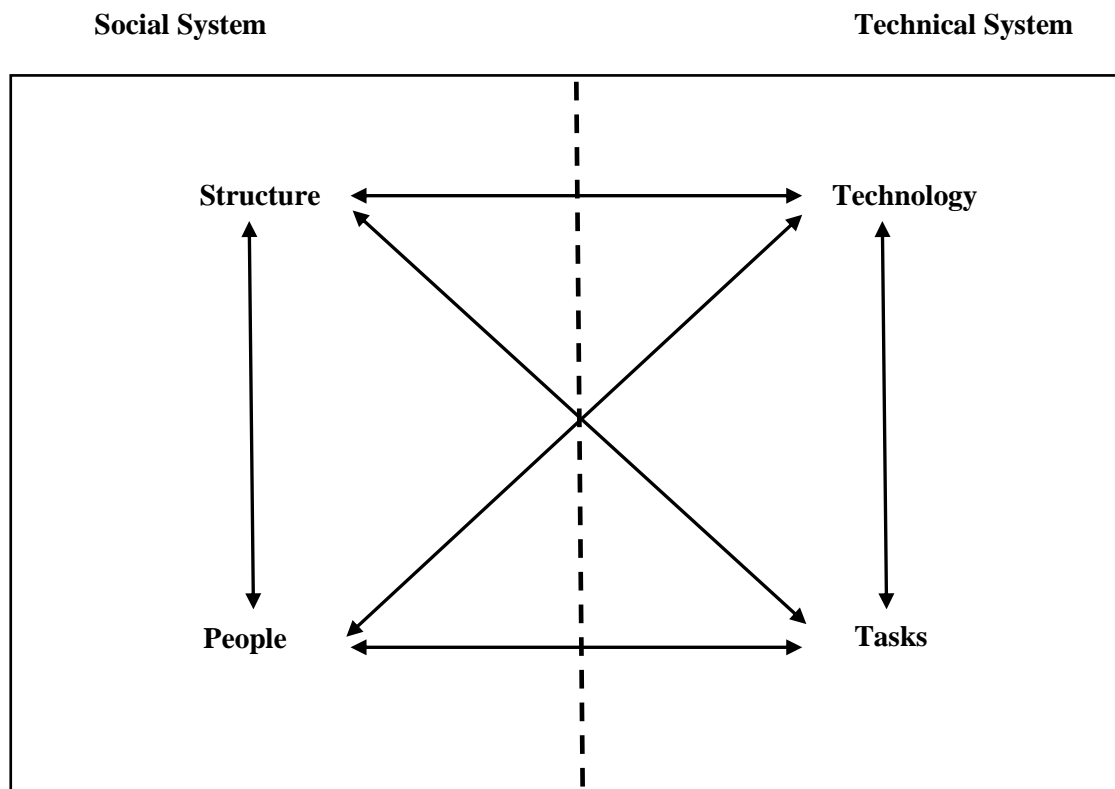


Figure 3.1: Socio-technical system (Bostrom & Heinen, 1977)

However, despite the socio-technical contribution to the society, Chen and Nath (2011) argue that there is no comprehensive mobile workforce framework that incorporates key issues from the technical, managerial, behavioural and cultural perspectives. Though the socio-technical framework incorporates bits of technology into our social environments, mobility and the problems associated with it are not handled properly (Chen & Nath, 2011). With this in mind, socio-technical theory is not sufficient to be used alone because it does not effectively incorporate mobility and the problems associated with it. Hence, the following section discusses mobility theory which encompasses the movement of people and objects and their interrelationship.

3.2.6 Mobilities theory

Hannam, Sheller and Urry (2006) define mobilities as a concept that deals with the massive movement of humans, information and objects across the globe and local environment. Urry (2012) holds the same view by defining mobilities as a model in the social sciences that investigates the movement of humans, ideas and objects, and the broader social implications of those movements (Urry, 2012). The social perspective of mobility mainly refers to the issues of movement and it examines the movement of objects, people and work in terms of space, place and time (Kakihara & Sørensen, 2001). On the other hand is the technical perspective of mobility: most tools and facilities in the office or at home have been reduced significantly to a smaller size and can be carried anywhere, making people geographically independent within the next decade. It is claimed that the usage of such devices enables people to travel freely and live wherever they wish (Makimoto & Manners, 1997). Most employees travel and respond to work-related business via their portable devices, especially their smartphones. Hence, this study adopts the mobility theory for the following reasons: firstly, to understand the concept that makes people travel with their mobile devices and exchange information including organizational data while travelling; secondly, to understand how mobility has influenced the way people interact; and lastly, to explain the implications of those movements.

The mobility construct will be used to identify the security threats associated with employees' location while using their personal devices for work purposes. Nunoo (2013) asserts that employees that travel with their mobile devices mostly used them to access open WiFi and not all these WiFi hot spots can be trusted. Some of these open connections are owned by malicious hackers who are sniffing around for any confidential data they can lay their hands on which could be used to blackmail the organization into giving them what they want or could be used against the organization to compromise its trustworthiness to the public. In addition, Urry (2012) also argues that mobility naturally influences the way entities interact. It is worth mentioning that security challenges cannot be fully addressed without analyzing mobility as this concept is changing the underlying theories of information systems, especially from the point of view of confidentiality, integrity and availability. According to Basole (2004), human interaction can be transformed through mobility and defined along spatial, temporal and contextual dimensions (Figure 3.2).

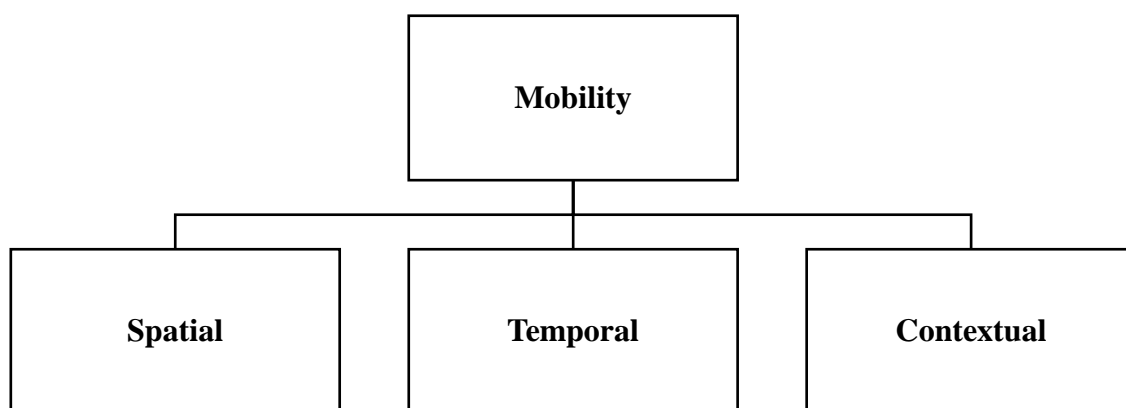


Figure 3.2: Dimension of mobility (Basole, 2004)

The spatial dimension examines human behaviour in relation to geographical locations (Basole, 2004). The temporal dimension enables time savings as well as allowing multiple activities to be conducted simultaneously and instantaneously (Hammer & Mangurian, 1987). Contextual dimension refers to “...the situation and environment in which humans perform their activities” (Basole, 2004, p. 3). More specifically, the contextual dimension provides explicit knowledge regarding the way and the circumstances in which the activity is being carried out.

Despite the benefits of mobility theory from different dimensions such as spatial, temporal and contextual, the theory suffers some limitations. Kakihara and Sørensen (2001) argue that there is a misconception about the mobility system as it only deals with human geographical movement and such a view is insufficient to capture the complicated reality emerging from the mobility system of our social lives. Hence, this study takes into cognizance the various dimensions of mobility and will be using mobilities theory as a construct that focuses on location or human geographical movement. This construct will be used along with other constructs in socio-technical theory as well as organization theory.

3.3 Conceptual model

This study adopts three basic theories as a foundation on which the conceptual model was developed. Organization theory was used to explain organization and individual practices as they relate to BYOD. Secondly, socio-technical theory was used to place the mobile devices as productive tools that are important in any social system so that they are not

seen as purely technical artefacts and the organization as a separate social entity. Socio-technical theory indicates that organizations are made up of people and technology coming together to create an environment for the success or failure of the organization (Walker, Stanton, Salmon & Jenkins, 2008). This knowledge helps to position personal mobile devices in their rightful place from a business perspective and helps incorporate the most relevant parts of the surrounding context into the analysis thereby creating conditions for successful performance at the workplace. Thirdly, mobilities theory was used to provide a basis for human geographical movement (Urry, 2012). Figure 3.3 presents the conceptual model that incorporates the three theories adopted.

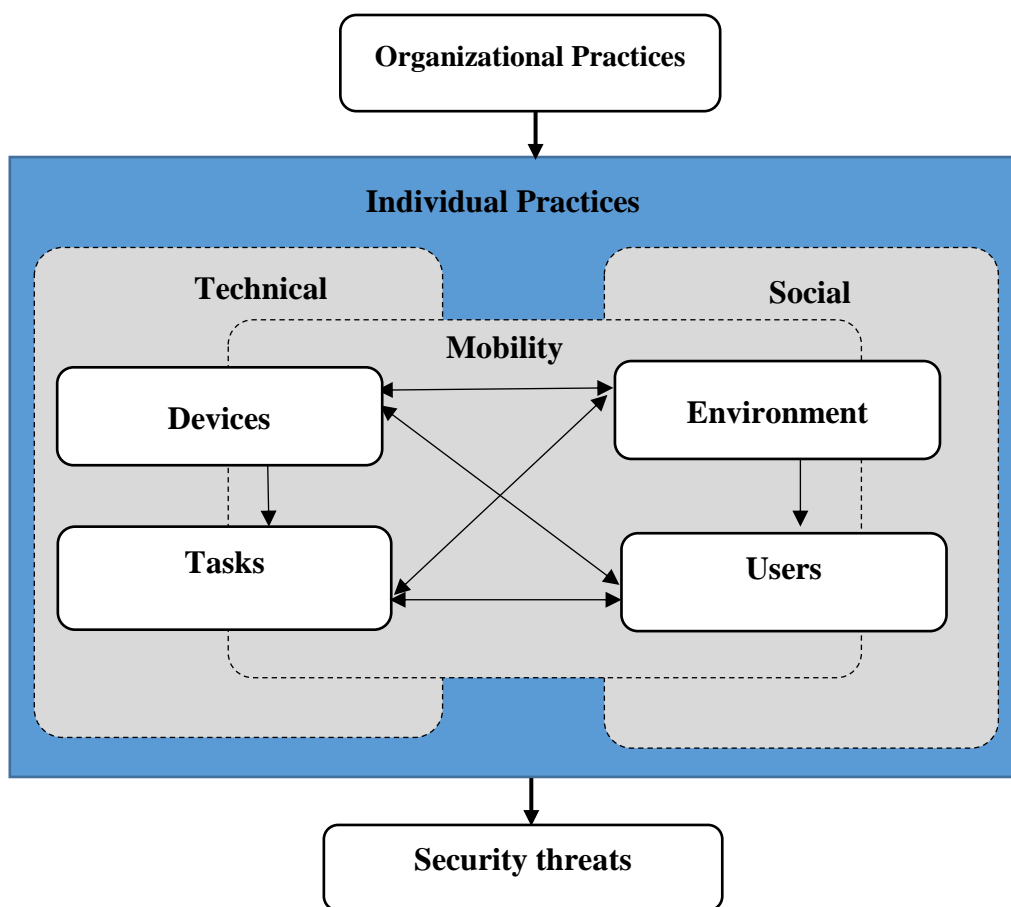


Figure 3.3: Conceptual model (Source: Author's own)

The organization practices have to do with the concept of allowing the BYOD trend in the Nigerian banking sector. This organization practices has a way of influencing the individual practices. However, the individual practices explore the interplay between the social, technical and mobility domains as they relate to the usage of mobile devices. These

mobile devices include those owned by individuals (employees) and/or the organization (bank).

The technical domain is influenced by two constructs, namely *devices* and the *tasks* (Chern, 1976). The ‘devices’ are used as a working instrument in the banking sector. These devices support the operation of the bank that enables communication and workflow, while the ‘task’ refers to the work the employees are expected to do and also how to get the work done. For example, if the work unit is a marketing department, the key tasks could be travelling out of the work environment to advertise or market the banks’ product and services to customers in other organizations. This could be a routine task (Nunoo, 2013).

The social domain is influenced by two constructs, namely the *environment* and the *users* (Chern, 1976). The ‘environment’ represents the structure (i.e. organization) where the employees carry out their official duties and communication while the ‘users’ represent the employees who are often the key consideration in any change initiative. They actively perform any given tasks with the use of technology and their beliefs, attitudes, skills, behaviours, and work policy greatly affect the success of change in any organization.

The mobility domain is significant to this study because of the overlap of mobility between the technical and social domains. This overlap explains the interplay between the technical and social domains in the context of employees’ movement from one location to another while using their mobile devices in performing official duties, possibly leading to security threats. Mobility was used to gain an understanding of the concept that makes people travel with their mobile devices and exchange information, including organizational data, while travelling (Urry, 2012). The risks associated with regard to exchanging organizational information with their personal devices while travelling were investigated. Based on the conceptual model, security threats that are associated with the three dimensional domains were identified.

3.4 Summary

This chapter presented the relevant theories in order to discover and identify the key research issues related to the BYOD phenomenon. The review approach can be viewed

as an ensemble method that combines three sets of theories which learn from past literature and observations. Drawing upon the existing theories reviewed, there is no single theory or model that sufficiently explains the variables (constructs) surrounding the BYOD phenomenon and its interrelationship with organization and individual practices for the following reasons.

Firstly, organization theory only focuses on how groups and individuals behave in differing organizational arrangements but does not capture how technology influences these behaviours or practices (Yang et al., 2013). Secondly, the socio-technical dimension helps to explain the concept of a work unit (organization) being made up of both the social and technical elements which is open to its environment, but it does not capture mobility and the problems associated with it (Chen & Nath, 2011). Lastly, mobility theory focuses only on human geographical movement and such a view is insufficient to capture the complicated reality emerging from the mobility system of our social lives (Kakihara & Sørensen, 2001).

Hence, the researcher combined the three theories, namely organization theory, and socio-technical and mobility theory so as to hypothesise the conceptual model for the Nigerian banking sector which will eventually add to the body of knowledge.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

Rajasekar, Philominathan and Chinnathambi (2006) define research as the procedure of discovering novel information on a particular topic. Research helps to provide answers to questions, solutions to problems or to gain more knowledge about a certain subject (Saunders & Tosey, 2013). Conversely, Van Wyk (2012) refers to research methodology as the procedures and approaches adopted when carrying out a research study. The research procedures and approaches used in this study to identify the security threats associated with a BYOD-enabled environment is informed by the research onion which was developed by Saunders, Lewis and Thornhill (2009). The summary of the research process establishing the research methodology is shown in Figure 4.1.

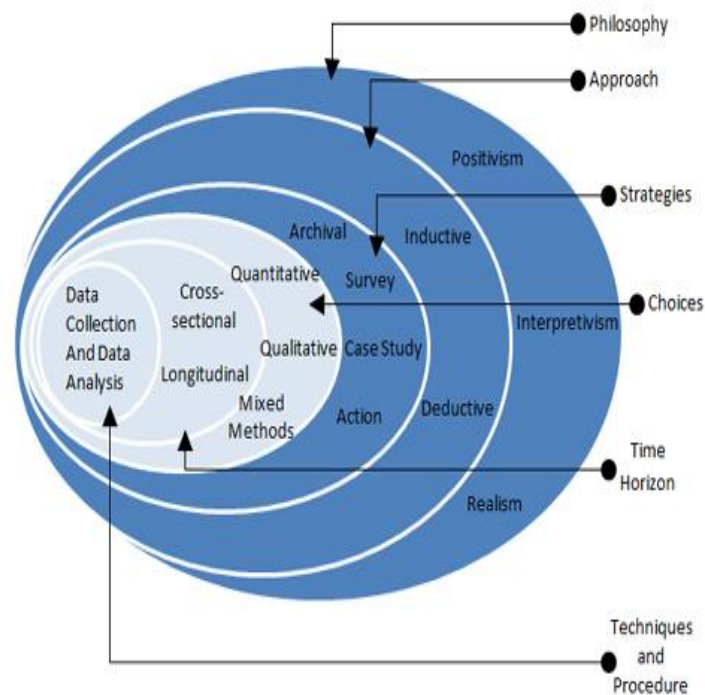


Figure 4.1: Research onion (Saunders et al., 2011, p. 108)

The research process and procedures such as research philosophy, research approach, research strategy, research design, techniques and procedures adopted in this study are elaborated in the various sections of the chapter to answer the research questions which are stated as follows:

1. What are the security threats associated with the technical system in the banking sector of Nigeria?
2. What are the security threats associated with the social system in the banking sector of Nigeria?
3. What are the security threats associated with the mobility system in the banking sector of Nigeria?
4. How does the security threat regarding the technical, social and mobility systems influence the banking sector of Nigeria?
5. How do the recommended security measures help to mitigate the security threats?

4.2 Research philosophies

Saunders et al. (2011) defines research philosophies as worldviews or different types of beliefs about a chosen enquiry which give rise to the design, process, strategies and methods of reinvestigating an existing knowledge on the construct or the object. This study discusses research philosophies in line with the views of Saunders et al. (2011, p. 108).

Positivism is commonly referred to as an objective research strategy which often follows the path of natural science (Saunders et al., 2011). Realism is a type of research philosophy that observes two specific features of positivism: an orientation that is totally different from the object that is being investigated, and an assumption that social and scientific science research must use the same method of data collection (Bryman & Bell, 2015). Interpretivism emphasizes the necessity to cut down the difference between what is being researched and the researcher as one social actor (Kelliher, 2011; Saunders et al., 2011). In addition, according to the literature, pragmatism relies on situations, actions and consequences (Creswell, 2013, p. 10). “Pragmatism argues that the most important determinant of the research philosophy adopted is the research question – one approach may be ‘better’ than the other for answering certain questions. Moreover, if the research question does not suggest unambiguously that either a positivist or interpretivist philosophy is adopted this confirms the pragmatist’s view that it is perfectly possible to work with both philosophies” (Creswell, 2013, p. 10). Pragmatism uses mixed methods to provide solutions to research questions and problems rather than focusing on information about truth and reality (Creswell, 2013). It emphasizes mixed methods to

produce better results. This implies that mixed methods, both qualitative and quantitative, are possible within one study.

Therefore, this study adopts the pragmatic philosophy for the following reasons; firstly, because it is a mixed-method research philosophy that addresses a real-world problem. Hence, it offers better results and is helpful in answering the study research questions. These research questions are considered suitable for mixed-methods research and especially for information systems and social science (Goodyear & Retalis, 2010). Venkatesh, Brown, and Bala (2013), assert that pragmatism is more applicable to research in information systems. Secondly, the study requires a high level of objectivity and for this reason the pragmatic approach was found to be most suitable. Lastly, pragmatic philosophy facilitates data triangulation. Data triangulation is essential in mixed-methods studies for data verification because it leads to better data collection, analysis and interpretation of results which produces outstanding results (Creswell, 2013). Venkatesh et al. (2013) and Goodyear and Retalis (2010) argue that while quantitative and qualitative studies are based on deductive and inductive reasoning respectively, pragmatism is based on abduction which falls between the two. Their argument is based on the fact that abduction moves forward and backward between deduction and induction, making it suitable for addressing real-world problems through a mixed-methods approach. The mixed method approach is further discussed in section 4.3.

4.3 Research approach

According to Saunders et al. (2011, p.108), "...research approach is an orderly and systematic move taken towards the allocation and analysis of data so that information can be obtained". There two types of research approaches, namely inductive and deductive approaches. Trochim and Donnelly (2001) define an inductive approach as starting with the specific and ending with the general. Arguments based on observation or experience are said to be better expressed inductively. It is a bottom-up approach which is mostly concerned with the methods of data collection to obtain un-mediated information on a phenomenon (Saunders et al., 2011). This obviously explains the reason why a qualitative approach is an inductive inquiry, especially with the use of observation and interviews to gain in-depth knowledge which inductively contributes to the body of knowledge (Goulding, 2002; Kelliher, 2011).

However, Soiferman (2010) defines a deductive approach as moving from the general to the specific. Studies have shown that arguments based on rules, laws or other related principles are best expressed deductively (Saunders et al., 2011). It is a top-down approach of scientific inquiry into the literature review which requires an understanding of the relationships among the variables (Saunders et al., 2011). This approach enables scientific methods of data collection which are subject to statistical analysis and also deductively contributes to the body of knowledge (Bryman & Bell, 2015). The major advantage of this approach is that it is highly objective while the major disadvantage is that owing to the rigorous statistical analysis and complex scientific methodology, it may not always be needed in social or management sciences research (Saunders et al., 2011).

Hence, this study combines both deductive and inductive research approaches because it has been found useful to combine these two approaches. While the questionnaire was used to collect data which deductively contributes to the body of knowledge, interviews were also used to gain in-depth knowledge which inductively contributes to the body of knowledge (Saunders et al., 2011). The integrated approach of deductive and inductive methods in a single study is referred to as mixed methods (Creswell, 2013). Therefore, the researcher selected this approach as the most appropriate approach to investigate the security threats associated with BYOD security threats in the Nigerian banking sector.

4.4 Research choices

Creswell (2013) categorized research choices into three, namely quantitative, qualitative and mixed methods. The quantitative approach is characterized by the use of numbers and closed-ended questions as opposed to the use of words and open-ended questions or interviews on which the qualitative approach centres (Creswell, 2013; Kumar, 2011). However, in developing theories it has been found useful to combine these two approaches, which is called mixed methods (Saunders et al., 2011). A mixed-methods approach involves the “mixing” of qualitative and quantitative data and integrating both within a single investigation (Creswell, 2013). This study adopts a mixed-methods research approach in addressing the research questions for the following reasons:

Firstly, it provides an in-depth and a richer understanding in identifying the security threats associated with technical, social and mobility domains as they relate to the

BYOD phenomenon in the Nigerian banking sector. It is important to note that different respondents and organizations may have different practices, views and experiences when using mobile devices in a BYOD-enabled environment. Hence, in order to achieve the objectives earmarked for this study, the quantitative approach employs closed-ended questions to explore individual practices and identify BYOD security threats. This was administered to a large sample of employees. On the other hand, a qualitative approach employs a face-to-face interview to explore organization practices and identify BYOD security threats as well as how these security threats are being mitigated. This was directed to a small number of employees, thus, enabling the development of a security framework for the Nigerian banking sector.

Secondly, it enables the simultaneous collection of quantitative and qualitative data (Hanson, Creswell, Clark, Petska & Creswell, 2005). The qualitative data for this study was used to support the quantitative data, hence preventing intrinsic bias that arises from a single method (Fidel, 2008). Thirdly, a mixed-method approach helps the researcher to understand the study's problem statement. Fourthly, a mixed-methods research approach also offers an opportunity for equal or skewed priority to be given to quantitative and qualitative data (Creswell, 2013; Hanson et al., 2005). In this study, higher priority was given to quantitative data: through this, generalisation of the study findings can be proposed. Lastly, it creates an avenue for separate analysis of quantitative and qualitative data which was later integrated at the interpretation stage. Hanson et al. (2005) noted that mixed methods enable quantitative (numerical) and qualitative (non-numerical) data to be collected and analysed either concurrently or sequentially, depending on the study's research questions and objectives as well as the problem statement. Thus, a mixed-methods approach was considered more suitable as it falls in line with the philosophical worldview of the study (Creswell, 2014). Two phases are considered in this study; the first phase is the threat identification which led to the development of a security framework, while the second phase is the framework evaluation.

For the first phase (i.e. threat identification) of the study which addressed the research questions, a quantitative approach was first of all used to gather information regarding individual practices as well as to identify the security threats associated with

technical, social and mobility domains as they relate to a BYOD-enabled environment. This was followed by a qualitative approach to ascertain organization practices and identify BYOD security threats as well as identifying the mitigating strategies. This implies that the first phase of the study followed the sequential mixed-methods research design. The sequential mixed-methods research design enables data to be analysed separately but integrated at the interpretation stage, enabling data triangulation in the course of the investigation (Hanson et al., 2005). The outcome of the data analysis and the interpretation gave rise to the development of a security framework (chapter 7).

In the second phase (i.e. framework evaluation) of the study, data was collected utilising numerical (quantitative) and non-numerical (qualitative) approaches, including a structured questionnaire containing closed and open-ended questions. This was administered to eight executive management staff (i.e. two each from the four participating banks) and four academic staff of information systems and technology (i.e. one each from four different universities) to evaluate the developed security framework and ascertain whether it meets the required criteria. Hence, the second phase of the study followed the concurrent mixed methods research design (Creswell, 2013).

4.5 Research strategy

Research strategy refers to the different strategies employed for data collection in order to draw realistic deductions (Azika, 2008). The diverse strategies involved in conducting a research study include case study, experimental, action, archival, ethnographic, grounded and survey research strategies.

A case study research strategy is mostly used for qualitative research but can employ both qualitative and quantitative methods for data collection and analysis (Saunders et al., 2011). The experimental research strategy is mostly adopted when dealing with both laboratory and field experiments (Sekaran & Bougie, 2009). Action research is a research strategy with the dual purpose of action and research (Dick, 1993). In other words, action research is either initiated to solve an instant problem or to reflectively solve a progressive problem. Archival research strategy involves the study of historical and administrative documents of organizations as a source of data collection (Saunders et al., 2011, p. 150).

An ethnographic research strategy employs an open-ended strategy to investigate meaning rather than using scientific approach to measure the phenomena (Saunders et al., 2011, p. 149). Grounded research is helpful to explain and predict behaviour or social phenomena or constructs (Creswell, 2013, p. 13). A survey research strategy is a type of research strategy that is frequently used in social science (Badke, 2004). It is mainly used to collect quantitative data but can also be used to collect qualitative data using open-ended questions or interviews. This type of research strategy is very flexible and is mostly used to gather various forms of data from large or small numbers of people (Badke, 2004).

This study adopts the survey research strategy for the quantitative approach for the following reasons. Firstly, the study used probability sampling techniques to draw an appropriate sample size from the population of the study in order to provide a numerical explanation or description of trends, attitudes or behaviour (Creswell, 2013; Maylor & Blackmon, 2005). The participating commercial bank branches were selected using simple random sampling. With this research strategy, there is the possibility of generalizing the study findings to the entire population. Secondly, a survey approach is flexible and can be used to gather different forms of data from a large population (Badke, 2004). Drawing upon its flexibility, the study explores the interplay between individual practices and the security threats experienced as they relate to the technical, social and mobility domains of BYOD. Thirdly, a survey research strategy allows respondents to remain anonymous. Hence, this current study allows respondents to remain anonymous based on requests for anonymity from the four participating banks. Lastly, a survey research strategy enables data to be subjected to statistical analysis using both descriptive and inferential statistics after which the outcomes are interpreted, conclusions are drawn and recommendations are provided (Sekaran & Bougie, 2009).

On the other hand, a grounded theory research strategy was used in this study for the qualitative approach. This enables the themes to be generated that could be used to support or as points of comparison for the quantitative study (Creswell, 2013; Leedy & Ormrod, 2014). Grounded theory provides guidelines on how to identify the associations between variables and how to develop a theoretical framework. This suggests that the guidelines can be adopted as a flexible tool (Creswell, 2013). According to Saunders et al. (2009, p. 149), grounded theory is better seen as a set of systematic inductive strategies for conducting qualitative research which leads to ‘theory building’.

4.6 Research design

“A research design refers to the plans and procedures which cover the entire decisions from broad assumptions through the methods of collecting data to the data analysis” (Creswell, 2013, p. 20). There are three kinds of research designs, namely exploratory, explanatory and descriptive (Van Wyk, 2012). An exploratory research design is a unique way of enquiry into what is happening and to find out new insights on a particular phenomenon (Sekaran & Bougie, 2009). It is useful in investigating a problem and providing a solution to the problem at hand (Saunders et al., 2011). A descriptive research design is an extension of exploratory research design that is used to expatiate on arguments or discussions (Saunders et al., 2011). It provides adequate description of the features of phenomena or variables of interest (Sekaran & Bougie, 2009). It is sometimes referred to as descripto-explanatory studies (Saunders et al., 2011). An explanatory research design is a study that builds relationships between variables (Saunders et al., 2011). Based on the nature of research questions, an explanatory study may be mixed methods or qualitative or quantitative (Bryman & Bell, 2015; Creswell, 2013; Sekaran & Bougie, 2009). Data can be subjected to statistical tests (correlation); this gives a better view of the relationship (Saunders et al., 2011). Furthermore, explanatory studies can be used to predict outcomes (Sekaran & Bougie, 2009).

An explanatory research design was therefore an appropriate design for the study because the study seeks to identify the security threats on the variables (technical, social and mobility) and how they influence the Nigerian banking sector based on the individual and organization practices that are propelled by the BYOD phenomenon. In addition, the data collected from the variables can be subjected to statistical tests as well as thematic analysis and this gives a better view of the relationship (Saunders et al., 2011). The study then classified these variables to gain an understanding of how they influence the Nigerian banking sector.

4.7 Research time horizon

According to Saunders et al. (2011, P. 110), a research time horizon “...refers to the length of time it takes for a scholar or researcher to collect data”. There are two types of time horizons, namely a longitudinal and a cross-sectional time horizon. A longitudinal time horizon research requires data collection more than one time in order to provide

answers to the research questions (Saunders et al., 2011; Sekaran & Bougie, 2009), while a cross-sectional research study only requires data collection at a particular time and is thus less expensive than a longitudinal study (Saunders et al., 2011; Sekaran & Bougie, 2009). Cross-sectional studies are commonly adopted by students in academic research for the award of degrees in management or related fields because of the time horizon: they require less time and expense for data collection (Wilson, 2014, p. 112). Hence, this study adopts the cross-sectional time-horizon approach because it uses a survey research strategy and data collection for threat identification and framework evaluation, and this was done within a short period of time.

4.8 Sample design

The term sample design refers to a road map that guides the selection of the survey sample as well as other important aspects of the sample which include the target population, study site and sampling techniques (Thomas, 2010). This section presents detailed explanations of the selected sample design used in this study.

4.8.1 Study site

The study was conducted in Lagos State, Nigeria. Lagos State is located in the southwest geo-political zone of Nigeria. The reasons for choosing Lagos State is that it is the commercial nerve centre of Nigeria and also the headquarters of the participating banks; this makes the city an appropriate enterprise hub connecting local banking sectors with the global firms. There are four banks involved in this study. The researcher maintained the anonymity of the four participating banks in Lagos State by using pseudonyms. The decision for concealing the names of the four participating banks was based on a request from the four banks to remain anonymous. Hence, pseudo-names such as Bank A, Bank B, Bank C, and Bank D were used to conceal the identity of participating banks throughout the study. Similarly, for the framework evaluation, the study maintained the anonymity of the four cybersecurity experts and researchers in academia across the countries by using pseudo-names such as Academic Expert 1, Academic Expert 2, Academic Expert 3 and Academic Expert 4.

4.8.2 Target population

The target population of a study can be referred to as a group of people the researcher wants to investigate (Sekaran & Bougie, 2009). Thus, in the context of this study, the target population refers to the clerical employees who deal directly with the customers and the executive management (executive managers and ICT department personnel) in the four banks under study. Thus, the estimated research population as at the fourth quarter of the year 2017 was 4,163 employees across the four participating banks in Lagos State, Nigeria. It is important to note that the study had a pyramidal structure. The beginning (threat identification) was broader in scope and it then narrowed towards the end (framework evaluation). Therefore, the target population for threat identification was 4,163 employees consisting of employees and executive management. However, for the framework evaluation, twelve participants were considered. This includes eight executive managers of the four participating banks (i.e. two each from the four participating banks) and four cyber security experts or researchers in academia across four different universities in the country. It is important to note that two of these participants are within South Africa, while two are outside South Africa (i.e. one from Nigeria and another from the United States of America [USA]).

4.8.3 Sampling and sampling techniques

According to Kumar (2011, p. 193), sampling is “...the process of selecting a few (sample) from a bigger group (population) to become the basis for estimating or predicting the prevalence of an unknown piece of information, situation or outcome regarding the bigger group”. It is a process of selecting a subset from the study population (Gill & Johnson, 2010; Sekaran & Bougie, 2013).

There are two categories of sampling techniques, namely probability and non-probability sampling (Sekaran & Bougie, 2009). Probability sampling can be defined as sampling in which each element in the population has an equal or non-zero chance of being selected in the sample (Sekaran & Bougie, 2009) while non-probability sampling can be defined as a sampling method in which the techniques are based on a non-statistical or subjective approach in selecting a sample (Sekaran & Bougie, 2009; Wilson, 2014). A simple random sampling technique is an example of probability sampling which requires that

every element of the study population has the same opportunity of being selected (Sekaran & Bougie, 2009).

Hence, this study adopts the simple random sampling technique in which the branches of the four participating banks in Lagos, Nigeria were selected randomly for the quantitative approach. This offers a high level of reliability and reduces the level of biases while making generalizations in relation to the total population (Bryman & Bell, 2015; Sekaran & Bougie, 2009). Based on the information obtained from the banks' documents, Bank 'A' had 76 branches, Bank 'B' had 79 branches, Bank 'C' had 73 branches and Bank 'D' had 71 as at the fourth quarter of 2017 in Lagos State, Nigeria. Hence, 10 branches were drawn at a regular interval of seven from each list of the bank branches. Thus, 40 branches were selected in all from the four participating banks' branches. This method enables each branch on the list to have an equal probability of being selected. Ninety-five (95) copies of the questionnaires were assigned to each bank and were later distributed to various branches in line with purposive sampling.

Purposive sampling is an example of a non-probability sampling technique. Purposive sampling allows participants to be selected based on their knowledge and experience of the phenomenon under investigation (Sekaran & Bougie, 2009). Hence this study adopts the purposive sampling technique for the qualitative data in order to draw samples based on the respondents' judgment in order to answer the research questions and achieve the study's objectives (Smith, Colombi & Wirthlin, 2013). More importantly, most researchers' choice of purposive is predicated on the knowledge of the participants and their willingness to participate in the study (Sekaran & Bougie, 2009). Thus, for threat identification, purposive sampling was used to select participants for the in-depth interview. Similarly, for the framework evaluation, purposive sampling was used to select participants. Other reasons for adopting purposive sampling in this study are its accessibility, proximity, ease of use, cost effectiveness and time requirements.

4.8.3.1 Sample size

Sekaran and Bougie (2013, p. 241) describe a sample as "...a subset of a population that has been chosen to participate in a study". In other words, sample size refers to the total number of people that participate in a study. The researcher selected 380 employees, that is, 95 employees per bank, as the required sample size to participate in the quantitative

study for threat identification using questionnaires (Table 4.1). A sample size of 380 is within the range greater than 30 but less than 500 (Krejcie & Morgan, 1970). At the end of eight weeks of distribution and follow-up, a total of 369 questionnaires were returned. Nine had not been properly completed and were left out of the analysis. The remaining 360 questionnaires were usable as shown in Table 4.1 and this represents a 94.7 per cent response rate. This decision was supported by the Table of minimum sample sizes for different population sizes at a 95 per cent confidence level (Krejcie & Morgan, 1970).

Table 4.1: Banks administered questionnaires

S/N	Name of Banks	Distributed Questionnaires	Returned Questionnaires	Unreturned Questionnaires	Discarded Questionnaires	Usable Responses
1	Bank A	95	92	3	2	90
2	Bank B	95	90	5	3	87
3	Bank C	95	93	2	1	92
4	Bank D	95	94	1	3	91
	Total	380	369	11	9	360

The qualitative study for threat identification consists of twelve participants. This includes eight (8) ICT department personnel (two each from the four participating banks) and four (4) executive managers (one each from the four participating banks (Table 4.2)).

Again, the framework evaluation consists of twelve (12) participants which were drawn using purposive sampling as shown in Table 4.3. This includes executive management (two each from the four participating banks) and four (4) cyber security expert/researchers in academia across four different universities in different countries (except two which are from the same country). Participants were selected based on their knowledge and experience of the phenomenon under investigation (Sekaran & Bougie, 2009).

Table 4.2: List of ICT department personnel and executive managers for the interview (Threat identification)

Target Group	Participant's Designation	Code
Bank A	1. ICT Department Personnel	Participant 1
	2. ICT Department Personnel	Participant 2
	3. Executive Manager	Participant 3
Bank B	1. ICT Department Personnel	Participant 4
	2. ICT Department Personnel	Participant 5
	3. Executive Manager	Participant 6
Bank C	1. ICT Department Personnel	Participant 7
	2. ICT Department Personnel	Participant 8
	3. Executive Manager	Participant 9
Bank D	1. ICT Department Personnel	Participant 10
	2. ICT Department Personnel	Participant 11
	3. Executive Manager	Participant 12

Table 4.3: List of participants for closed and open-ended questions (Framework evaluation)

Target Group	Participant's Designation	Code
Bank A	1. ICT Department Personnel	Participant 2
	2. Executive Manager	Participant 3
Bank B	1. ICT Department Personnel	Participant 4
	2. Executive Manager	Participant 6
Bank C	1. ICT Department Personnel	Participant 7
	2. Executive Manager	Participant 9
Bank D	1. ICT Department Personnel	Participant 11
	2. Executive Manager	Participant 12
Academic Expert 1	1. Professor (Prof)	Participant 13
Academic Expert 2	2. Doctorate (PhD)	Participant 14
Academic Expert 3	3. Professor (Prof)	Participant 15
Academic Expert 4	4. Doctorate (PhD)	Participant 16

4.9 Research instrument

A research instrument refers to the tools utilized for data collection (Saunders et al., 2009). In a quantitative study, data is collected through questionnaires, which are mostly analysed using a statistical package (Creswell, 2013). On the other hand, in a qualitative study data is collected using observation, open-ended questions, and interviews which can be unstructured, semi-structured or structured, and are mostly analysed using thematic analysis (Anderson et al., 2012). For threat identification, a questionnaire was useful in collecting quantitative data from the employees of the four participating banks (Appendix B). The purpose was to gather as much information as possible about employees' practices and the various BYOD security threats experienced as they relate to the technical, social and mobility domains. A structured interview was useful in collecting qualitative data from the executive managers (Appendix C) and ICT department personnel (Appendix D) of the four participating banks. The purpose was to obtain in-depth information regarding organizations' practices, the various BYOD security threats experienced or reported as well as the mitigating strategies. The result of the study was analysed and interpreted using statistical and thematic analysis for the questionnaire and interview respectively. The reason for using the questionnaire and interview as the study research instruments was to achieve the study's objectives by utilizing mixed methods for data collection and analysis.

However, for framework evaluation an evaluation questionnaire made up of mostly closed-ended and open-ended questions was used. This was done in order to assess whether the developed security framework it meets the required criteria. Open-ended questions were included at the end of the closed-ended question section with the intention of gathering important data that may be missed if only closed-ended questions were used. This was administered to twelve (12) participants. These include eight (8) representatives of executive management (i.e. one executive manager and one ICT department personnel each) from the four participating banks and four (4) representatives of the academic staff (i.e. one each) from the four participating universities. The closed-ended questions and open-ended questions were analyzed using statistical and thematic analysis respectively.

4.9.1 Questionnaire design

For the purpose of data collection, there are three issues that were considered in the design of questionnaire. The issues considered were in line with Brace's (2018) suggestion for the design of questionnaires. The first issue was to consider each research objective and align this with the research question. The second issue was the wording of the questionnaire. All questions were clearly stated and to the point, and the use of professional language was avoided. Simple language was used to structure the questions for easy understanding by respondents. The last issue that was considered is the questionnaire coverage in respect of the population of the study; the questionnaire was designed to cut across all employees of the four participating banks in Lagos, Nigeria. This consideration was necessary to gather adequate information of the current security threats associated with the technical, social and mobility domains in a BYOD-enabled environment which includes the Nigerian banking sector.

Two sets of questionnaires were used in this study. The first questionnaire was a closed-ended questionnaire which was used for threat identification. It was administered to both the employees and executive management with the purpose of identifying the security threats associated with a BYOD-enabled environment and their influence on the Nigerian banking sector (Appendix B). The second questionnaire was a structured questionnaire containing both closed and open-ended questions which was used for the framework evaluation (Appendix E). This was administered to twelve respondents which included executive management (i.e. one executive manager and one ICT department personnel each) from four participating banks and four cyber security experts or researchers in academia across four different universities in different countries.

First questionnaire: Threat identification

The first questionnaire was used for threat identification and it involved collecting massive data (Appendix B). The research instrument that was used for threat identification was made up of six sections. Section 'A' was designed to collect respondents' demographic information such as gender, marital status, age group, department, educational qualifications, and employment status and work experience. This was useful in examining the impact of demographic issues on the key points of this study. Section 'B' was designed to collect information regarding the general practice of the bank as it relates to BYOD. The general practices include both individual (employees) and the

organization (executive management responsible for policy making) practices. Sections 'C' was designed to collect information regarding the security threats associated with software and hardware, which are the core component of an organization's BYOD (Ketel & Shumate, 2015). In addition, it collected data regarding the security threats emanating from the technical knowledge in the use of mobile device (Pratt Jr & Jones, 2013). Section 'D' was designed to collect information regarding security threats relating to employees' attitude and knowledge skills, and organizations' policies in the Nigerian banking sector. Section 'E' was designed to collect information regarding the security threats encountered when employees perform banking operations with their portable mobile devices while travelling. In addition, it also collected information relating to security threats experienced with methods used to prepare and dispose of mobile devices. Lastly, Section 'F' was designed to identify specific types of security threats that have been experienced. For all these sections (i.e. sections 'A' to 'F'), the researcher provided a list of options for respondents to select the appropriate option for their responses. These options were developed in such a way by the researcher that they gave the respondents the opportunity to choose the appropriate answers that suited their responses.

Second questionnaire: Framework evaluation

The second questionnaire which included both closed and open-ended questions was used for framework evaluation (Appendix E). The evaluation questionnaire was made up of six criteria for the evaluation. Criterion 'one' was designed to gather information regarding the 'appropriateness' of the developed framework which included the following; firstly, whether the developed framework aligned with the policies and strategies of the bank; secondly, whether the developed framework enhanced the effectiveness of the bank data security; and lastly, whether the developed framework could contribute towards the efficiency of the bank operation. Criterion 'two' was designed to gather information regarding the 'adequacy' of the developed framework which included whether the developed framework could address all the technical, social and mobility threats identified in the study. Adequacy helps to check the sufficiency of the security framework in addressing the security threats associated with these three domains. Criterion 'three' was designed to gather information regarding the 'feasibility' of the developed framework. It assessed whether the developed security framework was cost-effective, whether it could be implemented in a short period of time and whether it could be implemented with the available resources. Criterion 'four' was designed to

gather information regarding the ‘flexibility’ of the developed framework. It sought to determine whether the developed security framework could be easily adopted with changing policies and whether it can be adopted for mitigating security threats within or across different branches of the bank. Criterion ‘five’ was designed to gather information regarding ‘intention to use’ the developed framework. It assessed whether the bank was willing to use the framework as it is or with changes. It also sought to know whether the bank was willing to adopt the framework immediately or in the near future. Furthermore, it sought to know whether the use of the framework by the employees would be difficult or easy.

For all of these criteria (i.e. criterion ‘one’, ‘two’, ‘three’, ‘four’ and ‘five’ respectively), the researcher used a six-point Likert scale rating. The reason behind embracing the Likert scale rating is because of its flexibility in terms of constructing questions and interpreting results (Hartley, 2014). Similarly, the reason for the six-point Likert scale is because such a scale compels respondents to think deeply before selecting any of the points since there is no provision for undecided views (Chomeya, 2010, p. 399). Chomeya (2010, p.399) asserts that the six-point Likert scale is an appropriate scale for determining the true behaviour of the respondents. Hence, the respondents were allowed to show their agreement level with the statements in the questionnaire in accordance with the six-point Likert scale rating.

On the other hand, criterion ‘six’ of the questionnaire is an open-ended question which was designed to enable participants to further express their opinions in their chosen words. The aim therefore is to obtain more information regarding security threats and solutions that had not been considered in the developed framework.

4.9.2 Interview design

An interview refers to the way a researcher collects data from respondents via face-to-face interactions. According to Kumar (2011), it is at the discretion of the interviewer or researcher to determine the format and content of questions, including their wordings and the order in which they are asked. In addition, the interview process can range from being flexible where the researcher is not restricted to asking only specific predetermined questions (unstructured), to being inflexible where the interviewer is restricted to asking only specific predetermined questions (structured). This study used a semi-structured

interview which falls between the structured and unstructured interview and draws from the characteristics of the two extreme forms of interview. Cohen and Crabtree (2006) state that a semi-structured interview has a paper-based interview guide which the interviewer follows just as in the case of a structured interview, but that discussions can diverge at any point in time as in the case of an unstructured interview. The interviews were directed towards the ICT department personnel (Appendix C) and the executive manager (Appendix D) and were designed based on three domains, namely technical, social and mobility. These three domains explore organizational practices in identifying BYOD security threats in the Nigerian banking sector. However, prior to each interview session, the participants were initially contacted by the researcher and they were all given a covering letter. The covering letter included the researcher's background, research topic, objectives of the study, an informed consent form, as well as the interview questions for the participants to study. This covering letter also guaranteed the anonymity and confidentiality of records that could identify the participants taking part in the study. All the participants voluntarily gave their consent to take part in the study by signing the consent form.

4.9.3 Data collection procedure

Data collection procedure is the process involved in collecting or gathering data for the purpose of providing solutions to the research questions, hypotheses and problem statement (Creswell, 2013; Saunders et al., 2011). The researcher strictly followed the data collection procedures in line with the research objectives. Both primary and secondary sources were used in the study. Questionnaires and interviews were used as the primary source of data collection while scholarly literature reviews served as a secondary source of data collection.

Primary sources of data collection

The first questionnaire (threat identification) was personally administered with the assistance of the executive managers. Three hundred and eighty (380) copies of the questionnaire were distributed to the four selected banks (i.e. 95 copies were evenly assigned to each bank). The choice of personally administered questionnaires ensured that respondents were given the opportunity to ask questions on the spot and the ability to collect questionnaires immediately after completion (Sekaran & Bougie, 2009). Furthermore, it promoted a high response rate because the researcher could easily follow

up on data collection. At the end of eight (8) weeks of distribution and follow-up, a sample of 369 completed responses was received. However, nine (9) of the returned questionnaires were discarded because multiple answers were given to some questions that required just one answer while some questions had not been answered. The major challenge of utilizing a personally administered approach was the travelling expenses involved in field work (Sekaran & Bougie, 2009; Wilson, 2014). This explains why a mixed method was adopted for the collection of quantitative and qualitative data at a single point in time. However, the second questionnaire (framework evaluation) was sent online to the e-mail addresses of twelve (12) participants using a purposive sampling technique. Two weeks later, responses were received. In addition, the interview conducted for threat identification was also a primary source of data. The researcher personally interviewed 12 executive management staff in their offices (two ICT department personnel and one executive manager each) from the four participating banks.

Secondary sources of data collection

Literature reviews and the theoretical framework underpinning the study were the secondary sources of data used by the researcher in order to fulfil the study objectives. Sources of secondary data employed included published and unpublished PhD theses, online journal articles, textbooks, and conference papers. These were instrumental in identifying BYOD security threats and also in investigating the existing security measures. The data gathered from the secondary sources provided justification for data triangulation by comparing data collected from secondary and primary sources; this reduced the level of bias that might have consciously or unconsciously occurred in this study.

4.10 Data quality control

Reliability and validity are important issues that must be considered by every researcher. Research may be questioned or, even worse, rejected as null and void if the validity and reliability of the findings are not assured.

4.10.1 Reliability

Reliability refers to the level at which a measurement can yield a consistent and stable outcome. (Carmines & Zellers in Wilson, 2014). McBurney and White (2009, p. 129)

have also defined reliability as the capability of a measuring instrument to produce the same outcome under the same situation over time. The aim of reliability is to reduce biases and error in a study. Reaves (1992) listed types of reliability tests which include internal consistency reliability which measures the extent to which items on the entire scales measure the same attribute; inter-rater reliability which measures the similarity between two individuals' verdicts on the same issue under study; test-retest reliability measuring the level to which a single instrument yields the same outcome in two different situations; and equivalent forms reliability measures the extent to which two different versions of the same research instrument produce similar results (Carmines & Zellers in Wilson, 2014).

However, because the research instrument used in this study was developed from scratch and because it is not an instrument that measures scales (such as optimism, for example), the usual tests are not appropriate. Hence, two different approaches were used. The first was to request a professional statistician to check for ambiguities and biases (Appendix G). Secondly, the research instruments were subjected to a pilot test to elicit dependable responses from a selected sample. A total of 38 participants were selected for the pilot test which represented ten per cent of the sample size. This was to check for clarity and to test whether the participants understood what was expected of them and guaranteed that the kind of data the study was seeking to collect was appropriate for the research question. The feedback obtained from the pilot test presented ideas, clarifications and correction that were used to improve the questionnaires.

4.10.2 Validity

Validity refers to the degree to which the measurement procedure actually measures the concept that it is intended to measure (Denzin & Lincoln, 2011). The relationship between constructs and its indicators is encompassed by validity. Different types of validity include face validity, content validity, construct validity, discriminant validity and convergent validity.

In this study, the researcher made use of content and construct validity. In content validity, experts' opinions and knowledgeable professionals in the field of study were sought to evaluate the research instrument, while the construct validity aligned the research instrument with the research constructs and objectives. In addition, most

constructs used in designing the research instruments were adapted from previous studies which were based on sound and tested theoretical frameworks (e.g. socio-technical model, and mobility model). This guaranteed the validity of the constructs. Lastly, the results of this study were compared with other similar studies to ensure the external validity of the instrument.

4.11 Ethical consideration

The ethical guidelines of the University of KwaZulu-Natal were followed to ensure credibility and authenticity of the study. The researcher completed the university's ethical clearance application form and also attached a copy of the research instrument and gatekeepers' letters from the participating banks. An ethical approval letter was issued to the researcher by the Humanities and Social Science Research Committee of the University of KwaZulu-Natal granting the researcher permission to conduct the study (Appendix A). The rights of all the participants in this research were considered by adhering to the ethical requirement highlighted as follows:

- i. Permission or approval (gatekeepers' letters) were officially obtained from the participating banks.
- ii. The researcher ensured that every participant in the study filled an informed consent form to validate their willingness to be involved.
- iii. It was clearly stated in the consent form that participation in the study was voluntary and that participants could withdraw at any stage.
- iv. Similarly, pseudo-names were used to conceal the identities of the participating banks as well as participating universities based on the request for anonymity.
- v. The researcher personally administered the research instrument to the respondents and abuse of collected data was avoided.
- vi. Data collected from secondary sources for this study were properly cited and referenced to avoid plagiarism.
- vii. Ethical clearance was secured from the University permitting the researcher to continue with the study.
- viii. All the data collected will be handed to the School of Management, Information Technology and Governance at the University of KwaZulu-Natal for safekeeping

4.12 Limitations of the research methodology

There were some limitations encountered in the research methodology despite the fact that the researcher carefully planned and executed the research methodology adopted in the study. Non-probability sampling techniques could not be used to sample respondents throughout the entire study in view of the size of the population. For example, while the purposive sampling technique was used in selecting participants for the executive management group, the technique could not be applied to the entire group of respondents. In this case, the researcher was left with no choice but to apply a probability sampling technique in selecting the entire group of respondents, specifically simple random sampling techniques. Furthermore, only the executive management group that was used for threat identification was also used for framework evaluation. In addition, the research instrument used in this study was limited to the four participating banks in Lagos State, Nigeria that gave their consent.

4.13 Summary

This chapter explained the different levels/layers of the ‘research onion’ showcasing fields of application, before adopting the most suitable ‘research onion’ for this study.

Figure 4.2 exhibits the summary of the research methodologies identified for this study. This includes research philosophy, research approach, research choices, research strategy, research design and research time horizon.

This chapter also justified the basis for the selection of a pragmatic philosophical stand for the study, as well as the mixed-method research approach. The threat identification followed the explanatory sequential mixed-methods research approach that enables data to be analysed separately but integrated at the interpretation stage, thereby enabling data triangulation in the course of the investigation (Hanson et al., 2005) while the framework evaluation of the study followed the concurrent mixed-methods research design (Creswell, 2013). This approach enables data to be analysed simultaneously and interpreted at the same time, thus enabling cross-validation of data.

In addition, a survey research strategy was used for the quantitative approach to explore the interplay between individual practices and the security threats experienced as they

relate to the technical, social and mobility domains of the BYOD phenomenon while a grounded theory research strategy was used for the qualitative approach in order to generate the themes to support and compare the quantitative study (Creswell, 2013; Leedy & Ormrod, 2014). Furthermore, the chapter also set out the research design, sampling technique, research methodology and the research instruments that were used to investigate individual practices and the security threats experienced as they relate to the technical, social and mobility domains of BYOD. Similarly, the ethical codes of conducts in the research were observed and clearly stated while the limitations of the research methodology were explained.

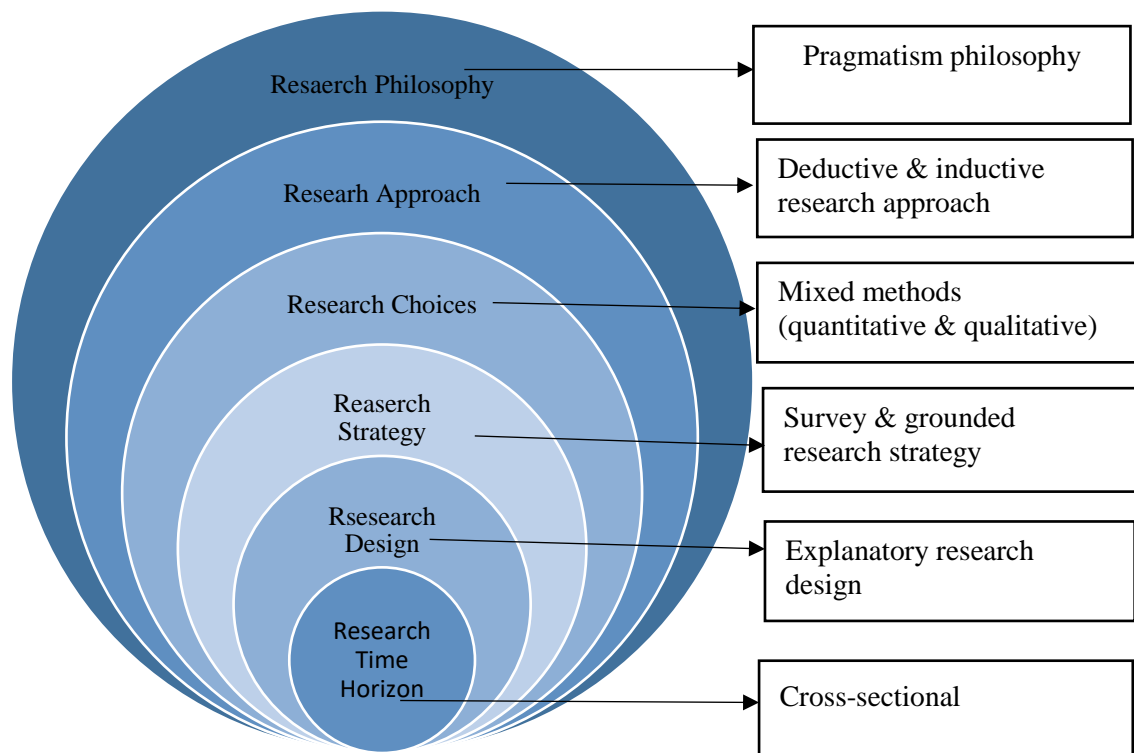


Figure 4.2: Research 'onion' adopted for the study

CHAPTER 5: DATA ANALYSIS AND INTERPRETATION OF RESULTS

5.1 Introduction

Johnson (2013) describes data analysis as the process of examining, cleansing and transforming collected data in order to reach a conclusion for a given problem. Irrespective of whether the data is quantitative or qualitative, the purpose of data analysis is to obtain useful and usable information. The benefits of data analysis as outlined by Johnson (2013) are as follows: firstly, data analysis helps to filter and extract meaningful information from a data set. Secondly, data analysis helps to structure the findings from various sources of data. Thirdly, data analysis provides a clarification of several concepts, frameworks, theories and methods used; and lastly, data analysis helps to minimize human bias with the help of proper statistical instruments when making a conclusion. In this study, data analysis enabled the researcher to structure the findings from collected data and extract meaningful information which helped in arriving at a conclusion. Thus, this chapter presents the data analysis and interpretation of results for the threats identification (quantitative and qualitative data).

However, it is important to note that all the data gathered (quantitative and qualitative) for the threat identification were used to answer the first, second and third research questions (section 1.4), as they relate to identifying BYOD security threats. The quantitative data (questionnaires) were analyzed using the Statistical Package for the Social Sciences (SPSS) version 21 while, the qualitative data (interviews) were analyzed using thematic analysis.

5.2 The response rate

A total of 380 copies of questionnaire were distributed to the four participating banks in Lagos State, Nigeria. Ninety-five (95) questionnaires were distributed to each of the banks as shown in Table 4.1. The questionnaires were personally administered to ensure that respondents were given the opportunity to ask questions on the spot and owing to the ability to collect questionnaires immediately after completion. This promoted a high response rate because the researcher could easily follow up on data collection. At the end of eight weeks of distribution and follow-up, only 369 responses had been returned out

of the 380 questionnaires distributed. However, out of the 369 returned questionnaires, nine were discarded because multiple answers had been given to some questions that required just one answer while some questions had not been answered. Hence the sample of 360 responses was usable as shown in Table 4.1. This represents a 94.7 per cent confidence level.

5.3 Overview of data analytical techniques

This section discusses the various tests used for the data analysis for the threats' identification. For quantitative data, the tests include descriptive and inferential analysis which includes the chi-square goodness of fit, chi-square test of independence and binomial test. It is important to note that the reason for choosing chi-square goodness of fit is because it has been proven to measure how well the observed distribution of data fits with the expected value (Lani, 2011). Similarly, McHugh, (2013) asserts that chi square test of independence is best used to determine the significant relationship between two categorical variable while the binomial test is best used to compute the number of 'successes' when the process is repeated a specific number of times, each asking a yes or no question with a given outcome which is either success or a failure. However, for the qualitative data, coding was used to develop themes within the raw data by identifying important patterns in the data and encoding these prior to interpretation. The various tests used for the data analysis for the threats' identification (quantitative and qualitative) are further discussed in detail as follows;

Wilson (2010, p.213) defines descriptive analysis as the summary or overview of demographic data achieved through the use of pie charts, bar graphs, histograms and frequency distribution tables which spell out some occurrence and percentage differences. Descriptive statistics are used to summarize or describe the crunch of numbers with few indices (Sekaran & Bougie, 2011). It is important to begin data analysis with descriptive statistics in order to give the reader an overview of the collected data before presenting the detailed analysis (Wilson, 2010). This suggests the reason why most researchers and students start the data analysis chapter of their theses, dissertations or projects with descriptive statistics. In addition, Treiman (2014) recommends the use of descriptive statistics to represent the background distribution characteristics of the study participants. Hence, this study also considered it essential to present the analysis of the demographic

data collected in Section 'A' of the questionnaire at the beginning of the analysis (Table 5.1). The demographic data includes participants' gender, marital status, age group, educational qualifications, department, employment status and work experience.

The chi-square goodness of fit test is a non-parametric test that is used to compare the observed value of a given phenomenon with the expected value (Lani, 2011). It is used to find out how the observed sample distribution is significantly different from the expected probability distribution (Pfeifer, 2008). In this study, the chi-square goodness of fit test was used on a categorical variable (i.e. the type of mobile devices and the purpose for usage) to test whether any of the response options are selected significantly more or less often than the others in Section 'B' of the questionnaire. The variables in this case are the types of mobile devices and the purpose for usage. Under the null hypothesis, it is assumed that all responses are equally selected.

The chi-square test of independence is mostly used to determine whether there is a significant relationship between two categorical (nominal) variables (McHugh, 2013). In this study, the chi-square test of independence was used on cross-tabulations to determine whether a significant relationship exists between the two variables (i.e. individual practices and the security threats) represented in the cross-tabulation in sections 'C', 'D' and 'E' of the questionnaire. It compares frequencies of cases that occur in the two categorical variables. When conditions are not met, Fisher's exact test is used.

The binomial test uses the binomial distribution to test the statistical significance of deviations from a theoretically expected distribution of observations into two categories (Norusis, 2006). In this study, a binomial test was used to test whether a significant proportion of respondents selected one of a possible two responses in Section 'F' of the questionnaire. This can be extended when data with more than two response options is split into two distinct groups.

Coding is mostly used in thematic analysis to create meaningful patterns or themes in order to determine the relationship between variables and to compare different sets of evidence that pertain to different situations in the study (Vaismoradi, Turunen & Bondas, 2013). Coding can be done manually or with a software program. This study found manual coding appropriate for the qualitative data because it provides flexibility for

approaching research patterns in two ways, i.e. inductive and deductive (Guest, MacQueen & Namey, 2011). In an inductive approach, themes are identified and are strongly linked to the data collected. In addition, an inductive approach uses research questions to narrow the scope of the study, while a deductive approach is mostly based on theory and usually begins with hypothesis (Corbin & Strauss, 2014). This study adopted the inductive approach because the data collected for this research was specifically through an interview and the themes identified are related to the data collected. The interview was conducted in English and transcribed into text. In addition, the transcribed text was stored as a separate Word document prior to analysis. This was to ensure that the data was properly organized and to enable the researcher to become more familiar with the data. The actual names of participants were not revealed based on their request to remain anonymous. Hence, coded names such as participant 1, 2, 3 and the like were assigned to participants (Table 4.2).

5.4 Data analysis: Quantitative data

This section presents the quantitative data analysis for the threat identification. The questionnaire is divided into six (6) sections. Section 'A' deals with demographic information; Section 'B' deals with information regarding the general practice of the bank as it relates to BYOD; and Section 'C', which is regarded as the technical domain, collects information regarding the security threats associated with software and hardware, which are the core components of an organization's BYOD (Ketel & Shumate, 2015). Section 'D', which is regarded as the social domain, collects information regarding security threats relating to employees' attitudes, knowledge, skills and the organizations' policies in the Nigerian banking sector. Section 'E', which is regarded as the mobility domain, collects information regarding the security threats encountered when employees perform banking operations with their portable mobile devices while travelling. In addition, it also collects information relating to methods used to prepare and dispose of mobile devices and the security threats experienced. Finally, Section 'F' collects data that identifies specific types of security threats experienced.

5.4.1 Demographic data

This section presents the demographic information of participants. This includes participants' gender, marital status, age group, department, educational qualification,

employment status and work experience. As presented in Table 5.1, the majority of the respondents were male 192 (53.3 per cent). In other words, there were more males than females 168 (46.7 per cent) who participated in the study, which reflects the representativeness of the randomly sampled respondents. In addition, the majority of the respondents were within the age group of 26-30 and 31-35; this constitutes 119 and 106 participants respectively, which represents 62.5 per cent of the total respondents. Likewise, Table 5.1 shows that most of the respondents, namely 158 (43.9 per cent) work in the marketing department. Furthermore, the majority (216 or 60 per cent) of the respondents' highest qualifications were a higher national diploma or a bachelor's degree.

This implies that the banking sector relies on human skills and technological innovations to achieve its objectives. The educational achievements of the employees in this sector explain the reason why most of the questionnaires that were returned were properly completed, with only nine exceptions.

Table 5.1: Demographic data

	Background Characteristics	Frequency	Percentage
Gender	Male	192	53.3
	Female	168	46.7
Marital Status	Single	143	39.7
	Married	215	59.7
	Divorced/Separated	2	0.6
Age Group	<21	10	2.8
	21-25	52	14.4
	26-30	119	33.1
	31-35	106	29.4
	36-40	64	17.8
	>40	9	2.5
Department	Operations	90	25
	Marketing	158	43.9
	Human Resource	28	7.8
	Customer Service	50	13.9

Table 5.1: Demographic data (Contd...)

	ICT	20	5.6
	Executive Manager	4	1.1
	Others	10	2.8
Educational Qualification	Senior Certificate	2	0.6
	National Diploma	82	22.8
	HND/Degree	216	60
	Masters	60	16.7
Employment Status	Contract/Temporal	102	28.3
	Probation	42	11.7
	Permanent	190	52.8
	Outsourced	22	6.1
	Others	4	1.1
Work Experience	Up to 5years	166	46.1
	6-10years	108	30
	11-15years	59	16.4
	16-20years	20	5.6

5.4.2 General practices

This section focuses on the general practices of banks' employees in relation to using mobile devices. A descriptive analysis was applied on item 1 in the questionnaire (Appendix B).

5.4.2.1 Type of device and purpose of usage

The distribution of respondents based on the type of mobile device and purpose of usage is represented in a bar graph in Figure 5.1. A total of 66.7 per cent of the respondents use a smartphone for work and personal usage while a total of 40.3 per cent of the respondents use a laptop for work and personal usage. Tablets and 'other' devices are used by an insignificant percentage of respondents i.e. 21.1 per cent and 8.1 per cent respectively. The 'other' option gives the respondents ample opportunity to specify other types of mobile devices used that may have been omitted.

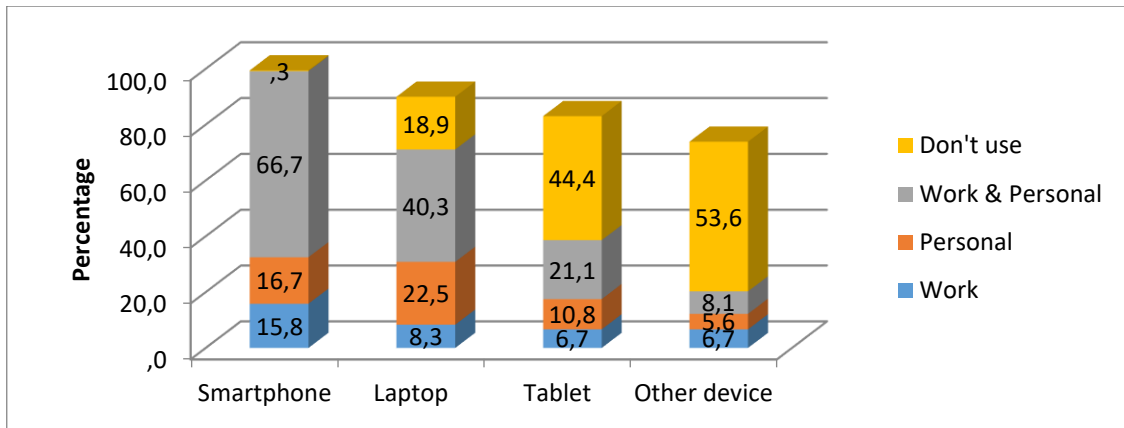


Figure 5.1: Bar graph distribution of type of mobile device and purpose of usage

For each of the devices, a chi-square goodness of fit test was used to test whether any of the uses (response options) are selected significantly more than the others. A significant number of participants, namely 240 representing 66.7 per cent of the respondents indicated that they use a smartphone for work and personal use ($\chi^2(3) = 362.112$, $p < 0.0005$), while 145 participants representing 40.3 per cent use a laptop for work and personal usage ($\chi^2(3) = 84.765$, $p < 0.0005$). Tablets and ‘other’ devices are not used at all by a significant number of respondents ($p < 0.0005$, in each case).

Table 5.2: Chi-square goodness of fit test for device usage

	1.1 Smartphone Purpose	1.2 Laptop Purpose	1.3 Tablet Purpose	1.4 Other devices Purpose
Chi-Square	362.112 ^a	84.765 ^b	148.799 ^c	321.459 ^d
df	3	3	3	3
Asymp. Sig.	.000	.000	.000	.000

This section has clearly revealed the general practice of employees in terms of using mobile devices. This includes the type of device and the purpose for which the device is used. These questions help to clearly understand what to include in the security framework. The following section will investigate the technical practices of the employees and security threats experienced.

5.4.3 Technical practices

A bivariate analysis was carried out to determine whether there is a significant relationship between the technical practices on these items 7, 11, 12 and 15 in the

questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). These specific items were chosen because the practices directly relate to some of the threats on item 28. For all these analyses a chi-square test of independence was used to test for a significant relationship between the practice and the security threats, and where the conditions for this test are not met, Fisher's exact test was used.

5.4.3.1 Managing credentials with security software on the device

A bivariate analysis was performed in Table 5.3 to show the relationship between the row (I allow security software on my device to manage credentials on smartphone) and column (data leakage) variables. The relationship is such that allowing security software to manage credentials on smartphone (item 7.2) is related to encountering data leakage (item 28.8) and not allowing security software to manage credentials on smartphone (item 7.2) is associated with not encountering data leakage (28.8). If there were no relationships between the row and column variables (items 7.2 and 28.8), then the number of respondents who fell in each of the four (4) cells would be the 'expected count'. The illustration in Table 5.3 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 31 is greater than the expected count of 25.4) and the NO/NO block (i.e. 37 is greater than the expected count of 31.4). Similarly, fewer than expected fell in the YES/NO (i.e. 18 is less than the expected count of 23.6) and the NO/YES (i.e. 28 is less than the expected count of 33.6) blocks. Thus, there is a relationship between the two variables.

Table 5.3: Cross-tab of respondents managing credential with smartphone and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)		Total
			Yes	No	
7.2 Smartphone I allow security software on my device to manage the credentials	Yes	Count	31	18	49
		Expected Count	25.4	23.6	49.0
		% within 7.2S I allow security software on my device to manage the credentials	63.3%	36.7%	100.0%
		Std. Residual	1.1	-1.2	
	No	Count	28	37	65
		Expected Count	33.6	31.4	65.0
		% within 7.2S I allow security software on my device to manage the credentials	43.1%	56.9%	100.0%
		Std. Residual	-1.0	1.0	
Total	Count	59	55	114	
	Expected Count	59.0	55.0	114.0	
	% within 7.2S I allow security software on my device to manage the credentials	51.8%	48.2%	100.0%	
	Std. Residual				

For each of the variables, a chi-square test of independence was used to test whether any of variables are selected significantly more than the others. Table 5.4 shows that there is a significant relationship between allowing security software on a smartphone to manage credentials and data leakage, $\chi^2(1) = 4.560$, $p=0.033$. This means that significantly more than expected respondents that allow security software on a smartphone to manage credentials experience data leakage.

Table 5.4: Chi-square test of independence for respondents managing credentials with smartphone and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4.560 ^a	1	.033		
Continuity Correction ^b	3.788	1	.052		
Likelihood Ratio	4.600	1	.032		
Fisher's Exact Test				.039	.026
Linear-by-Linear Association	4.520	1	.033		
N of Valid Cases	114				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 23.64.

b. Computed only for a 2x2 table

5.4.3.2 Updating mobile devices on public network

A bivariate analysis was performed in Table 5.5 to show the relationship between the row (updating mobile device from public network) and column (unauthorized modification of confidential information) variables. The relationship is such that always updating mobile devices from public networks (item 11.3) is related to encountering a security threat (item 28.1) and not always updating from public network (item 11.3) is associated with not encountering the risk (item 28.1). The illustration in Table 5.5 shows that more than the expected number of respondents fell into the ALWAYS/YES block (i.e. 11 is greater than the expected count of 3.2) and SOMETIMES/NO block (i.e. 127 is greater than the expected count of 120.1). Similarly, fewer than expected fell in the ALWAYS/NO (i.e. 8 is less than the expected count of 15.8) and SOMETIMES/YES (i.e. 17 is less than the expected count of 23.9) blocks. Thus, there is a relationship between the two variables.

Table 5.5: Cross-tab of respondents updating mobile device on public network and unauthorized modification of confidential information

			28.1 Unauthorized modification of confidential information (e.g. customer's bank statement)		Total
			Yes	No	
11.3 Updating mobile device from public network (e.g. restaurant, airport)	Always	Count	11	8	19
		Expected Count	3.2	15.8	19.0
		% within 11.3 Public network (e.g. restaurant, airport)	57.9%	42.1%	100.0%
		Std. Residual	4.4	-2.0	
	Sometimes	Count	17	127	144
		Expected Count	23.9	120.1	144.0
		% within 11.3 Public network (e.g. restaurant, airport)	11.8%	88.2%	100.0%
		Std. Residual	-1.4	.6	
	Never	Count	6	36	42
		Expected Count	7.0	35.0	42.0
		% within 11.3 Public network (e.g. restaurant, airport)	14.3%	85.7%	100.0%
		Std. Residual	-.4	.2	
Total	Count	34	171	205	
	Expected Count	34.0	171.0	205.0	
	% within 11.3 Public network (e.g. restaurant, airport)	16.6%	83.4%	100.0%	
	Std. Residual				

For each of the variables, a chi-square test of independence was used to test for a significant relationship between updating mobile devices on public network and

unauthorized modification of confidential information. Significantly more than expected of those employees who update mobile devices on public networks experience unauthorized modification of confidential information ($\chi^2(2) = 25.975, p < 0.0005$). This is presented in Table 5.6.

Table 5.6: A chi-square test of independence for updating mobile devices on public networks and unauthorized modification of confidential information

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability
Pearson Chi-Square	25.975 ^a	2	.000	.000		
Likelihood Ratio	19.325	2	.000	.000		
Fisher's Exact Test	19.546			.000		
Linear-by-Linear Association	9.567 ^b	1	.002	.003	.001	.001
N of Valid Cases	205					

a. 1 cells (16.7%) have expected count less than 5. The minimum expected count is 3.15.

b. The standardized statistic is 3.093.

5.4.3.3 Saving work document from laptop to a free cloud storage

A bivariate analysis was performed in Table 5.7 to show the relationship between the row (saving work document from laptop to a free cloud storage) and column (data leakage). The relationship reveals that saving work documents from a laptop to a free cloud storage (item 12.4) is related to encountering data leakage (item 28.8) and not saving work documents from a laptop to a free cloud storage (item 12.4) is associated with not encountering the risk (item 28.8). The illustration in Table 5.7 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 88 is greater than the expected count of 63.6) and the NO/NO block (i.e. 69 is greater than the expected count of 44.6). Similarly, fewer than expected fell in the YES/NO (i.e. 34 is less than the expected count of 58.4) and NO/YES (i.e. 24 is less than the expected count of 48.4) blocks. Thus, there is a relationship between the two variables.

Table 5.7: Cross-tab of respondents saving work document from laptop to a free cloud storage and Data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)	
			Yes	No
12.4Laptop Saving work document from a laptop to a free cloud storage (eg dropbox)	Yes	Count	88	34
		Expected Count	63.6	58.4
		% within 12.4L A free cloud storage (eg dropbox)	72.1%	27.9%
		Std. Residual	3.1	-3.2
	No	Count	24	69
		Expected Count	48.4	44.6
		% within 12.4L A free cloud storage (eg dropbox)	25.8%	74.2%
		Std. Residual	-3.5	3.7
Total	Count	112	103	
	Expected Count	112.0	103.0	
	% within 12.4L A free cloud storage (eg dropbox)	52.1%	47.9%	

For each of the variable, a chi-square test of independence was used to test for a significant relationship between saving work document to a free cloud storage and data leakage. Significantly more than expected of those employees who save work document to a free cloud storage experience data leakage, ($\chi^2(1)=45.379$, $p<0.0005$). This illustrated in Table 5.8.

Table 5.8: A chi-square test of independence for respondents saving work document from laptop to a free cloud storage and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	45.379 ^a	1	.000	.000	.000
Continuity Correction ^b	43.541	1	.000		
Likelihood Ratio	47.089	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	45.168 ^c	1	.000	.000	.000
N of Valid Cases	215				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 44.55.

b. Computed only for a 2x2 table

5.4.3.4 Adherence to security measures

Participants were asked to indicate whether they use security measures for their mobile devices. These include password authentication, antiviruses, firewalls and hardware

tokens. A bivariate analysis was carried out to determine whether there is a significant relationship between using security measures on item 15 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). Thereafter, a chi-square test of independence was used to test for a significant relationship between types of security measures used and the security threats experienced. However, the results presented in Tables 5.9 to 5.16 show that most of the security measures are not used and this has resulted in some security threats.

Password authentication

A bivariate analysis was performed in Table 5.9 to show the relationship between the row (password authentication) and column (unauthorized access to social interactive network) variables. The relationship is such that NOT using password authentication (item 15.1) is related to encountering unauthorized access to social interactive networks (item 28.3) and using password authentication (item 15.1) is associated with not encountering the risk (item 28.3). The illustration in Table 5.9 shows that more than the expected number of respondents fell in the NO/YES block (i.e. 13 is greater than the expected count of 8.3) and the YES/NO block (i.e. 217 is greater than the expected count of 212.3). Similarly, fewer than expected fell in the YES/YES (i.e. 66 is less than the expected count of 70.8) and the NO/NO (i.e. 20 is less than the expected count of 24.8) blocks. Thus, there is a relationship between the two variables.

Table 5.9: Crosstab of respondents not using password authentication and unauthorized access to social interactive network

			28.3 Unauthorized access to your social interactive network (e.g. Facebook, WhatsApp, BBM, WeChat)	
			Yes	No
15.1 Not using password authentication	Yes	Count	66	217
		Expected Count	70.8	212.3
		% within 15.1 Password authentication	23.3%	76.7%
		Std. Residual	-.6	.3
	No	Count	13	20
		Expected Count	8.3	24.8
		% within 15.1 Password authentication	39.4%	60.6%
		Std. Residual	1.7	-1.0
Total	Count	79	237	
	Expected Count	79.0	237.0	
	% within 15.1 Password authentication	25.0%	75.0%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between not using password authentication and encountering unauthorized access to social interactive network. There is a significant relationship between not using password authentication and unauthorized access to social interactive network, ($\chi^2(1)=4.072$, $p=0.044$). Significantly more than expected respondents who do not use password authentication experience unauthorized access to social interactive networks. This is illustrated in Table 5.10.

Table 5.10: A chi-square test of independence for not using password authentication and unauthorized access to social interactive network

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4.072 ^a	1	.044	.055	.039
Continuity Correction ^b	3.260	1	.071		
Likelihood Ratio	3.731	1	.053	.089	.039
Fisher's Exact Test				.055	.039
Linear-by-Linear Association	4.059 ^c	1	.044	.055	.039
N of Valid Cases	316				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 8.25.

b. Computed only for a 2x2 table

Anti-virus

A cross-tabulation was used in Table 5.11 to show the relationship between the row (not using anti-virus) and column (software making copies of itself) variables. The relationship is such that NOT using anti-virus on mobile devices (item 15.3) is related to software making copies of itself on the device (item 28.11) and using anti-virus (item 15.3) is associated with not encountering the risk (item 28.11). The illustration in Table 5.11 shows that more than the expected number of respondents fell in the NO/YES block (i.e. 40 is greater than the expected count of 27.1) and the YES/NO block (i.e. 142 is greater than the expected count 129.1). Similarly, fewer than expected fell in the YES/YES (i.e. 82 is less than the expected count 94.9) and NO/NO (i.e. 24 is less than the expected count 36.9) blocks. Thus, there is a relationship between the two variables.

Table 5.11: Cross-tab of respondents for not using anti-virus and software keeps making copies of itself on the device

			28.11 Software keeps making copies of itself on your device		Total
			Yes	No	
15.3 Not using anti-virus	Yes	Count	82	142	224
		Expected Count	94.9	129.1	224.0
		% within 15.3 Anti-virus	36.6%	63.4%	100.0%
		Std. Residual	-1.3	1.1	
	No	Count	40	24	64
		Expected Count	27.1	36.9	64.0
		% within 15.3 Anti-virus	62.5%	37.5%	100.0%
		Std. Residual	2.5	-2.1	
Total	Count	122	166	288	
	Expected Count	122.0	166.0	288.0	
	% within 15.3 Anti-virus	42.4%	57.6%	100.0%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between not using anti-virus on mobile devices and software continually making copies of itself on the device. Table 5.12 shows that there is a significant relationship between not using anti-virus on mobile device and software continually making copies of itself on the device, ($\chi^2(1) = 13.668, p = 0.000$). Significantly more than expected respondents who do not use anti-virus on their mobile devices experience this security threat (i.e. Software keeps making copies of itself on one's device).

Table 5.12: A chi-square test of independence for not using anti-virus and software keeps making copies of itself on your/one's device

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	13.668 ^a	1	.000	.000	.000
Continuity Correction ^b	12.628	1	.000		
Likelihood Ratio	13.563	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	13.621 ^c	1	.000	.000	.000
N of Valid Cases	288				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 27.11.

b. Computed only for a 2x2 table

Firewall

A bivariate analysis was performed in Table 5.13 to show the relationship between the row (not using firewall) and column (unauthorized access to social interactive network) variables. The relationship is such that NOT using a firewall on a mobile device (item 15.5) is related to software making copies of itself on the device (item 28.3) and using a firewall (item 15.5) is associated with not encountering the risk (item 28.3). The illustration in Table 5.13 shows that more than the expected number of respondents fell in NO/YES block (i.e. 36 is greater than the expected count of 24.2) and the YES/NO block (i.e. 104 is greater than the expected count of 92.2). Similarly, fewer than expected fell in the YES/YES (i.e. 21 is less than the expected count of 32.8) and NO/NO (i.e. 56 is less than the expected count of 67.8) blocks. Thus, there is a relationship between the two variables.

Table 5.13: Cross-tab of respondents for firewall and unauthorized access to social interactive network

			28.3 Unauthorized access to your social interactive network (e.g. Facebook, WhatsApp, BBM, WeChat)		
			Yes	No	Total
15.5 Not using Firewall	Yes	Count	21	104	125
		Expected Count	32.8	92.2	125.0
		% within 15.5 Firewall	16.8%	83.2%	100.0%
		Std. Residual	-2.1	1.2	
	No	Count	36	56	92
		Expected Count	24.2	67.8	92.0
		% within 15.5 Firewall	39.1%	60.9%	100.0%
		Std. Residual	2.4	-1.4	
Total	Count	57	160	217	
	Expected Count	57.0	160.0	217.0	
	% within 15.5 Firewall	26.3%	73.7%	100.0%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between not using a firewall on mobile devices and unauthorized access to one's social interactive network. Significantly more than expected respondents who do not use a firewall experience unauthorized access to their social interactive network ($\chi^2(1)=13.644$, $p<0.0005$). This is represented in Table 5.14.

Table 5.14: A chi-square test of independence for not using firewall and unauthorized access to social interactive network

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	13.644 ^a	1	.000	.000	.000
Continuity Correction ^b	12.516	1	.000		
Likelihood Ratio	13.580	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	13.582 ^c	1	.000	.000	.000
N of Valid Cases	217				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 24.17.

b. Computed only for a 2x2 table

Hardware token

A bivariate analysis was performed in Table 5.15 to show there is a relationship between the row (not using hardware token) and column (you saw a number in your dialling list that you haven't dialled) variables. The relationship is such that NOT using a hardware token on a mobile device (item 15.8) is related to having an unknown number in the dialling list (item 28.12) and using a hardware token (item 15.8) is associated with not encountering the risk (item 28.12). The illustration in Table 5.15 shows that more than the expected number of respondents fell in the NO/YES block (i.e. 18 is greater than the expected count of 11.5) and the YES/NO block (i.e. 172 is greater than the expected count of 165.5). Similarly, fewer than expected fell in the YES/YES (i.e. 17 is less than the expected count of 23.5) and NO/NO (i.e.75 is less than the expected count 81.5) blocks. Thus, there is a relationship between the two variables.

Table 5.15: Cross-tab of respondents for hardware token and unknown number in the dialling list

			28.12 You saw a number in your dialling list that you haven't dialled	
			Yes	No
15.8 Not using Hardware token	Yes	Count	17	172
		Expected Count	23.5	165.5
		% within 15.8 Hardware token	9.0%	91.0%
		Std. Residual	-1.3	.5
	No	Count	18	75
		Expected Count	11.5	81.5
		% within 15.8 Hardware token	19.4%	80.6%
		Std. Residual	1.9	-.7
Total	Count	35	247	
	Expected Count	35.0	247.0	
	% within 15.8 Hardware token	12.4%	87.6%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between not using a hardware token and an unknown number in the dialling list. A significant relationship exists between not using a hardware token and an unknown number in the dialling list ($\chi^2(1)=6.154, p=0.013$). Significantly more than expected respondents who do not use a hardware token experience this security threat (i.e. unknown number in the dialling list). This is represented in Table 5.16.

Table 5.16: A chi-square test of independence for not using hardware token and unknown number in the dialling list

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	6.154 ^a	1	.013	.020	.013
Continuity Correction ^b	5.238	1	.022		
Likelihood Ratio	5.823	1	.016	.020	.013
Fisher's Exact Test				.020	.013
Linear-by-Linear Association	6.132 ^c	1	.013	.020	.013
N of Valid Cases	282				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 11.54.

b. Computed only for a 2x2 table

This section has clearly revealed the technical practices of employees in terms of using mobile devices. This includes the managing of credentials with software, updating devices from public networks, saving work documents to a free cloud storage and adhering to security measures. All of these questions help to clearly understand what to

include in the security framework. The following section will investigate the social practices of employees and the security threats encountered.

5.4.4 Social practices

A bivariate analysis was carried out to determine whether there is a significant relationship between social practices on items 18, 19 and 23 in the questionnaire (appendix B) and the security threats experienced on item 28 in the questionnaire (Appendix B). These specific items were chosen because the practices directly relate to some of the threats on item 28. For all these analyses, a chi-square test of independence was used to test for a significant relationship between social practices and the security threat. In addition, where the conditions for this test were not met, Fisher's exact test was used.

5.4.4.1 Clicking on items on social media

Participants were asked to indicate items on which they click on social media. These include links, advertisement and videos or audios. A bivariate analysis was carried out to determine whether there is a significant relationship between what was selected on item 18 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). Thereafter, a chi-square test of independence was used to test for a significant relationship between what was clicked, and the security threats experienced. The results are presented in Tables 5.17 to 5.21.

Links

A bivariate analysis was performed in Table 5.17 to show that there is a relationship between the row (clicking on links) and column (data leakage) variables. The relationship is such that clicking on links (item 18.1) is related to encountering data leakage (item 28.8) and not clicking on links (item 18.1) is associated with not encountering data leakage (item 28.8). The illustration in Table 5.17 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 139 is greater than the expected count of 120.8) and the NO/NO block (i.e. 52 is greater than the expected count of 33.8). Similarly, fewer than expected fell in the YES/NO (i.e. 101 is less than the expected count of 119.2) and NO/YES (i.e. 16 is less than the expected count 34.2) blocks. Thus, there is a relationship between the two variables.

Table 5.17: Cross-tab of respondents for clicking on links and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)	
			Yes	No
18.1 Clicking on Links (e.g. shortened links)	Yes	Count	139	101
		Expected Count	120.8	119.2
		% within 18.1 Links (e.g. shortened links)	57.9%	42.1%
		Std. Residual	1.7	-1.7
	No	Count	16	52
		Expected Count	34.2	33.8
		% within 18.1 Links (e.g. shortened links)	23.5%	76.5%
		Std. Residual	-3.1	3.1
Total	Count	155	153	
	Expected Count	155.0	153.0	
	% within 18.1 Links (e.g. shortened links)	50.3%	49.7%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between clicking on links and data leakage. Significantly more than expected respondents who clicked on links on the device experience data leakage ($\chi^2(1)=25.064$, $p<0.0005$). This is presented in Table 5.18.

Table 5.18: A chi-square test of independence for clicking on links and data leakage.

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	25.064 ^a	1	.000	.000	.000
Continuity Correction ^b	23.707	1	.000		
Likelihood Ratio	26.096	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	24.982 ^c	1	.000	.000	.000
N of Valid Cases	308				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 33.78.

b. Computed only for a 2x2 table

Advertisement

A bivariate analysis was performed in Table 5.19 to show that there is a relationship between the row (clicking on advertisement) and column (malicious messages were sent to your contact list without your knowledge) variables. The relationship is such that clicking on an advertisement (item 18.3) is related to encountering malicious messages

(item 28.8) and not clicking on an advertisement (item 18.3) is associated with not encountering malicious messages (item 28.8). The illustration in Table 5.19 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 136 is greater than the expected count of 124) and the NO/NO block (i.e. 43 is greater than the expected count of 31). Similarly, fewer than expected fell in the YES/NO (i.e. 108 is less than the expected count of 120) and NO/YES (i.e. 20 is lesser than the expected count of 32) blocks. Thus, there is a relationship between the two variables.

Table 5.19: Cross-tab of respondents for clicking on advertisement and malicious messages

			28.9 Malicious messages were sent to your contact list without your knowledge		
			Yes	No	Total
18.3 clicking on Advertisement	Yes	Count	136	108	244
		Expected Count	124.0	120.0	244.0
		% within 18.3 Advertisement	55.7%	44.3%	100.0%
		Std. Residual	1.1	-1.1	
	No	Count	20	43	63
		Expected Count	32.0	31.0	63.0
		% within 18.3 Advertisement	31.7%	68.3%	100.0%
		Std. Residual	-2.1	2.2	
Total	Count	156	151	307	
	Expected Count	156.0	151.0	307.0	
	% within 18.3 Advertisement	50.8%	49.2%	100.0%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between clicking on an advertisement and malicious messages. Significantly more than expected respondents who clicked on an advertisement on the device encounter malicious messages ($\chi^2(1)=11.532$, $p=0.0010$). This is illustrated in Table 5.20.

Table 5.20: A chi-square test of independence for clicking on advertisement and malicious messages

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	11.532 ^a	1	.001	.001	.001
Continuity Correction ^b	10.592	1	.001		
Likelihood Ratio	11.733	1	.001	.001	.001
Fisher's Exact Test				.001	.001
Linear-by-Linear Association	11.494 ^c	1	.001	.001	.001
N of Valid Cases	307				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 30.99.

b. Computed only for a 2x2 table

Videos/Audios

A cross-tabulation was used in Table 5.21 to show that there is a relationship between the row (clicking on videos/audios) and column (you received an access request to device resources as part of the terms and conditions to install) variables. The relationship is such that clicking on videos/audios (item 18.4) is related to encountering access requests to device resources (item 28.16) and not clicking on videos/audios (item 18.4) is associated with not encountering an access request to device resources (item 28.16). The illustration in Table 5.21 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 230 is greater than the expected count of 211.7) and the NO/NO block (i.e. 33 is greater than the expected count of 14.7). Similarly, fewer than expected fell in the YES/NO (i.e. 49 is less than the expected count of 67.3) and NO/YES (i.e. 28 is lesser than the expected count of 46.3) blocks. Thus, there is a relationship between the two variables.

Table 5.21: Cross-tab of respondents for clicking on videos/audios and access request to device resources

			28.16 You received an access request to device resources as part of terms & conditions to install		
			Yes	No	Total
18.4 Clicking on Videos/Audios	Yes	Count	230	49	279
		Expected Count	211.7	67.3	279.0
		% within 18.4 Videos/Audios	82.4%	17.6%	100.0%
		Std. Residual	1.3	-2.2	
	No	Count	28	33	61
		Expected Count	46.3	14.7	61.0
		% within 18.4 Videos/Audios	45.9%	54.1%	100.0%
		Std. Residual	-2.7	4.8	
Total	Count	258	82	340	
	Expected Count	258.0	82.0	340.0	
	% within 18.4 Videos/Audios	75.9%	24.1%	100.0%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between clicking on a video/audio and an access request to device resources. Significantly, more than expected respondents who clicked on a video/audio on their device receive an access request to device resources ($\chi^2(1)=36.510$, $p<0.0005$). This is presented in Table 5.22.

Table 5.22: A chi-square test of independence for clicking on videos/audios and access request to device resources

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	36.510 ^a	1	.000	.000	.000
Continuity Correction ^b	34.541	1	.000		
Likelihood Ratio	32.199	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	36.403 ^c	1	.000	.000	.000
N of Valid Cases	340				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 14.71.

b. Computed only for a 2x2 table

5.4.4.2 Types of confidential information attached on social media

Participants were asked to indicate types of confidential information attached on social media. A bivariate analysis was carryout to determine whether there is a significant

relationship between attaching confidential information on item 19 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). Thereafter, a chi-square test of independence was used to test for a significant relationship between attaching confidential information and the security threats experienced. The results are presented in Tables 5.23 and 5.24.

Customer bank statement

A bivariate analysis was performed in Table 5.23 to show that there is a relationship between the row (attaching customer bank statement) and column (unauthorized modification of confidential information) variables. The relationship is such that attaching a customer bank statement (item 19.1) is related to encountering unauthorized modification of confidential information (item 28.1) and not attaching a customer bank statement (item 19.1) is associated with not encountering unauthorized modification of confidential information (item 28.1). The illustration in Table 5.29 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 43 is greater than the expected count of 29.9) and the NO/NO block (i.e. 140 is greater than the expected count of 126.9). Similarly, fewer than expected fell in the YES/NO (i.e. 113 is less than the expected count of 126.1) and NO/YES (i.e. 17 is less than the expected count of 30.1) blocks. Thus, there is a relationship between the two variables.

Table 5.23: Cross-tab of respondents for attaching customer bank statement and unauthorized modification of confidential information

			28.1 Unauthorized modification of confidential information (e.g. customer's bank statement)	
			Yes	No
19.1 Attaching Customers bank statement	Yes	Count	43	113
		Expected Count	29.9	126.1
		% within 19.1 Customers bank statement	27.6%	72.4%
		Std. Residual	2.4	-1.2
	No	Count	17	140
		Expected Count	30.1	126.9
		% within 19.1 Customers bank statement	10.8%	89.2%
		Std. Residual	-2.4	1.2
Total	Count	60	253	
	Expected Count	60.0	253.0	
	% within 19.1 Customers bank statement	19.2%	80.8%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between attaching a customer bank statement to e-mails or instant messaging and the unauthorized modification of confidential information. Significantly more than expected respondents who attach a customer bank statement to e-mails or instant messaging experience unauthorized modification of confidential information ($\chi^2(1)=14.145$, $p<0.0005$). This is illustrated in Table 5.24.

Table 5.24: A chi-square test of independence for attaching customer bank statement and unauthorized modification of confidential information

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	14.145 ^a	1	.000	.000	.000
Continuity Correction ^b	13.086	1	.000		
Likelihood Ratio	14.533	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	14.100 ^c	1	.000	.000	.000
N of Valid Cases	313				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 29.90.

b. Computed only for a 2x2 table

5.4.4.3 Sharing password with the following people and security threats

Participants were asked to indicate the people with whom they share a password. This includes colleagues and family or friends. A bivariate analysis was carried out to determine whether there is a significant relationship between people with whom they share a password on item 23 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). Thereafter, a chi-square test of independence was used to test for a significant relationship between the people with whom they share a password and the security threats experienced. The results are presented in Tables 5.25 to 5.28.

Sharing password with Colleagues

A bivariate analysis was performed in Table 5.25 to show the relationship between the row (sharing password with colleagues) and column (data leakage) variables. The relationship is such that sharing a password with colleagues (item 23.1) is related to encountering data leakage (item 28.8) and not sharing a password with colleagues (item 23.1) is associated with not encountering data leakage (item 28.8). The illustration in Table 5.25 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 22 is greater than the expected count of 12.6) and the NO/NO block (i.e. 150

is greater than the expected count of 140.6). Similarly, fewer than expected fell in the YES/NO (i.e. 3 is less than the expected count 12.4) and NO/YES (i.e. 133 is less than the expected count 142.4) blocks. Thus, there is a relationship between the two variables.

Table 5.25: Cross-tab of respondents for sharing password with colleagues and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)		Total
			Yes	No	
23.1 Sharing password with Colleagues	Yes	Count	22	3	25
		Expected Count	12.6	12.4	25.0
		% within 23.1 PW	88.0%	12.0%	100.0%
		Std. Residual	2.7	-2.7	
	No	Count	133	150	283
		Expected Count	142.4	140.6	283.0
		% within 23.1 PW	47.0%	53.0%	100.0%
		Std. Residual	-.8	.8	
Total	Count	155	153	308	
	Expected Count	155.0	153.0	308.0	
	% within 23.1 PW	50.3%	49.7%	100.0%	

For each of the variables, a chi-square test of independence was used to test for a significant relationship between sharing a password with colleagues and data leakage. Significantly more than expected respondents who share a password with colleagues experience data leakage ($\chi^2(1)=15.449$, $p<0.0005$). This is presented in Table 5.26.

Table 5.26: A chi-square test of independence for sharing password with colleagues and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	15.449 ^a	1	.000	.000	.000
Continuity Correction ^b	13.852	1	.000		
Likelihood Ratio	17.320	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	15.399 ^c	1	.000	.000	.000
N of Valid Cases	308				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 12.42.

b. Computed only for a 2x2 table

Sharing password with family/friends

A bivariate analysis was performed in Table 5.27 to show the relationship between the row (sharing password with family or friends) and column (data leakage) variables. The

relationship is such that sharing a password with family or friends (item 23.2) is related to encountering data leakage (item 28.8) and not sharing a password with family or friends (item 23.2) is associated with not encountering data leakage (item 28.8). The illustration in Table 5.27 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 46 is greater than the expected count of 32.7) and the NO/NO block (i.e. 134 is greater than the expected count of 120.7). Similarly, fewer than expected fell in the YES/NO (i.e. 19 is less than the expected count of 32.3) and NO/YES (i.e. 109 is less than the expected count of 122.3) blocks. Thus, there is a relationship between the two variables.

Table 5.27: Cross-tab of respondents for sharing password with family/friends and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)		Total
			Yes	No	
23.2 Sharing password with Family/friends	Yes	Count	46	19	65
		Expected Count	32.7	32.3	65.0
		% within 23.2 PW	70.8%	29.2%	100.0%
		Std. Residual	2.3	-2.3	
	No	Count	109	134	243
		Expected Count	122.3	120.7	243.0
		% within 23.2 PW	44.9%	55.1%	100.0%
		Std. Residual	-1.2	1.2	
Total	Count	155	153	308	
	Expected Count	155.0	153.0	308.0	
	% within 23.2 PW	50.3%	49.7%	100.0%	

Again for each of the variables, a chi-square test of independence was used to test for a significant relationship between sharing a password with family or friends and data leakage. Significantly more than expected respondents who share a password with family or friends experience data leakage ($\chi^2(1)=13.775$, $p<.0005$). This is illustrated in Table 5.28.

Table 5.28: A chi-square test of independence for sharing password with family/friends and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	13.775 ^a	1	.000	.000	.000
Continuity Correction ^b	12.758	1	.000		
Likelihood Ratio	14.126	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	13.730 ^c	1	.000	.000	.000
N of Valid Cases	308				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 32.29.

b. Computed only for a 2x2 table

This section has clearly revealed the social practices of employees in terms of using mobile devices. This includes clicking on different types of items, attaching confidential information on social media and sharing a password with colleagues, family or friends. All of these questions help to clearly understand what to include in the security framework. The following section will investigate the mobility practices of the employees and security threats encountered.

5.4.5 Mobility practices

A bivariate analysis was carried out to determine whether there is a significant relationship between mobility practices on items 24, 25, 26 and 27 in the questionnaire (Appendix B) and the security threats experienced in item 28 in the questionnaire (Appendix B). These specific items were chosen because the practices directly relate to some of the threats on item 28. For all these analyses a chi-square test of independence was used to test for a significant relationship between mobility practices and the security threat. Where the conditions for this test are not met, Fisher's exact test was used.

5.4.5.1 Methods used to prepare mobile device for disposal

Participants were asked to indicate methods used to prepare their mobile device for disposal. This includes permanently deleting data from the recycle bin, formatting the storage device, replacing the hard drive and resetting the device to the factory setting. A bivariate analysis was carried out to determine whether there is a significant relationship between the methods used to prepare a mobile device for disposal on item 24 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). Thereafter, a chi-square test of independence was used to

test for a significant relationship between methods used to prepare a mobile device for disposal and the security threats experienced. The results are presented in Table 5.29 to 5.36.

Permanently delete data from recycle bin

A bivariate analysis was performed in Table 5.29 to show the relationship between the row (permanently delete data from recycle bin to get rid of confidential information) and column (unauthorized modification of confidential information) variables. The relationship is such that permanently deleting data from the recycle bin to get rid of confidential information (item 24.1) is related to encountering unauthorized modification of confidential information (item 28.1) and not permanently deleting data from the recycle bin to get rid of confidential information (item 24.1) is associated with not encountering unauthorized modification of confidential information (item 28.1). The illustration in Table 5.29 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 52 is greater than the expected count of 36.5) and the NO/NO block (i.e. 98 is greater than the expected count of 82.5). Similarly, fewer than expected fell in the YES/NO (i.e. 132 is less than the expected count of 147.5) and NO/YES (i.e. 5 is less than the expected count of 20.5) blocks. Thus, there is a relationship between the two variables.

Table 5.29: Cross-tab of respondents for permanently deleting data from the recycle bin and unauthorized modification of confidential information

			28.1 Unauthorized modification of confidential information (e.g. customer's bank statement)	
			Yes	No
24.1 Permanently delete data from the recycle bin to get rid of critical information	Yes	Count	52	132
		Expected Count	36.5	147.5
		% within 24.1 Permanently delete data from the recycle bin to get rid of critical information	28.3%	71.7%
		Std. Residual	2.6	-1.3
	No	Count	5	98
		Expected Count	20.5	82.5
Total	Count	57	230	
	Expected Count	57.0	230.0	
		% within 24.1 Permanently delete data from the recycle bin to get rid of critical information	19.9%	80.1%

A chi-square test of independence was used to test for a significant relationship between permanently deleting data from the recycle bin to get rid of critical information and the unauthorized modification of confidential information. Significantly more than expected respondents who permanently delete data from the recycle bin to get rid of critical information experience unauthorized modification of confidential information ($\chi^2(1)=22.730, p<0.0005$).

Table 5.30: A chi-square test of independence for permanently deleting data from the recycle bin and unauthorized modification of confidential information

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	22.730 ^a	1	.000	.000	.000
Continuity Correction ^b	21.284	1	.000		
Likelihood Ratio	27.005	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	22.651 ^c	1	.000	.000	.000
N of Valid Cases	287				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 20.46.

b. Computed only for a 2x2 table

Format the storage devices to get rid of critical information

A bivariate analysis was performed in Table 5.31 to show the relationship between the row (not formatting the storage devices to get rid of critical information) and column (data leakage) variables. The relationship is such that NOT formatting the storage devices to get rid of critical information (item 24.2) is related to encountering data leakage (item 28.8) and formatting the storage devices to get rid of critical information (item 24.2) is associated with not encountering data leakage (item 28.8). The illustration in Table 5.31 shows that more than the expected number of respondents fell in the NO/YES block (i.e. 117 is greater than the expected count of 88.9) and the YES/NO block (i.e. 84 is greater than the expected count of 55.9). Similarly, fewer than expected fell in the YES/YES (i.e. 34 is less than the expected count of 62.1) and NO/NO (i.e. 52 is less than the expected count of 80.1) blocks. Thus, there is a relationship between the two variables.

Table 5.31: Cross-tab of respondents for not formatting the storage devices to get rid of critical information and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)	
			Yes	No
24.2 Not formatting the storage devices to get rid of critical information	Yes	Count	34	84
		Expected Count	62.1	55.9
		% within 24.2 Format the storage devices to get rid of critical information	28.8%	71.2%
		Std. Residual	-3.6	3.8
	No	Count	117	52
		Expected Count	88.9	80.1
		% within 24.2 Format the storage devices to get rid of critical information	69.2%	30.8%
		Std. Residual	3.0	-3.1
Total	Count	151	136	
	Expected Count	151.0	136.0	
	% within 24.2 Format the storage devices to get rid of critical information	52.6%	47.4%	

Again, a chi-square test of independence was used to test for a significant relationship between not formatting the storage devices to get rid of critical and data leakage. Significantly more than expected respondents who do not format the storage devices to

get rid of critical information experience data leakage ($\chi^2(1)=45.527$, $p<0.0005$). This is represented in Table 5.32.

Table 5.32: A chi-square test of independence for not formatting the storage devices to get rid of critical and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	45.527 ^a	1	.000	.000	.000
Continuity Correction ^b	43.920	1	.000		
Likelihood Ratio	46.743	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	45.368 ^c	1	.000	.000	.000
N of Valid Cases	287				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 55.92.

b. Computed only for a 2x2 table

Replace the hard drive

A bivariate analysis was performed in Table 5.33 to show the relationship between the row (not replacing the hard drive of the device to get rid of the critical information) and column (data leakage) variables. The relationship is such that NOT replacing the hard drive of the device to get rid of the critical information (item 24.3) is related to encountering data leakage (item 28.8) and replacing the hard drive of the device to get rid of the critical information (item 24.3) is associated with not encountering data leakage (item 28.8). The illustration in Table 5.33 shows that more than the expected number of respondents fell in the NO/YES block (i.e. 129 is greater than the expected count of 116.2) and the YES/NO block (i.e. 40 is greater than the expected count of 27.2). Similarly, fewer than expected fell in the YES/YES (i.e. 18 is less than the expected count of 30.8) and NO/NO (i.e. 90 is less than the expected count of 102.8) blocks. Thus, there is a relationship between the two variables.

Table 5.33: Cross-tab of respondents for not replacing the hard drive of the device to get rid of the critical information and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)	
			Yes	No
24.3 Not replacing the hard drive of the device to get rid of the critical information	Yes	Count	18	40
		Expected Count	30.8	27.2
		% within 24.3 Replace the hard drive of the device to get rid of the critical information	31.0%	69.0%
		Std. Residual	-2.3	2.4
	No	Count	129	90
		Expected Count	116.2	102.8
		% within 24.3 Replace the hard drive of the device to get rid of the critical information	58.9%	41.1%
		Std. Residual	1.2	-1.3
Total	Count	147	130	
	Expected Count	147.0	130.0	
	% within 24.3 Replace the hard drive of the device to get rid of the critical information	53.1%	46.9%	

A chi-square test of independence was used to test for a significant relationship between NOT replacing the hard drive of the device to get rid of the critical information and data leakage. Significantly more than expected respondents who do not replace the hard drive of the device to get rid of the critical information experience data leakage ($\chi^2(1)=14.301$, $p<0.0005$). Thus, the relationship is such that not replacing the hard drive of the device to get rid of the critical information is related to data leakage and replacing the hard drive to get rid of the critical information is associated with not encountering data leakage. This relationship is significant.

Table 5.34: A chi-square test of independence for not replacing the hard drive of the device to get rid of the critical information and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	14.301 ^a	1	.000	.000	.000
Continuity Correction ^b	13.203	1	.000		
Likelihood Ratio	14.496	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	14.249 ^c	1	.000	.000	.000
N of Valid Cases	277				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 27.22.

b. Computed only for a 2x2 table

Resetting the devices to factory default settings

A bivariate analysis was performed in Table 5.35 to show the relationship between the row (not resetting the device to factory default settings to get rid of critical information) and column (data leakage) variables. The relationship is such that NOT resetting the device to factory default settings to get rid of critical information (item 24.4) is related to encountering data leakage (item 28.8) and resetting the device to factory default settings to get rid of critical information (item 24.4) is associated with not encountering data leakage (item 28.8). The illustration in Table 5.35 shows that more than the expected number of respondents fell in the NO/YES block (i.e. 118 is greater than the expected count of 92.4) and the YES/NO block (i.e. 73 is greater than the expected count of 47.4). Similarly, fewer than expected fell in the YES/YES (i.e. 28 is less than the expected count of 53.6) and NO/NO (i.e. 56 is less than the expected count of 81.6) blocks. Thus, there is a relationship between the two variables.

Table 5.35: Cross-tab of respondents for resetting the device to factory default settings to get rid of critical information and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)	
			Yes	No
24.4 Not Resetting the devices to factory default settings to get rid of the critical information	Yes	Count	28	73
		Expected Count	53.6	47.4
		% within 24.4 Reset the devices to factory default settings to get rid of the critical information	27.7%	72.3%
		Std. Residual	-3.5	3.7
	No	Count	118	56
		Expected Count	92.4	81.6
		% within 24.4 Reset the devices to factory default settings to get rid of the critical information	67.8%	32.2%
		Std. Residual	2.7	-2.8
Total	Count	146	129	
	Expected Count	146.0	129.0	
	% within 24.4 Reset the devices to factory default settings to get rid of the critical information	53.1%	46.9%	

A chi-square test of independence was used to test for a significant relationship between NOT resetting the devices to factory default settings to get rid of the critical information and data leakage. Significantly more than expected respondents that do not reset the devices to factory default settings to get rid of the critical information experience data leakage ($\chi^2(1)=41.248$, $p<0.0005$).

Table 5.36: A chi-square test of independence for not resetting the devices to factory default settings to get rid of the critical information and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	41.248 ^a	1	.000	.000	.000
Continuity Correction ^b	39.654	1	.000		
Likelihood Ratio	42.305	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	41.098 ^c	1	.000	.000	.000
N of Valid Cases	275				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 47.38.

b. Computed only for a 2x2 table

5.4.5.2 Methods used to dispose of obsolete or faulty devices

Participants were asked to indicate methods used to dispose of their mobile devices. This includes putting them up for sale, giving them to family or friends, and throwing away the faulty devices. A bivariate analysis was carried out to determine whether there is a significant relationship between the methods used to dispose mobile device on item 25 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (Appendix B). Thereafter, a chi-square test of independence was used to test for a significant relationship between methods used to dispose mobile device and the security threats experienced. The results are presented in Table 5.37 to 5.42.

Put it up for sale

A bivariate analysis was performed in Table 5.37 to show the relationship between the row (put it up for sale) and column (unauthorized modification of confidential information) variables. The relationship is such that putting it up for sale (item 25.1) is related to encountering unauthorized modification of confidential information (item 28.1) and not putting it up for sale (item 25.1) is associated with not encountering unauthorized modification of confidential information (28.1). The illustration in Table 5.37 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 38 is greater than the expected count of 28.4) and the NO/NO block (i.e. 136 is greater than the expected count of 126.4). Similarly, fewer than expected fell in the YES/NO (i.e. 112 is less than the expected count of 121.6) and NO/YES (i.e. 20 is less than the expected count of 29.6) blocks. Thus, there is a relationship between the two variables.

Table 5.37: Cross-tab of respondents for disposing of obsolete or faulty devices and unauthorized modification of confidential information

			28.1 Unauthorized modification of confidential information (e.g. customer's bank statement)	
			Yes	No
25.1 Put it up for sale	Yes	Count	38	112
		Expected Count	28.4	121.6
		% within 25.1 Put it up for sale	25.3%	74.7%
		Std. Residual	1.8	-.9
	No	Count	20	136
		Expected Count	29.6	126.4
		% within 25.1 Put it up for sale	12.8%	87.2%
		Std. Residual	-1.8	.9
Total	Count	58	248	
	Expected Count	58.0	248.0	
	% within 25.1 Put it up for sale	19.0%	81.0%	

A chi-square test of independence was used to test for a significant relationship between disposing of obsolete or faulty devices by putting them up for sale and unauthorized modification of confidential information. Significantly more than expected respondents disposing of obsolete or faulty devices by putting them up for sale experience unauthorized modification of confidential information ($\chi^2(1)=7.794$, $p=0.005$).

Table 5.38: A chi-square test of independence for disposing obsolete/ faulty device and unauthorized modification of confidential information

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	7.794 ^a	1	.005	.006	.004
Continuity Correction ^b	7.001	1	.008		
Likelihood Ratio	7.888	1	.005	.006	.004
Fisher's Exact Test				.006	.004
Linear-by-Linear Association	7.769 ^c	1	.005	.006	.004
N of Valid Cases	306				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 28.43.

b. Computed only for a 2x2 table

Give to family/friends

A bivariate analysis was performed in Table 5.39 to show the relationship between the row (give to family or friends) and column (data leakage) variables. The relationship is such that giving them to family or friends (item 25.2) is related to encountering data leakage (item 28.8) and not giving them to family or friends (item 25.2) is associated with

not encountering data leakage (item 28.8). The illustration in Table 5.39 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 126 is greater than the expected count of 109.3) and the NO/NO block (i.e. 60 is greater than the expected count of 43.3). Similarly, fewer than expected fell in the YES/NO (i.e. 89 is less than the expected count of 105.7) and NO/YES (i.e. 28 is less than the expected count of 44.7) blocks. Thus, there is a relationship between the two variables.

Table 5.39: Cross-tab of respondents for disposing of obsolete or faulty devices by giving them to family/friends and data leakage

			28.8 Data leakage (Confidential data were sold out to the bank's competitors)	
			Yes	No
25.2 Give it to family/friends	Yes	Count	126	89
		Expected Count	109.3	105.7
		% within 25.2 Give it to family/friends	58.6%	41.4%
		Std. Residual	1.6	-1.6
	No	Count	28	60
		Expected Count	44.7	43.3
Total	Count	154	149	
	Expected Count	154.0	149.0	
		% within 25.2 Give it to family/friends	50.8%	49.2%

A chi-square test of independence was used to test for a significant relationship between disposing of obsolete or faulty device by giving them to family or friends and data leakage. Significantly more than expected respondents who dispose of obsolete or faulty devices by giving them to family or friends experience data leakage ($\chi^2(1)=17.926$, $p<0.0005$).

Table 5.40: A chi-square test of independence for disposing of obsolete or faulty devices by giving them to family/friends and data leakage

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	17.926 ^a	1	.000	.000	.000
Continuity Correction ^b	16.870	1	.000		
Likelihood Ratio	18.224	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	17.867 ^c	1	.000	.000	.000
N of Valid Cases	303				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 43.27.

b. Computed only for a 2x2 table

Throw away faulty device

A bivariate analysis was performed in Table 5.41 to show the relationship between the row (throw away faulty device) and column (unauthorized modification of confidential information) variables. The relationship is such that throwing away a faulty device (item 25.3) is related to encountering unauthorized modification of confidential information (item 28.1) and not throwing away a faulty device (item 25.3) is associated with not encountering unauthorized modification of confidential information (item 28.1). The illustration in Table 5.41 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 25 is greater than the expected count of 15.1) and the NO/NO block (i.e. 185 is greater than the expected count of 175.1). Similarly, fewer than expected fell in the YES/NO (i.e. 55 is less than the expected count of 64.9) and NO/YES (i.e. 31 is less than the expected count of 40.9) blocks. Thus, there is a relationship between the two variables.

Table 5.41: Cross-tab of respondents for throwing away faulty device and unauthorized modification of confidential information

			28.1 Unauthorized modification of confidential information (e.g. customer's bank statement)	
			Yes	No
25.3 Throw away the faulty device	Yes	Count	25	55
		Expected Count	15.1	64.9
		% within 25.3 Throw away the faulty device	31.3%	68.8%
		Std. Residual	2.5	-1.2
	No	Count	31	185
		Expected Count	40.9	175.1
		% within 25.3 Throw away the faulty device	14.4%	85.6%
		Std. Residual	-1.5	.7
Total	Count	56	240	
	Expected Count	56.0	240.0	
	% within 25.3 Throw away the faulty device	18.9%	81.1%	

A chi-square test of independence was used to test for a significant relationship between disposing of obsolete or faulty devices by throwing them away and unauthorized modification of confidential information. Significantly more than expected respondents disposing of obsolete or faulty devices by throwing them away experience unauthorized modification of confidential information ($\chi^2(1)=10.867$, $p=0.001$).

Table 5.42: A chi-square test of independence for throwing away faulty device and unauthorized modification of confidential information

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	10.867 ^a	1	.001	.001	.001
Continuity Correction ^b	9.793	1	.002		
Likelihood Ratio	10.091	1	.001	.002	.001
Fisher's Exact Test				.001	.001
Linear-by-Linear Association	10.830 ^c	1	.001	.001	.001
N of Valid Cases	296				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 15.14.

b. Computed only for a 2x2 table

5.4.5.3 Sharing mobile devices with the following people

Participants were asked to indicate with whom they share their mobile device. This included colleagues and family or friends. A bivariate analysis was carried out to determine whether there is a significant relationship between sharing mobile devices with the people on item 26 in the questionnaire (Appendix B) and the experience of security threats on item 28 in the questionnaire (appendix B). Thereafter, a chi-square test of independence was used to test for a significant relationship between with whom they share their mobile device and the security threats experienced. The results are presented in Table 5.43 to 5.46.

Sharing mobile device with colleagues

A bivariate analysis was performed in Table 5.43 to show the relationship between the row (sharing device with colleagues) and column (software keeps making copies of itself on the device) variables. The relationship is such that sharing a device with colleagues (item 26.1) is related to encountering software that keeps making copies of itself on the device (item 28.11) and not sharing the device with colleagues (item 26.1) is associated with not encountering software that keeps making copies of itself on the device (item 28.11). The illustration in Table 5.43 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 59 is greater than the expected count of 37.9) and the NO/NO block (i.e. 152 is greater than the expected count of 130.9). Similarly, fewer than expected fell in the YES/NO (i.e. 28 is less than the expected count of 49.1) and NO/YES (i.e. 80 is less than the expected count of 101.1) blocks. Thus, there is a relationship between the two variables.

Table 5.43: Cross-tab of respondents for sharing device with colleagues and software keeps making copies of itself on the device

			28.11 Software keeps making copies of itself on your device		
			Yes	No	Total
26.1 sharing device with colleague	Yes	Count	59	28	87
		Expected Count	37.9	49.1	87.0
		% within 26.1 M	67.8%	32.2%	100.0%
		Std. Residual	3.4	-3.0	
	No	Count	80	152	232
		Expected Count	101.1	130.9	232.0
		% within 26.1 M	34.5%	65.5%	100.0%
		Std. Residual	-2.1	1.8	
Total	Count	139	180	319	
	Expected Count	139.0	180.0	319.0	
	% within 26.1 M	43.6%	56.4%	100.0%	

A chi-square test of independence was used to test for a significant relationship between sharing a mobile device with colleagues and software that keeps making copies of itself on one's device. Significantly more than expected respondents sharing a mobile device with colleagues experience replication of software on their devices ($\chi^2(1)=28.594$, $p<0.0005$).

Table 5.44: A chi-square test of independence for sharing mobile device with colleagues and software keeps making copies of itself on one's device

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	28.594 ^a	1	.000	.000	.000
Continuity Correction ^b	27.254	1	.000		
Likelihood Ratio	28.726	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	28.504 ^c	1	.000	.000	.000
N of Valid Cases	319				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 37.91.

b. Computed only for a 2x2 table

Sharing mobile device with family/friends

A bivariate analysis was performed in Table 5.45 to show the relationship between the row (sharing device with family or friends) and column (personal information on your mobile device was used without your knowledge) variables. The relationship is such that sharing a device with family or friends (item 26.2) is related to encountering personal information on one’s mobile device being used without one’s knowledge (item 28.7) and not sharing a device with family or friends (item 26.2) is associated with not encountering personal information on one’s mobile device being used without one’s knowledge (item 28.7). The illustration in Table 5.45 shows that more than the expected number of respondents fell in the YES/YES block (i.e. 71 is greater than the expected count of 53) and the NO/NO block (i.e. 98 is greater than the expected count of 80). Similarly, fewer than expected fell in the YES/NO (i.e. 100 is less than the expected count of 118) and NO/YES (i.e. 18 is less than the expected count of 36) blocks. Thus, there is a relationship between the two variables.

Table 5.45: Cross-tab of respondents for sharing device with family/friends and personal information on one’s mobile device were used without one’s knowledge

			28.7 Personal information on your mobile device such as private photo, login credentials were used without your knowledge		
			Yes	No	Total
26.2 sharing device with family/friends	Yes	Count	71	100	171
		Expected Count	53.0	118.0	171.0
		% within 26.2 M	41.5%	58.5%	100.0%
		Std. Residual	2.5	-1.7	
	No	Count	18	98	116
		Expected Count	36.0	80.0	116.0
		% within 26.2 M	15.5%	84.5%	100.0%
		Std. Residual	-3.0	2.0	
Total	Count	89	198	287	
	Expected Count	89.0	198.0	287.0	
	% within 26.2 M	31.0%	69.0%	100.0%	

A chi-square test of independence was used to test for a significant relationship between sharing a mobile device with family or friends and personal information on one’s mobile device such as private photos and log-in credentials being used without one’s knowledge.

Significantly more than expected respondents sharing a mobile device with family or friends encounter personal information on their mobile devices being used without their knowledge ($\chi^2(1)=21.844$, $p<0.0005$).

Table 5.46: A chi-square test of independence for sharing mobile device with family/friends and personal information on your mobile device were used without your knowledge

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	21.844 ^a	1	.000	.000	.000
Continuity Correction ^b	20.646	1	.000		
Likelihood Ratio	23.172	1	.000	.000	.000
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	21.768 ^c	1	.000	.000	.000
N of Valid Cases	287				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 35.97.

b. Computed only for a 2x2 table

5.4.6 Security threats experienced

Table 5.47 shows the binomial test scores of responses ('yes', 'no' or 'not sure' responses) of security threats experienced. In this output ≤ 1 implies YES, while > 1 implies NO or NOT SURE. A significant proportion indicated that they have experienced unavailable networks during the cause of interaction (69 per cent, $p<0.0005$) and they have received messages stating that they have won a prize and should call a number to redeem the prize (73 per cent, $p<0.0005$). Another significant proportion indicated that they have received messages they have won a prize and should click a link to redeem the prize (75 per cent, $p<0.0005$). Similarly, a significant proportion indicated that they have received an e-mail request to update their personal information (78 per cent, $p<0.0005$) and a significant proportion indicated they have received an access request to device resources as part of terms and conditions to install (72 per cent, $p<0.0005$).

Table 5. 47: Binomial test to determine significant proportion of security threats experienced

	Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (2-tailed)
28.1 Unauthorized modification of confidential information (e.g. customer's bank statement)	Group 1	60	.17	.50	.000 ^a
	Group 2	298	.83		
	Total	358	1.00		
28.2 Unauthorized login into your storage account (e.g. Office server, Google)) drive)	Group 1	34	.09	.50	.000 ^a
	Group 2	324	.91		
	Total	358	1.00		
28.3 Unauthorized access to your social interactive network (e.g. Facebook, WhatsApp, BBM, WeChat)	Group 1	80	.22	.50	.000 ^a
	Group 2	278	.78		
	Total	358	1.00		
28.4 Unauthorized access to your bank account	Group 1	32	.09	.50	.000 ^a
	Group 2	325	.91		
	Total	357	1.00		
28.5 Unauthorized interception of private communication such as a phone call, instant message e.t.c.	Group 1	151	.42	.50	.004 ^a
	Group 2	207	.58		
	Total	358	1.00		
28.6 Unavailable network during the cause of interaction	Group 1	247	.69	.50	.000 ^a
	Group 2	111	.31		
	Total	358	1.00		
28.7 Personal information on your mobile device such as private photo, login credentials were used without your knowledge	Group 1	89	.25	.50	.000 ^a
	Group 2	268	.75		
	Total	357	1.00		
28.8 Data leakage (Confidential data were sold out to the bank's competitors)	Group 1	155	.43	.50	.015 ^a
	Group 2	202	.57		
	Total	357	1.00		
28.9 Malicious messages were sent to your contact list without your knowledge	Group 1	156	.44	.50	.020 ^a
	Group 2	201	.56		
	Total	357	1.00		
28.10 Confidential information were deleted without your knowledge (e.g. customer credential details)	Group 1	40	.11	.50	.000 ^a
	Group 2	317	.89		
	Total	357	1.00		
28.11 Software keeps making copies of itself on your device	Group 1	140	.39	.50	.000 ^a
	Group 2	217	.61		
	Total	357	1.00		
28.12 You saw a number in your dialing list that you haven't dialed	Group 1	47	.13	.50	.000 ^a
	Group 2	311	.87		
	Total	358	1.00		
28.13 You received messages that you have won a prize and should call a number to redeem the prize	Group 1	262	.73	.50	.000 ^a
	Group 2	96	.27		
	Total	358	1.00		
28.14 You received messages that you have won a prize and should click a link to redeem the prize	Group 1	269	.75	.50	.000 ^a
	Group 2	88	.25		
	Total	357	1.00		
28.15 You received e-mail request to update your personal information (e.g. login credentials)	Group 1	278	.78	.50	.000 ^a
	Group 2	80	.22		
	Total	358	1.00		
28.16 You received an access request to device resources as part of terms & conditions to install	Group 1	258	.72	.50	.000 ^a
	Group 2	100	.28		
	Total	358	1.00		

a. Based on Z Approximation.

However, a significant proportion indicated that they did not experience unauthorized modification of confidential information (83 per cent, $p < 0.0005$); they did not experience unauthorized login into a storage account (91 per cent, $p < 0.0005$); did not experience unauthorized access to social interactive networks (78 per cent, $p < 0.0005$); did not experience authorizing access to a bank account (91 per cent, $p < 0.0005$); did not experience unauthorized interception of private communication (58 per cent, $p = 0.004$); did not experience unauthorized usage of personal information (75 per cent, $p < 0.0005$); did not experience data leakage (83 per cent, $p = 0.015$); did not experience malicious messages (56 per cent, $p < 0.020$); did not experience replication of software (61 per cent, $p < 0.0005$); and did not experience unknown numbers in their dialling list (87 per cent, $p < 0.0005$).

This section has clearly revealed other security threats experienced. These include an unavailable network during the course of an interaction, receiving messages stating that they have won a prize and should call a number or click a link to redeem the prize, receiving an e-mail request to update their personal information and receiving an access request to device resources as part of terms and conditions to install. All of these responses help to clearly understand what to include in the security framework. The following sections (i.e. section 5.5) will further investigate organizations' practices (executive managers and ICT department personnel practices) in terms of using mobile devices.

5.5 Data analysis: Qualitative data

This section presents the threat identification for the qualitative data analysis. All the responses gathered from the structured interview with the ICT department personnel and executive managers of the Nigeria banking sector are presented in this section. The qualitative data provided additional information, thereby creating room for the triangulation of data. Fundamental to this section is to present and analyse findings of the non-numerical data from the study. The non-numeric data was transcribed using thematic analysis. The following section presents the non-numeric data collected for this study.

5.5.1 ICT Department personnel interview

Table 5.48 presents the categories and themes that emerged in the interviews conducted with the ICT department personnel of the four participating banks (i.e. two representatives each from the four banks). The emerged themes from the interviews were subsequently classified into three major categories, namely technical, social and mobility practices.

Table 5.48: Categories and themes that emerged in the qualitative analysis for IT personnel

Categories	Major Themes
1. Technical Practice	Mobile device registration
	Mobile device access to operational service
	Existing security measures
	Security threats experienced/reported
	Measures used to mitigate the security threats experienced or reported
	Aspects of the bank security that needs more focus
2. Social Practice	Social media
	Backup of organisation's information
	Employees' non-compliance with security policy
3. Mobility Practice	Sharing mobile device
	Lost/stolen device
	Mobile device disposal

5.5.1.1 Technical practice

This study carried out interviews to establish the banks' practices in relation to using mobile devices (which are either owned by the employee or the bank). The identified major themes from the semi-structured interview with the ICT Department personnel on questions number 4, 9, 10, 11, 12 and 14 (Appendix C) are presented in this section.

Mobile device registration

Three banks (A, C and D) acknowledged that they do not register employees' mobile devices. According to one participant:

"No, our bank do not register the mobile devices" (Participant 2).

Similarly, another participant commented:

“The bank does not see that as an issue so employee’s mobile device are not registered.” (Participant 7).

Again, another participant noted:

“The bank does not register employees’ mobile device.” (Participant 11).

In line with the above statements, it is apparent that the banks do not register employees’ mobile devices in their database for knowledge. Hence, the banks cannot easily trace or track down any abnormal behaviour in the network.

Mobile device access to operational service

Two banks (B and D) out of the four banks affirmed that they allow employees’ personal devices to access operational services. The narratives of the two participants are as follows:

“Yes, we allow employees’ personal devices to access operational services, but they must authenticate through active directory” (Participant 4).

“Employees’ personal devices are allowed to access operational services” (Participant 10).

This statement reveals that the banks permit employees’ personal devices to access operational services.

Existing security measures

The four banks (A, B, C and D) affirmed that they have certain forms of security measures. Some of the responses of the participants are stated as follows:

“My bank use firewall, antispysware and antivirus” (Participant 1)

“The bank makes use of proxy server, firewall, intrusion detection system, antispysware and antivirus” (Participant 5).

“Firewall, hardware token, and antivirus” (Participant 8).

“Proxy server, firewall, antispymware and antivirus are major security measures the bank uses” (Participant 11).

The above excerpts suggest that most of the security measures used in the Nigerian banking sector were central around firewall, anti-spyware and antivirus software.

Security threats experienced or reported

Two banks (A and D) affirmed that they have received security threats that have posed a risk to the Nigerian banking sector. According to a participant:

“Yes, some hackers attempted to access the bank’s network through a rogue device, but we were able detect on time through firewall” (Participant 1).

Another participant quipped that:

“Yes, there was a security threat by hackers using a keystroke logger from a remote access to allow a direct connection to a system already connected to a trusted website” (Participant 10).

The above excerpts confirm that there have been some security threats experienced by employees as identified from the quantitative analysis (section 5.4.3).

Measures used to mitigate the security threat experienced or reported

The two banks (A and D) use different approaches in mitigating the security threats. According to a participant:

“Through the firewall we were able to detect unauthorized access. There was an alert that calls the attention of the IT” (Participant 2).

Another interviewee reported:

“The IT department increased the security protocol by performing attack and penetration check to identify those vulnerable areas in the network that can easily

be accessed by both internal and external users. We also ensure a change of password was made on all the system that access the API” (Participant 11).

Aspects of the bank security that need more focus

Three banks (A, C and D) suggested different/various areas of the security system that need more focus. One of the participants remarked that:

“The bank needs a security program that can pinpoint unauthorized program attempting to transmit data over the bank’s network” (Participant 1).

Similarly, another participant indicated that:

“Customer database is prone to hackers” (Participant 5).

Again, another participant commented that:

“The banks’ network system” (Participant 11).

5.5.1.2 Social practice

This study carried out interviews to establish the banks’ practices in relation to social media, the backup of organisations’ information and employees’ non-compliance with security policy. The identified major themes from the semi-structured interview for ICT Department personnel on questions number 15, 16 and 17 (Appendix C) are presented in this section.

Social media

The four banks (A, B, C and D) affirm that they do not allow employees to access social media. The responses of the participants are stated as:

“Not all employees have access to social media, only the executive managers and the network filter help to filter unwanted messages. It is a crime for employee to indulge in that act” (Participant 2).

“The network team filters traffic in and outside the bank such that illegal access are easily detected and blocked. Access is blocked to some sites such as Facebook,

Twitter during working hours so that it won't consume the time bits, the more the traffic the slower the network" (Participant 4).

"Employees are not allowed to access to social media. It is against the bank's policy" (Participant 7).

"Access to social media are blocked during working hours so employees cannot access social media" (Participant 10).

The excerpts above suggest that employees are not allowed to access social media for official purposes. However, this is in contrast with the quantitative analysis which revealed that employees access social media and click on links, images, advertisement, videos and audios and games (section 5.4.4).

Backup of organisation's information

Three banks (A, B and D) confirm that they allow employees to back up work documents on their laptops as well as the bank's server. One of the participants stated that:

"Employees are allowed to backup work documents on server and laptop" (Participant 1).

Similarly, another participant remarked:

"The bank allows employees' to backup work documents on their laptops and the bank's server" (Participant 5).

Again, another participant commented:

"Employees are allowed to back up on the bank's server. Although the bank also allows backup on their laptop" (Participant 11).

Employees' non-compliance with security policy

All the four banks (A, B, C and D) assert that they have been faced with security threats due to employees' non-compliance with security policy. The responses of the participants are stated as follows:

“The bank has once been vulnerable to hackers which led to loss of confidential information” (Participant 2).

“Due to employees' non-compliance there have been cases of data leakage” (Participant 4).

“The bank lost some confidential information” (Participant 7).

“Several confidential information has been lost as a result of employees' non-compliance. This has also led to the dismissal of such employees” (Participant 10).

This is a validation of the security threats experienced as outlined in the quantitative analysis (section 5.4.3 to 5.4.6). This suggests that some of security threats faced in the Nigerian banking sector were central around non-compliance with security policies.

5.5.1.3 Mobility practice

This study carried out interviews to establish the banks' practices in relation to the sharing of mobile devices, lost or stolen devices and mobile device disposal. The identified major themes from the semi-structured interviews with ICT Department personnel on questions number 18, 22, 23 and 24 (appendix C) are presented in this section.

Sharing mobile devices

Two banks (C and D) out of the four banks affirmed that employees are not allowed to share their mobile devices. One of the participants remarked that:

““No, the bank does not allow employees' to share mobile devices” (Participant 8).

Another participant pointed out:

“Sharing of mobile device is not allowed when it is being used for work purpose”
(Participant 11).

The above excerpts are in contrast with the quantitative finding that revealed that employees’ do share their mobile devices (section 5.4.5). This explains the reason why some of the employees are experiencing security threats as identified in the quantitative analysis (section 5.4.5).

Lost/stolen devices

Three banks (A, C and D) acknowledged that they did not recover employees lost or stolen mobile devices. According to one participant:

“Yes, it was reported but not recovered” (Participant 1).

Another participant stated that:

“There was no way the bank could recover the lost/stolen device since it was not registered” (Participant 8).

Again, another participant remarked:

“There are reported cases of lost/stolen device, but the bank could not recover them” (Participant 11).

All the comments made by the participants suggest that that there have been cases of lost or stolen devices that were reported but not recovered. In addition to the lost/ or stolen devices, when questions were raised regarding how the banks were able to address the security threats caused by lost or stolen devices, the following responses were given:

“Unfortunately, the bank could not do anything to the security issues”
(Participant 2).

“If the mobile devices were registered, the bank would have been able to wipe out confidential data from the device but that was not possible since it was not registered” (Participant 5).

“There were no security measures used for the lost/stolen” (Participant 10).

The excerpts above imply that cases of lost or stolen devices are not been taken seriously as a major security concern.

Mobile device disposal

Two banks (B and D) affirmed that they allow employees to dispose of their mobile devices by themselves. According to a participant:

“It is employees’ personal device, so they are allowed to dispose it if they want to” (Participant 5).

Another participant responded that:

“Employees are allowed to dispose their mobile device, but they are at their own risk” (Participant 10).

These responses suggest that it is the sole responsibility of the employees to dispose of their mobile devices.

5.5.2 Executive managers’ interview

Table 5.49 presents the categories and themes that emerged in the interviews conducted with the executive managers of the four participating banks (i.e. one representative each from the four banks). This was done in order to examine the banks’ policies regarding the BYOD phenomenon. The themes emerged from the interviews were subsequently classified into three major categories, namely technical, social and mobility.

Table 5.49: Categories and themes that emerged in the qualitative analysis for executive managers

Categories	Major Themes
1. Technical practice	Policies that supports BYOD trend
	Acquisition, monitoring and maintenance
	Operating system
2. Social practice	Time interval for policy review
	Policy guiding employees' interaction
	Budget constraint for framework development
3. Mobility practice	Policy guiding retrieval of lost/stolen device
	Policy guiding disposal of faulty/obsolete device
	Policy guiding sharing of mobile device

5.5.2.1 Technical

This study carried out interviews to establish the banks' policies in relation to the BYOD phenomenon. The major themes identified from the semi-structured interviews with the executive managers on questions number 1, 2 and 3 (Appendix D) are presented in this section.

Policies that support BYOD trend

Three banks (A, C and D) out of the four banks indicated that they do not have a definite policy that supports the BYOD trend. The responses of the participants are stated as follows:

“There is no definite policy that support the use of BYOD” (Participant 3).

“The bank does not have a policy that guides BYOD” (Participant 9).

“There is no policy for BYOD. The bank might consider reviewing the security policy to accommodate BYOD phenomenon in the future” (Participant 12).

This implies that employees are allowed to bring their own devices without any policy guiding those devices.

Acquisition, monitoring and maintenance

The four banks (A, B, C and D) affirmed that they allow their employees to acquire the mobile devices they used for office work by themselves. In addition, two out of the four banks (A and B) admits they give out laptops to their employees. However, the banks do not monitor or maintain these devices. The statement below is a response from one of the participants and it reads as follows:

“In terms of acquisition, the bank gives out laptops to the employee for official purpose and also allows employees to bring in their personal devices such as smartphones and tablets. In terms of monitoring, we don’t monitor usage of these devices but update is being sent from the central server. In terms of maintenance, the IT department does the maintenance of the mobile devices” (Participant 3).

Similarly, another participant commented:

“Employees are allowed to personally acquire their mobile device. However, the banks do not monitor these devices. Also, the maintenance of these devices is the responsibility of the employee” (Participant 6).

Again, another participant commented thus:

“Since the bank allows employees’ to bring their mobile devices, it means they are allowed to acquire their mobile device. The bank does not monitor the device but if there is any form of security breach, the employee will be held responsible. In terms of maintenance, the employees’ takes care of their mobile devices’ themselves” (Participant 9).

Furthermore, another participant commented:

“The bank gives out laptops and also allows employees to acquire their personal devices such as smartphones and tablets. In terms of monitoring, the bank does not monitor apps or track mobile location” (Participant 12).

Operating system

The four banks (A, B, C and D) acknowledged that there is no specific operating system approved for employees’ mobile devices. The responses of the participants are stated as follows:

“The bank does not have any specific operating system approved for mobile device” (Participant 3).

“Employees’ are allowed to acquire their mobile device with any operating system they wish” (Participant 6).

“There is no restriction as to which operating system the device must have” (Participant 9).

“Employees can use whichever operating system they want” (Participant 12).

It can be inferred that the banks do not have a specific operating system expected to be used by the employees who bring their mobile devices to the bank.

5.5.2.2. Social

This study carried out interviews to establish the banks’ practices regarding the time interval for policy review, policy guiding employees’ interaction and budget constraints for framework development. The identified major themes from the semi-structured interviews with the executive managers on questions number 9, 10 and 11 (Appendix D) are presented in this section.

Time interval for policy review

Two banks (A and C) claim they do not have a specific time interval for reviewing security policy. One participant indicated:

“The bank does not have a particular interval for reviewing security policies” (Participant 3).

Another participant remarked:

“The bank only review security policy once there a need for it” (Participant 9).

From the excerpt above, it implies two banks only review security policy if they deem it necessary.

Policy guiding employees' interaction

The respondents claimed that there are restrictions that guide the interaction of ex-employees, disgruntled and outsourced employees. The responses of the participants are stated as follows:

“There are restrictions on the network that don't allow access to previous employees. For disgruntled employees', their activities are being monitored by their actions while contract employees don't have full access to the bank's resources same with outsourced employees” (Participant 3).

“Once an employee is disengaged, his/her rights and accessibility to bank's resources is withdrawn. There is no way the bank can know a disgruntled employee except he/she comes to complain. However, contract and outsourced employees' have limited access to the bank's resources” (Participant 6).

“Previous employees cannot access the bank's network because they have been disconnected. When the bank notices that an employee is misbehaving in an unusual way, then we know he/she is not happy. Both contract and outsourced employees' can only access limited resources” (Participant 9).

“Previous employees cannot access the bank's network; their access code has been disabled. The bank does not know if an employee is disgruntled or not. The bank does not give full access contract and outsourced employees” (Participant 12).

Budget constraint for framework development

Notably, two banks (B and D) confirmed that they do not have the financial capability in terms of developing a security framework. The statement below is a response from one of the participants and it reads as follows:

“Yes, we have budget constraint in upgrading the security system” (Participant 6).

Another participant commented:

“Most of the security resources are expensive, it will cost the bank a lot of money to acquire it and this is not in the bank’s budget” (Participant 12).

5.5.2.3. Mobility

This study carried out interviews to establish the banks’ policies regarding the retrieval of lost or stolen devices, the disposal of faulty or obsolete devices and the sharing of mobile devices. The identified major themes from the semi-structured interviews with the executive managers on questions number 12, 14 and 15 (Appendix D) are presented in this section.

Policy guiding retrieval of lost or stolen devices

Three banks (A, C and D) out of the four banks confirmed that the banks do not have a policy that supports the retrieval of lost or stolen devices. The responses of the participants are stated as follows:

“There is nothing the bank can do in terms of retrievals once it is lost or stolen” (Participant 3).

Once the bank is aware of the lost/stolen device the employee involved will be held responsible for the cost because there is no way the bank can retrieve it” (Participant 9).

The bank does not have a policy for retrieval of lost/stolen device. The bank can now start thinking of that” (Participant 12).

This implies that the bank does nothing regarding the lost or stolen devices; rather the employee is held responsible for any misfortune that comes out of it.

Policy guiding disposal of faulty/obsolete

The four banks (A, B, C and D) confirmed that they do not have a policy that guides the disposal of faulty or obsolete devices owned by employees. The statement below is a response from one of the participants and it reads as follows:

“No employee has the right to dispose the mobile device given to him/her by the bank, except the device owned by the employee” (Participant 3).

“The bank does not have anything to do with employees’ faulty/obsolete device. It is the responsibility of the employee to take care of it” (Participant 6).

“It is the responsibility of the employee; the bank has no policy for that” (Participant 9).

“So far the mobile device is for employees, they are at liberty to do whatsoever they want with it including disposing it” (Participant 12).

The above excerpt explains the reason why some employees are experiencing security threats as identified in the quantitative data (section 5.4.5).

Policy guiding sharing mobile devices

Two banks (A and B) out of the four banks indicated that there are no rules guiding the sharing of mobile devices but there are rules for sharing access rights. One of the participants remarked that:

“There are no rules guiding sharing of mobile devices but sharing of access right such as password is not allowed” (Participant 3).

“The bank only has rules for sharing of password but there are no rules guiding sharing of mobile devices” (Participant 6).

The above statement implies that employees are not guided in terms of sharing mobile devices. This validates the quantitative data that reveals that employees share mobile devices with colleagues and family or friends (section 5.4.5) but contradicts the quantitative data which shows that employees share passwords (section 5.4.4.3)

5.6 Summary

The study revealed the security threats associated with BYOD in the Nigerian banking sector which help to answer research questions one, two and three respectively. In addressing these questions, three variables (domains) of interest, namely, technical, social and mobility, were scrutinized. These domains were found to be suitable in identifying the security threats emanating from BYOD while exploring individual and organizational practices.

It is important to note that while the quantitative component of the study revealed different types of BYOD security threats that emanate from individual practices which were considered under these domains (technical, social, mobility), the qualitative component of the study revealed various types of security threats that emanate from organizations' practices and were also considered under the same domains.

Some sections of the qualitative study also support the findings of the quantitative study. For example, the quantitative study shows that employees share mobile devices because the qualitative findings indicate there are no rules guiding the sharing of mobile devices. However, contrary to the finding from the quantitative study which indicates that employees access social media to click on links, images and advertisement, the qualitative findings show that employees are not allowed to access social media for official purpose. Likewise, contrary to the quantitative study which reveals that employees share passwords, the qualitative findings reveal that there are rules guiding the sharing of passwords. This implies that employees do not comply with organizational rules and policy guiding the sharing of passwords. Additionally, while there seem to be no security threats relating to keystroke logging and rogue devices for the quantitative findings, the qualitative findings revealed some security threats experienced and these include keystroke logging and rogue devices. This indicates that keystroke logging and rogue devices are also part of BYOD security threats identified.

A discussion of the findings which concluded the development of a security awareness framework is presented in the next chapter (i.e. chapter 6).

CHAPTER 6: DISCUSSION OF FINDINGS

6.1 Introduction

This chapter discusses the results of the data analysis (both quantitative and qualitative results) that were presented in chapter 5. A comprehensive discussion in which the results corroborate or refer to past literature or theories on the security threats associated with the BYOD phenomenon is presented. The goal of this chapter is to establish whether research questions were answered and whether the objectives of the study were met. The relevant research questions considered for discussion are stated as follows:

1. What are the security threats associated with the technical system in the banking sector of Nigeria?
2. What are the security threats associated with the social system in the banking sector of Nigeria?
3. What are the security threats associated with the mobility system in the banking sector of Nigeria?

In addition, this chapter covers a detailed explanation as to whether the findings of the study confirm or refute the literature. The discussion on the findings emanating from the analyzed data explains the link between individual and organization practices in exploring BYOD security threats under three major domains, namely technical, social and mobility. Hence, section 6.2 provides a detailed discussion on technical security threats as they relate to BYOD hardware and software as well as the technical skills in the use of mobile device. Section 6.3 details social security threats as they relate to individuals' attitudes, and organizations' norms, principles, policies and values that define the practices among employees. Section 6.4 presents mobility security threats as they relate to the use of portable mobile devices while travelling, methods used to prepare mobile devices for disposal and methods used to dispose of mobile devices. Consequently, in this study, the findings are synthesized into a security framework for the Nigerian banking sector as discussed in chapter 7.

6.2. Technical security threats

In this study, technical security threats are threats emanating from the technical knowledge in the use of mobile devices as well as from BYOD hardware and software technology

used for work-related purpose. This technology supports the operation of the bank that enables communication and workflow (Bello et al., 2015). It is important to discuss these security threats because by their very nature, they can be harmful to individuals or organizations to the extent that they expose them to other security threats that require separate security management (Pratt Jr & Jones, 2013).

6.2.1 Quantitative findings

From the data collected through questionnaires from the bank employees on technical security threats, four major technical practices exercised by individuals (employees) that lead to security threats have been identified. Two out of these four technical practices which are “*allowing software on device to manage login credentials*” and “*saving work documents from laptop to a free cloud storage*” (questions number 7 and 12 in the questionnaire) have the same responses to the security threat which is “*data leakage*” (sections 5.4.3.1 and 5.4.3.3). Supporting this finding, Karen (2015) confirms that mobile device users that allow software to manage login credentials on their mobile devices are vulnerable to data leakage by other users who have access to their mobile devices. Not only can other users who gain access to their mobile devices log into their accounts, but hackers can do the same as well if the mobile device falls into wrong hands. This in turn leads to data leakage (Wang, Streff & Raman, 2012). On the other hand, Bakshi and Yogesh (2010) argue that free cloud storage such as iCloud, Dropbox and Google Drive enable individuals to copy files into the cloud for later retrieval. However, corporate information residing in such services may pose a security threat since they no longer reside in the protected corporate boundaries (Bakshi & Yogesh, 2010). Dimensional Research (2013) and Uz (2014) reveal that individuals that use free or personal hired cloud storage to save or backup information face the danger of “*data leakage and data ownership violation*”. This is because such information can be stolen by a knowledgeable hacker while uploading into the cloud storage (Dimensional Research, 2013; Uz, 2014). Furthermore, it can also be mismanaged by the third party (Bakshi & Yogesh, 2010).

The third technical practice, “*updating mobile device on public network*” (question number 11) leads to “*unauthorized modification of confidential information*” (section 5.4.3.2). According to Felt, Finifter, Chin, Hanna and Wagner (2011), unauthorized modification of confidential information occurs as a result of “*WiFi eavesdropping*”. WiFi eavesdropping works in several ways such as accessing confidential information,

accessing location information and activating a device's camera or microphone in order to modify information, or gain access to a user's browsing history (Du & Zhang, 2006). Hence, when individuals update their mobile devices on public networks, such a device is susceptible to WiFi eavesdropping (Chanda & Zaorski, 2013). Hackers take advantage of such wireless networks to eavesdrop on conversations and remotely modify messages from the device (Needham & Lampson, 2008). It is also important to note that accessing location information and activating a device's camera or microphone is also part of the function of WiFi eavesdropping (Du & Zhang, 2006). However, some studies have referred to "accessing location information" as "unauthorized location tracking" because it is being accessed under wrap (Nguyen et al., 2013). Most mobile device are endowed with various sensors that can be used to deduce the user's whereabouts and also collect as much data as possible (Nguyen et al., 2013). Unfortunately, most users are ignorant of this and have fallen prey to cybercriminals who use this information to perpetrate fraud (Enck, Gilbert, Han, Tendulkar, Chun, Cox and Sheth, 2014).

The fourth technical practice, namely "not adhering to security measures" (question number 15) leads to "unauthorized access to social interactive network", "software making copies of itself on the device" and "having an unknown number in the dialling list" (section 5.4.3.4). APWG (2013) refers to unauthorized access to social interactive networks as a type of "phishing". A phishing attack is a form of deception from hackers with the aim of collecting or forcing mobile device users to send confidential information about themselves (Ngoqo & Flowerday, 2015). It can be used to persuade individuals to download malicious applications onto their mobile devices (APWG, 2013). Disterer and Kleiner (2013) affirm that one of the major concerns of mobile users is when attackers spy on data exchanges being transmitted to a mobile device. In addition, Morrow (2012) refers to software making copies of itself on the device without the user's consent as a "virus". A virus affects the device negatively by altering the way the device works without the user's permission (Lee, 2015). In addition, "having an unknown number in a dialling list" is a form of "malware attack" (Wang et al., 2014). One of the ways malware functions is to initiate phone calls or encrypt data on one's device (Wang et al., 2014). For example, WannaCry is a type of malware which gets into the computer or mobile device through e-mail attachments or WhatsApp messages and automatically encrypts every file (Ehrenfeld, 2017). Furthermore, Karen (2015) and Juniper Network (2011) argues that some mobile device users do not enable the security software that comes with

their mobile devices because they believe using their mobile device to surf the Internet is safer or as safe as surfing on their computers.

6.2.2 Qualitative findings: ICT department personnel

The interview conducted with the ICT department's personnel confirms that there have been cases of security threats that involve hackers using a "*keystroke logger*" and "*rogue device*" from a remote area to access the organization's resources (section 5.5.1.1). Ladakis et al. (2013) argue that keylogging is used to record typed characters on mobile devices in order to capture valuable or sensitive information such as a user's identification, password and credit card numbers. The captured information is usually transferred to a cybercriminal e-mail address or website (Pratt Jr & Jones, 2013). Keylogging occurs when an attacker monitors and archives keystrokes in order to access sensitive information (Pratt Jr & Jones, 2013). On the other hand, a rogue device is an unauthorized connection of mobile devices to the network which poses a security threat to the organization (Golde et al., 2012). It is used to breach the key areas of security for mobile subscribers such as intercepting communication, impersonating traffic and tracking phones (Chen, Chen, Lin & Sun, 2014; Golde et al., 2012). This is a pointer to the fact that the organizations are vulnerable to any form of attacks.

6.2.3 Qualitative findings: Executive managers

From the interview conducted with the executive managers, three major technical practices exercised by the organization that lead to security threats are identified. Firstly, "*there is no definite policy guiding the use of BYODs*" (section 5.5.2.1). In other words, the organization lacks a BYOD policy guiding mobile device usage. Bello (2014) asserts that where there are no policies guiding the use of BYOD, security threats such as malware, phishing, and data leakage are inevitable. This confirms the security threats identified from employees (section 5.4.3). Supporting this claim, Vance et al. (2012) argue that owing to the liberty given to individuals to bring their own devices, most organizations are constantly facing several challenges in ensuring that the organizations' information is protected.

Secondly, "*the organization provides laptops to individuals' for official purpose as well as allowing employees to personally acquire their own mobile, but the organization does*

not monitor or maintain this device” (section 5.5.2.1). This implies that regardless of the organization-owned laptops given to individuals, they are allowed to acquire their own mobile devices and also maintain them personally. However, the effect of allowing individuals to acquire their devices implies a lack of control over what is on individuals’ devices and a lack of control over the amount of information that should be stored at the endpoint of the mobile device (Astani et al., 2013). Similarly, these devices are not being monitored, neither are they being maintained by the organization. This implies that individuals are at liberty to do whatsoever they want with their mobile devices which includes downloading unapproved applications. Supporting this claim, CISCO (2013) reveals that 69 per cent of BYOD users have unapproved applications which makes it challenging for the ICT department’s personnel to track the applications running on these devices. According to Rogers (2012), most mobile device users jailbreak their devices in order to enjoy the flexibility of downloading preferred software or modifying the operating system. “*Jailbreaking*” allows users to install third-party applications that are unavailable on official vendor stores, modify the operating system and perform other operation that would normally be restricted or that the manufacturer would not have allowed (Rogers, 2012). The implication of jailbreaking is that some applications are malicious in nature and if downloads are not being monitored, information security can be jeopardized once these applications have been downloaded (Gharibi, 2012).

Lastly, the finding reveals that “*the organization does not have a specific operating system approved to be used*” (section 5.5.2.1). The implication of this is that if some versions of an operating system no longer release updates or patches, it makes the device vulnerable to security threats such as malware, phishing and virus attacks (Gharibi, 2012). For example, patches on the latest versions of Windows give clues to vulnerabilities on older software that had not been discovered previously.

6.2.4 Overview of technical security threats

The section presents an overview of all the technical security threats identified. The data collected through questionnaires from the bank employees identified the following security threats: data leakage, WiFi eavesdropping, phishing, viruses and malware. The data collected through interviews with ICT departments’ personnel identified keystroke logging and rogue devices. However, the data collected through interviews with executive managers did not specifically identify any threat, but the literature points out some

security threats associated with their practices (section 6.2.3) which include malware, phishing, data leakage and jailbreaking. These security threats confirm the security threats identified through questionnaires from the bank employees. It is important to note that Nguyen et al. (2013) also identified unauthorized location tracking as one of the security threats associated with bank employees using their mobile devices outside the workplace (section 6.2.1).

This section has been able to establish the fact that these technical security threats occurred as a result of individuals' and organizations' practices which relate to all categories of BYOD hardware and software technology used for work-related purposes. It has also been able to ascertain that some of these technical security threats occur as a result of individuals' technical knowledge of the use of mobile devices. This suggests that there is a lack of adequate awareness and comprehension amongst employees on the severity and vulnerability of using mobile devices in a work context. Supporting this claim, Astani et al. (2013) maintain that security awareness on BYODs is so poor that it leaves businesses vulnerable to security threats.

6.3 Social security threats

In this study, social security threats are threats emanating from employees' attitudes and norms, and the organizations' principles, policies and values that define the practices of individuals (i.e. employees). Whilst these threats are normally not well addressed because of their invisibility compared to other forms of security threats, it is important that organizations recognise their influence on the security system (Bello et al., 2015). Otherwise, they have the potential to expose organizations to other security threats owing to their association with people and their environment (Arregui et al., 2016).

6.3.1 Quantitative findings

From the data collected through questionnaires from the bank employees, three major social practices exercised by individuals (employees) that lead to security threats have been identified. Firstly, "*Clicking on links*", "*advertisement*" and "*videos/audios*" on social media (question number 18 from the questionnaire) results in "*data leakage*", "*unsolicited malicious messages*" and "*access request to device resources*" respectively (section 5.4.4.1). According to Chanda and Zaorski (2013), hackers coax unsuspecting individuals into clicking on links on social media in order to steal and sell confidential

information in exchange for financial gain, hence leading to data leakage. Aula (2010) argues that some of the personal and organization's information made available on social media is being stolen by knowledgeable hackers who buy and sell the information in order to commit security breaches. Moreover, IBM (2014) describes the mass distribution of unsolicited malicious messages as "*spamming*". In spamming, massive amounts of unsolicited messages are sent to unsuspecting people directing them to visit a website where they are asked to update personal information such as passwords, and credit card and personal information (Lin, Lin, Chiou & Liu, 2013). Spamming can easily be found on the Internet via social networking sites (Lin et al., 2013; Sheu, Chu, Li & Lee, 2017). In addition, "*granting access request to device resources as part of the terms and condition to install*" can be regarded as "*jailbreaking*" (Rogers, 2012). Jailbreaking gives users the flexibility to download preferred software. However, some of these downloads are contaminated and they open the device up to security risks that can compromise sensitive data on the device (Rogers, 2012). Furthermore, if these devices are used in a BYOD-enabled environment, it will affect the information security of the organization (Arregui et al., 2016). Supporting this claim, Chanda and Zaorski (2013) reveal that when individuals access social media platforms (e.g. Facebook, Twitter, WhatsApp, LinkedIn) through their devices for either work or personal purpose, they risk endangering the organization's information by unknowingly acquiring "*malware, viruses and spyware*". Additionally, hackers coax unsuspecting individuals into clicking on links, images, advertisements, videos, games or downloading free applications that covertly deliver spyware which infiltrates the organization's entire system (Chanda & Zaorski, 2013).

Secondly, "*attaching customer bank statement to e-mail/instant messages*" (question number 19 from the questionnaire) results in "*unauthorized modification of confidential information*" (section 5.4.4.2). According to Du and Zhang (2006), unauthorized modification of confidential information is a form of "*WiFi eavesdropping*". This security threat is concomitant with several earlier works that also confirm that while it is convenient for an employee to attach confidential information to e-mails or instant messaging, it can be dangerous to the information security of the organization because such attachments can be captured in transit and modified (Goverdhan & Sammual, 2013).

Thirdly, “*sharing of password with colleagues or friends/family*” (question number 23 from the questionnaire) results in “*data leakage*” (section 5.4.4.3). Supporting these findings, Notoatmodjo and Thomborson (2009) assert that the greatest volume of security breaches comes from employees’ inadvertently misusing data as a result of shared passwords (Notoatmodjo & Thomborson, 2009). This implies that some employees casually share passwords in order to make their lives easier without any idea of how it might cause a security breach. They unknowingly share sensitive information that could fall into the wrong hands almost on a daily basis (Notoatmodjo & Thomborson, 2009).

6.3.2 Qualitative findings: ICT department personnel

In contrast to the quantitative findings on social media (section 5.4.4.1) where individuals (i.e. employees) acknowledged that they click on links, advertisements and videos or audios on social media, the interviews conducted with the ICT department personnel have revealed that “*the banks do not allow employees to use social media*” (section 5.5.1.2). This is a clear indication of employees’ non-compliance. Most BYOD users use social media as a platform to interact with other colleagues or other users (Aula, 2010). Unfortunately, some of the personal and organization’s information that is made available on the social media is being stolen and used to commit security breaches, referred to as “*data privacy violation*” (Aula, 2010). In addition, the interviews conducted with the ICT department personnel have revealed that “*organization information backups are allowed on laptops as well as the bank’s server*” (section 5.5.1.2). This is line with the quantitative results (section 5.4.3.3) where employees admit to saving work documents on laptops before uploading it to free cloud storage. However, Bakshi and Yogesh (2010) point out that free cloud storage services may pose a security threat such as data leakage (Bakshi & Yogesh, 2010). This is because such information can be stolen by a knowledgeable hacker while being uploaded into the cloud storage (Dimensional Research, 2013; Uz, 2014). These results satisfied the objective of utilizing mixed methods in this study owing to the limitations of mono methods (Creswell, 2013). However, while the portability of these mobile devices allows continuous access to work-related functions and personal information from any location, it also leads to incidences of theft or loss (Karen, 2015). The implication of such lost or stolen mobile devices is that confidential information can be compromised by a malicious hacker (Karen, 2015).

Lastly, the interviews conducted with ICT department personnel reveal “*employees’ non-compliance to security policies*” (section 5.5.1.2) which has resulted in “*loss of confidential information*”. Supporting this finding, CISCO (2009) confirms that 69 per cent of mobile device users do not comply with security policies: this has paved the way for hackers to penetrate and hack into the device. According to Ehimen and Bola (2010), employees’ non-compliance with security policies is a major challenge to any organization. Disterer and Kleiner (2013) argue that employees’ non-compliance is as a result of their inadequate knowledge of what constitutes a security threat.

6.3.3 Qualitative findings: Executive managers

From the interview conducted with the executive managers, three social practices exercised by the organization that lead to security threats have been identified. Firstly, “*there is no specified interval for reviewing security policies*” (section 5.5.2.2). In support of this finding, SAN (2001) affirms that the policies, standards, guidelines, and training materials that are not reviewed are “*obsolete*” and are particularly dangerous to any organization because management is often deceived into believing that security policies do not exist and that the organization is operating more effectively than it actually is. All organizations need to periodically review, test, and discard obsolete rules, controls, and procedures to avoid this false sense of security (Bulgurcu et al., 2010).

Secondly, “*disgruntled employees are only being monitored by their action*” (section 5.5.2.2). However, Cardenas et al. (2009) argue that merely monitoring disgruntled employees by actions may not be sufficient because the organization’s confidential information can easily be destroyed or compromised by a highly disgruntled employee. An employee normally becomes disgruntled owing to an unmet expectation or an unfortunate event such as been dismissed from work or not been promoted, or they could be dissatisfied with their current wages (CERT insider threat, 2015). Furthermore, disgruntled employees always have their target, which can either be the organization or a specific co-employee; whichever way, a disgruntled employee is a threat to any organization (Andrew & Kyle, 2015; CERT insider threat, 2015). According to Bulgurcu et al. (2010), there should be strict security policies that relate to disgruntled employees and which must be reviewed regularly.

Lastly, “*there are budget shortages in developing a security framework*” (section 5.5.2.2). This establishes the fact that there is an issue with the security policy just as the study has confirmed “*obsolete security policy*” (section 6.2.3). What this implies is that either the organization is ignorant of the potential security threats that can have a detrimental impact on the information security, or they are nonchalant about information security (Yayla & Hu, 2014).

6.3.4 Overview of social security threats

The section presents an overview of all the identified social security threats while the data collected from the bank employees through the questionnaire identified the following security threats: data leakage, spamming, jailbreaking and WiFi eavesdropping. The data collected through interviews with the ICT departments’ personnel identified employees’ non-compliance and loss of confidential information (i.e. data leakage). However, the data collected through interviews with executive managers did not specifically identify any particular threat but the literature point’s outs some security threats associated with their practices (section 6.3.3) which include obsolete security policies, budget shortages, and disgruntled employees. It is also important to note that the literature has established some other security threats that can also be found in the social domain which include malware, viruses and spyware, data privacy violation, data leakage and the sharing of passwords. These security threats confirm some of the technical threats identified (section 6.2.1). Hence, all these security threats will be taken into consideration in the development of a security framework.

This section has been able to establish the fact that these security threats relate to organizations’ principles, policies and values that define the practices of individuals (i.e. employees’). The organizations need to acknowledge that employees can be ‘the weakest link’ in the security environment because they fail to perform specified security functions owing to insufficient awareness (Johnston, Warkentin, McBride & Carter, 2016). Additionally, employees’ non-compliance is as a result of their inadequate knowledge of what constitutes a security threat (Kathleen, 2015). Thus, it is important for any organization to have adequate measures of security awareness.

6.4 Mobility security threats

In this study, mobility threats refer to those threats associated with device location. These devices are connected to secure and unsecure networks where the security policies differ (Bello, 2015). In addition, they also refer to the security threats experienced with methods used to prepare mobile devices for disposal as well as methods used to dispose of mobile devices.

6.4.1 Quantitative findings

From the data collected through questionnaires from the bank employees, there are three major mobility practices exercised by individuals (employees) that lead to security threats. Two out of these three mobility practices, namely “*methods used to prepare mobile device for disposal*” (question number 24 in the questionnaire) and “*methods employees’ used to dispose obsolete/faulty devices*” (question number 25 in the questionnaire) have the same responses to a security threat which is “*unauthorized modification of confidential information (i.e. WiFi eavesdropping)*” and “*data leakage*” (sections 5.4.5.1 and 5.4.5.2 respectively). Supporting this claim, Gartner (2014) asserts that methods used to prepare mobile devices for disposal can result in security breaches which can be harmful to organizational systems and customers’ information when such device are disposed of. What this implies is that the method used to prepare a mobile device before disposal certainly determines whether such a device will be vulnerable to attack when disposed of. Supporting these findings, the UCSC (2015) confirms that there are several reports of mobile device disposal (i.e. e-waste) that contained sensitive information which has led to exposure of data (i.e. data leakage). Unfortunately, most employees are not aware of this and have ignorantly fallen victim of data leakage (Keys, 2013). This implies that necessary precautions have to be taken to avoid these security threats.

Lastly, “*sharing mobile devices with colleagues*” and “*sharing mobile device with family/friends*” (question 26 in the questionnaire) lead to “*software making copies of itself on their device (i.e. virus attack)*” and “*personal information on their mobile device were used without their knowledge (i.e. phishing)*” respectively (section 5.4.5.3). A virus has been defined as a computer program which can make a copy of itself without the user's consent (Lee, 2015). It can cause the loss of critical information as it negatively

alters the way the computer works (Ghosh, Gajar & Rai, 2013). In addition, Khan (2013) referred to the situation where personal information on the mobile device is used without users' consent as "*phishing*". It is also important to note that when these devices are shared with colleagues or family and friends to check e-mails, social media or do other personal work, they can come across some confidential information (e.g. personal identification number) which can be retrieved and used without the knowledge of the owner (Ghosh et al., 2013). Thus, the study highlights the importance of awareness because phishing is not just a technical issue but also a mobility issue.

6.4.2 Qualitative findings: ICT department personnel

Contrary to the quantitative findings on the sharing of mobile devices (section 5.4.5.3) where employees admitted they share mobile devices, the interviews conducted with the ICT department personnel have revealed that "*employees' are not allowed to share their mobile devices*" (section 5.5.1.3). This implies that employees do not comply with the organizations' policy regarding sharing mobile devices. According to Karen (2015), most employees share their mobile devices that contain sensitive information without realizing the adverse effect.

Furthermore, the qualitative findings reveal that there have been cases of "*lost/stolen devices*" that were reported but not recovered (5.5.1.3). Supporting this finding, Juniper Network (2011) confirms that there have been several cases of security breaches as a result of lost or stolen devices in every sector, especially the banking sector. The implication of lost or stolen devices that contain confidential information is that it can be compromised by a malicious hacker (Juniper Network, 2011).

Again, the qualitative findings for ICT department personnel reveal "*how security issues caused by lost/stolen device was addressed*" (section 5.5.1.3). Unfortunately, the banks were unable to address security issues caused by lost or stolen devices (section 5.5.1.3) because these devices were not registered in the first place. If the device had been registered, the bank would have been able to remotely wipe off confidential data from the device using the device International Mobile Equipment Identity (IMEI) code (Friedman & Hoffman, 2008). Remote wipe can be used to either permanently delete data on a lost mobile device or recover the device (Friedman & Hoffman, 2008). However, before using these functionalities, it is recommended there should be a policy for this technology

asking users to sign a consent form (Friedman & Hoffman, 2008). This is because remote wipe could put users' personal data at risk (Friedman & Hoffman, 2008).

Lastly, the qualitative findings for the ICT department personnel reveal that "*employees are allowed to dispose their faulty/obsolete device by themselves*" (section 5.5.1.3). This finding is in affirmation of the findings from the executive manager, namely "*there is no policy guiding employees' disposal of mobile device*" (section 5.5.2.3.). The UCSC (2015) warns that the improper disposal of devices that contain a wealth of useful information can cause a security breach if they fall into wrong hands.

6.4.3 Qualitative findings: Executive manager

From the interview conducted with the executive managers, three major mobility practices exercised by the organization that lead to security threats were identified. Firstly, "*there is no policy that guides lost/stolen device*" (section 5.5.2.3). In other words, the bank does nothing to retrieve lost or stolen devices (section 5.5.2.3). This implies that the organization is nonchalant about missing devices. This could be as a result of a lack of awareness of what constitutes a security threat or inadequately crafted policy (Ghosh et al., 2013).

Secondly, "*there is no policy guiding sharing of mobile devices*" (section 5.5.2.3). This confirms the quantitative findings which also revealed that employees share mobile devices with colleagues, family and friends (section 5.4.5.3). This happens as a result of a lack of policy guiding the sharing of mobile devices. This implies that employees are at liberty to share their devices. However, the sharing of mobile devices with colleagues or family and friends has resulted in the security threats as identified in the quantitative analysis (section 5.4.5.3).

Lastly, the interview conducted with the executive managers affirms that "*that there is no policy that guides employees' disposal of mobile devices*" (section 5.5.2.3.). This finding confirms the qualitative findings from the ICT department personnel, namely "*employees are allowed to dispose of their mobile devices by themselves*" (section 5.5.1.3.). This also confirms employees' responses in the questionnaire where they acknowledged using different methods to dispose of their mobile devices has led to security threats (section 5.4.5.2).

6.4.4 Overview of mobility security threats

The section presents an overview of all the mobility security threats identified. The data collected through the questionnaire from the bank employees identified the following security threats: WiFi eavesdropping, data leakage, viruses and phishing. The data collected through interviews with the ICT departments' personnel identified the sharing of mobile devices, lost or stolen devices and faulty or obsolete devices as threats. Similarly, the data collected through interviews with executive managers identified lost/ or stolen devices, the sharing of mobile devices and the disposal of mobile devices (e-waste) as security threats. It is important to note that most of the security threats identified from the executive managers' findings confirm the security threats from the ICT department personnel.

This section has been able to establish the fact that most of these identified security threats occurred as a result of individual (employees) and organization practices which relate to travelling from one location to another, methods used to prepare mobile devices before disposal and methods used to dispose of mobile devices. These findings show that there is inadequate awareness amongst individuals and organizations regarding the severity and vulnerability of using mobile devices outside the work environment as well as methods used to dispose of mobile devices. In support of this finding, some studies have argued whether individuals should be allowed to access or connect to the organizations' network with their mobile devices (Astani et al., 2013). The study thus recommends that organizations should have an awareness sensitization framework that conscientizes its employees (individual) on the threats posed to the institution as a result of the aforementioned practices.

6.5 Summary

This chapter concludes that there are some security threats that are peculiar to only one domain (i.e. they affect one domain at a time), whilst some security threats are related to two domains (i.e. they affect two domains at a time). Additionally, there are some security threats that are related to all three domains (i.e. they are common to three domains and only affect three domains at a time), hence a threat classification is required to give an understanding of the influence of these security threats. Additionally, in as much as organizations may have substantial knowledge of the subject of BYOD, research findings

have shown that individuals are either still not aware of the possible threats associated with BYOD or decide to ignore them. Most employees who bring their personal devices to the workplace to access organizations' information are not fully aware of what constitutes security threats. In addition, the organization does not ensure employees' compliance to security policies because they do not understand the severity of these security threats. Lack of awareness is capable of infiltrating all the risk regions regardless of the powerful firewalls, proxy servers and encryptions the organization may have (Elwess, 2015). However, it is important to know the influence of these security threats on the banking sector. Hence, the outcome of the data analysis and the interpretation were used to answer the fourth research question which gave rise to the development of the security awareness framework (chapter 7).

CHAPTER SEVEN: THREE-DIMENSIONAL (3-D) SECURITY FRAMEWORK FOR BYOD ENABLED BANKING INSTITUTIONS IN NIGERIA

7.1 Introduction

This chapter attempts to answer the fourth research question (section 1.4) by developing a security framework for the Nigerian banking sector based on the outcome of the research findings. Hence, the following five steps were followed:

Firstly, a broad classification of threats based on the influence of technical, social and mobility domains on the Nigerian banking sector is established in section 7.2. Threats' classifications are important in identifying the impact of the security threat at the various risk levels such as low risk, medium risk and high risk (Jouini, Rabai & Aissa, 2014). Moreover, it takes into consideration the security threats that threaten the systems and assists in understanding the appropriate capabilities and countermeasures per security impacts to reduce risks (Gerić & Hutinski, 2007).

Secondly, the classified security threats were further grouped based on individual and organization practices. This is to help in distinguishing the security threats that are specific to individual practices from organization practices as presented in sections 7.3 and 7.4 respectively. In addition, it helps the organizations to identify threats which influence their information systems and the areas which each threat could affect as a result of their practices and hence to protect their systems in advance (Jouini et al., 2014). Likewise, it gives the individuals a better understanding of threats and how to curtail practices that expose their mobile devices to vulnerabilities (Jouini et al., 2014).

Thirdly, solutions to the classified security threats as they relate to individual and organization practices are discussed in sections 7.5 and 7.6 respectively. In a BYOD-enabled environment, information security is critical for both individuals and organizations (Peltier, 2010). Whilst no one organization is immune to security threats, there is an urgency to proffer solutions that can mitigate against these security threats (Gerić & Hutinski, 2007). Hence the study proposes suitable countermeasures to mitigate the security threats.

Fourthly, the representation of the activities involved in device management as they relate to both individual and organization practices are presented in section 7.7. These activities include device acquisition, device monitoring, device maintenance and device disposal. Each activity enforces a connection between individual and organization. This is important as multiple systems are required to complete each activity involved in the management process for the various set of devices running several operating systems, which frequently leads to increased disintegration of data, workflows and processes between the systems in place (Miradore, 2016).

Lastly, a 3-D security framework for BYOD-enabled banking institutions in Nigeria is incrementally developed from section 7.2 and presented in section 7.8. This framework encompasses the security threats and their corresponding security solutions as well as the stages involved in device management with respect to both individual and organization practices. A security framework that captures the security threats has the potential to protect the banking sector from the security threats that can harm their business and expose them to significant market and revenue losses (Jouini et al., 2014).

7.2 Security threats classification

Threats classification is a representation of threats in diagrams or charts in order to enhance the organization's understanding (Margaret, 2013). It is a tool for communicating specific risks an organization is undertaking (Jouini et al., 2014). The goal of threats classification is to inform the organization of the various risk levels and their impact on the organization (Margaret, 2013). Thus, this study adopts a threats classification technique in exploring the influence of technical, social and mobility security threats in the Nigerian banking sector because it gives a clearer pictorial representation of the security threats that helps enhances the organization's understanding. It also creates security consciousness of the various risk levels of the security threats and how these affect the organization.

Hence, based on the discussion from the research findings in chapter six, security threats were considered under three major domains (i.e. technical, social and mobility). The following security threats, namely data leakage, WiFi eavesdropping, unauthorized location tracking, phishing, viruses, malware, jailbreaking, keylogging and rogue devices

(section 6.1) were identified under the technical domain. Similarly, data leakage, spamming, jailbreaking, WiFi eavesdropping, data privacy violation, malware, viruses, spyware, obsolete security policies, budget shortages, disgruntled employees, sharing of passwords, and employees' non-compliance (section 6.2) were identified under the social domain. Finally, WiFi eavesdropping, data leakage, viruses, malware, phishing, sharing of mobile devices, lost or stolen devices, faulty or obsolete devices and e-waste (section 6.3) were identified under the mobility domain.

From the above-mentioned security threats, there are some security threats that are specific to only one domain (i.e. they are common to only one domain and affect one domain at a time), whilst there are some security threats that are related to two domains (i.e. they are common to two domains and affect two domains at a time). Additionally, there are some security threats that are related to all three domains (i.e. they are common to three domains and affect all three domains at a time), hence a threat classification is required to give an understanding of the influence of these security threats. Furthermore, it will also be used to identify different risk levels, namely low, medium and high risk.

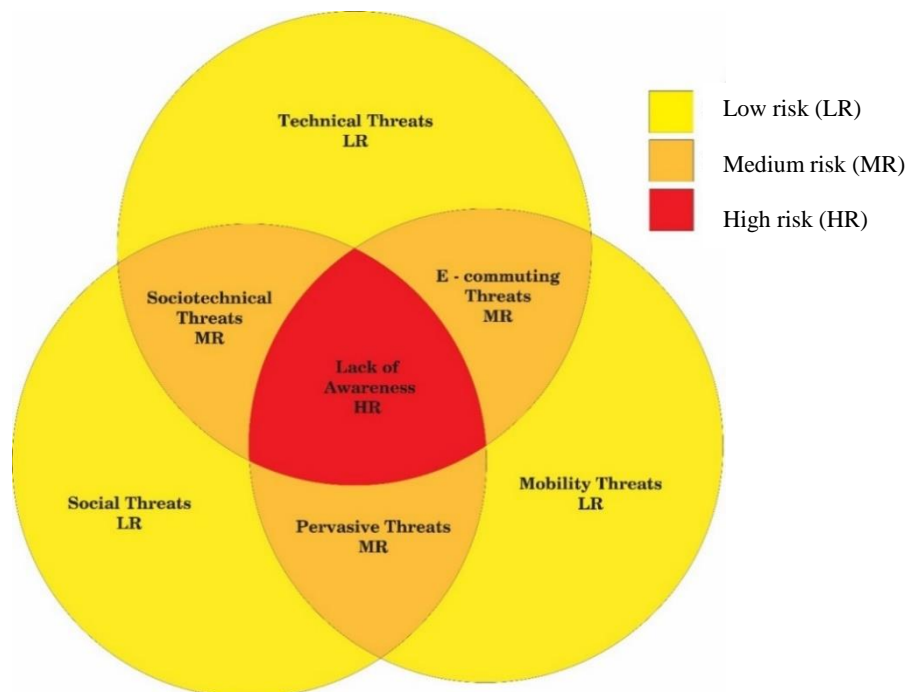


Figure 7.1: Broad classification of threats

Low risk

Goguen, Stoneburner and Feringa (2017) describe low risk (LR) security threats as threats that have little or no impact on information security systems. Similarly, in this study, LR represents those security threats that are specific to each domain: they do not affect more than one domain at a time (Figure 7.1). These include technical, social and mobility domains. The security threats that are specific to each of these domains are discussed as follows.

Technical threats are threats associated with software and hardware which are the core component of an organization's BYOD (Ketel & Shumate, 2015). Hence, key logging and rogue devices are technical threats which occur only in the technical domain. Similarly, social threats are threats emanating from people's attitudes and organizations' policies (Ifinedo, 2012). Whilst these threats are normally not well addressed because of their invisibility compared to other forms of security threats, it is important that organizations recognize their influence on the security system (Bello et al., 2015). Hence, employees' non-compliance, disgruntled employees, obsolete security policies and budget shortages are social threats which occur only in the social domain. Likewise, mobility threats refer to those threats associated with device location (Ghosh et al., 2013). These devices are connected to secure and unsecure networks where the security policies differ (Bello et al., 2015). In addition, they also refer to the security threats associated with methods used to prepare mobile devices for disposal as well as methods used to dispose of mobile devices. Hence, lost or stolen devices, faulty or obsolete devices, and e-waste are mobility threats which occur only in the mobility domain.

Thus, technical, social and mobility domains can be regarded as LR domains because the security threats are only related to one domain; they do not affect more than one domain at a time (Yang & Yao, 2009). Thus, LR are security threats that are harmful but not to the same extent as the other two risks that will be discussed later, namely medium risk (MR) and high risk (HR) (Ghosh et al., 2013).

Medium risk

Security threats are classified as medium risk (MR) if their impact on information security system is moderate (Goguen et al., 2017), in other words, if they are not considered to be high risk. In this study, MR represents those security threats that affect two domains at a

time (Figure 7.1). These include the socio-technical, pervasive and e-commuting domains. Hence, the security threats that are common to two domains will be identified and the literature will be referred to where necessary to properly assign the security threats that best fit these domains.

Sociotechnical threats are threats that are common to social and technical domains (Figure 7.1). The relationship is such that these security threats involve people communicating with one another through the use of network technology rather than the natural world, hence it is can be referred to as sociotechnical (Appelbaum, 1997; Ostwald, 2017). Thus, security threats such as jailbreaking, WiFi eavesdropping, data privacy violation and spamming are related to two domains (social and technical) and are considered under the sociotechnical domain.

Similarly, pervasive threats are threats that are common to social and mobility domains (Figure 7.1). The relationship is such that the interaction is between people and devices, hence it is can be referred to as pervasive (Urry, 2012). Thus, the sharing of mobile devices is related to two domains (i.e. social and mobility) and is considered under the pervasive domain.

Likewise, e-commuting threats are threats that are common to technical and mobility domains (Figure 7.1). This relationship is such that the threats occur as a result of work undertaken at a location while using mobile technology, hence it can be referred to as e-commuting (Raffaele & Connell, 2016). Thus, security threats such as unauthorized location tracking, phishing and spyware are related to two domains (i.e. technical and mobility) and are considered under the e-commuting domain.

Hence, sociotechnical, pervasive and e-commuting domains can be regarded as MR domains because the security threats are only common to two domains and can bring down the two domains at the same time if the right security measures are not put in place (Ghosh et al., 2013). Thus, MR are security threats that are harmful but not to the same extent as the High Risk (HR) and are more harmful than LR (Goguen et al., 2017).

High risk

High risk (HR) security threats are threats that could have a significant impact on information security systems if the right security measures are not put in place (Goguen et al., 2017). Thus, in this study, HR represents those security threats that affect the three domains at a time, hence they are referred to as a lack of awareness domain (Figure 7.1). The following security threats are considered under the lack of awareness domain, namely data leakage, viruses and malware. It is important to note that a lack of awareness is a fundamental issue responsible for most of the identified security threats that emanate from all categories of BYOD hardware, software, database and network technology (Astani et al., 2013). Furthermore, “*unavailable network during the cause of interaction*” (section 5.4.6) which is being referred to as ‘denial of service’ is also related to three domains (i.e. technical, social and mobility). The relationship is such that denial of service (DoS) involves someone who is technologically knowledgeable to be able to disrupt or make unavailable network resources intended for users (Dittrich, Reiher & Dietrich, 2004). In addition, “*receiving messages stating that they have won a prize and should call a number or click a link to redeem the prize*” (section 5.4.6) which is referred to as the ‘Wangiri scam’ also affects the three domains at the same time. The Wangiri scam is a type of phone fraud where the perpetrator dials random mobile numbers and then hangs up after one ring to give a missed call on the recipient’s phone (Geldenhuis, 2016). When the recipient returns this call (believing it to be a legitimate call), an avalanche of spam messages is triggered (Zhang, 2017). However, this can only happen when the individual or organization is not adequately informed of these security threats; hence it can be considered under the lack of awareness domain (Kathleen, 2015).

The lack of awareness domain is considered a HR domain because it affects the three domains at the same time which can be very harmful to the organization (Ghosh et al., 2013). Kathleen (2015) argues that lack of awareness is a major factor attributed to most security threats. Thus, it is very important for individuals and organizations to understand the risk level associated with the classified threats.

Based on the above-mentioned risk levels (i.e. low, medium and high), the study has been able to establish the influence of these security threats associated with technical, social and mobility domains on the Nigerian banking sector. Hence, both individuals and organizations need to be well informed of these security threats and take the necessary

precautions. Supporting this claim, Rose (2013) asserts that most employees that bring their mobile devices to the workplace to access organizations' information are not fully aware of what constitutes security risk. Some employees are completely unaware of the type of device allowed to be used in an organization as well as the security policies guiding those devices (Ray, 2014). Obviously, this lack of awareness is a major challenge that leads to some arguments among the researchers whether employees should be allowed to access or connect to the organizations' network with their mobile devices (Astani et al., 2013). Some studies also reveal that most networks have been hacked as a result of employees accessing organizations' information from their mobile devices (Astani et al., 2013; Ehimen & Bola, 2010). Although this study identified some security measures put in place such as firewalls, antivirus software, antispymware, proxy servers and intrusion detection systems (section 5.5.1.1), these are effective for mobile security but are not sufficient and may not address employees' and organizations' lack of awareness (Granneman, 2013). Furthermore, the findings reveal some areas that need more security focus which include the banks' network systems and customer databases (section 5.5.1.1). This also justifies the fact that the existing security measures are not sufficient, hence a security framework is required. However, in order to effectively develop this security framework, the classified security threats are grouped based on individual and organizational practices in sections 7.3 and 7.4 respectively. This is done in order to distinguish the security threats that are specific to individual practices from organization practices to be able to proffer solutions accordingly.

7.3 Threats based on individual practices

In this study, the security threats for individual practices are discussed under the classified threats which includes technical, social, mobility, sociotechnical, pervasive, e-commuting and lack of awareness threats.

Technical threats represent those threats that relate to susceptible device usage (Figure 7.2). Keystroke logging is considered under susceptible device usage. However, browsers' exploits and drive-by downloads can also be considered under susceptible device usage (Thilagavathi & Saradha, 2014). This is because they are associated with hardware, software and network technology (Ketel & Shumate, 2015).

Social threats relate to sabotage behaviour (Figure 7.2) such as employees' non-compliance and disgruntled employees. However, they are not limited to the above-mentioned; other social threats such as insider abuse and employees' sabotage can also be considered under sabotage behaviour (Matthew, 2013). This is because they are associated with individuals' attitudes (Ifinedo, 2012).

Mobility threats represent those threats that relate to device misuse (Figure 7.2). Hence, faulty or obsolete devices and lost or stolen devices are considered under device misuse. However, using recycled or pre-owned mobile devices can be also considered under device misuse (Kearns, 2016). Although recycling is generally considered to be a good thing, however when it comes to recycling mobile devices, it can constitute a security threat (Ghosh et al., 2013).

Sociotechnical threats are threats that are associated with data protection violation (Figure 7.2). The following security threats are considered under data protection violation, namely data privacy violation and jailbreaking. However, 'Man-in-the-middle' (MITM) can also be considered under data protection violation because it involves people communicating with one another through the use of network technology (Appelbaum, 1997; Ostwald, 2017).

Pervasive threats represent those threats that relate to ethical violation (Figure 7.2). Hence, the sharing of mobile devices is considered under ethical violations. However, other pervasive threats such as e-mail or instant messaging violation can be considered under ethical violations because it involves the interaction of people with devices (Urry, 2012).

E-commuting threats relate to location-based threats (Figure 7.2). Phishing and spyware are considered to be location-based threats. However, they are not limited to the above-mentioned; electronic eavesdropping can also be considered under location-based threats because it can occur as a result of work undertaken at a location while using mobile technology (Raffaele & Connell, 2016).

Lack of awareness represents those threats that relate to obliviousness as a result of individual practices. These include data leakage, Wangiri scam, viruses and malware.

These security threats occur as a result of individual obliviousness. However, they are not limited to the above-mentioned as employees' ignorance, carelessness and non-compliance (Ray, 2015) can also be attributed to a lack of awareness.

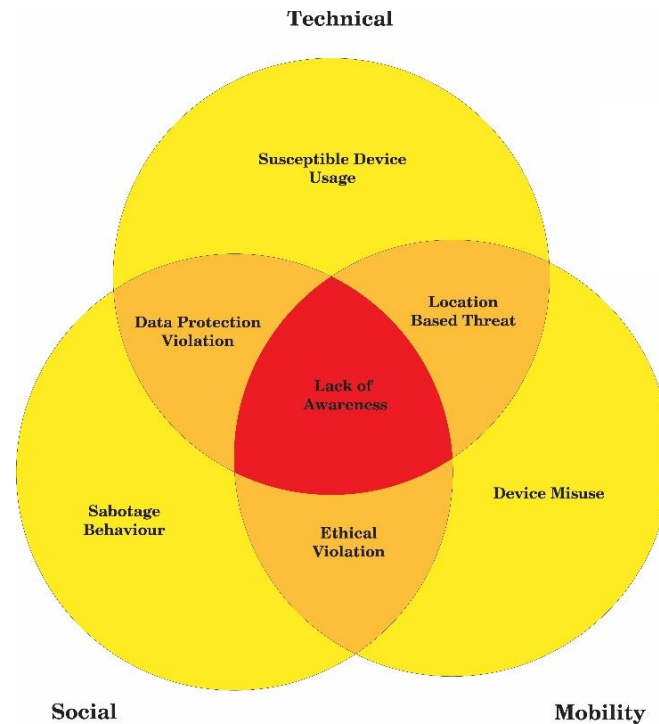


Figure 7.2: Threats based on individual practices

7.4 Threats based on organization practices

Again, the security threats for organization practices are presented under the classified threats which include technical, social, mobility, sociotechnical, pervasive, e-commuting and lack of awareness threats.

Technical threats represent those threats that relate to unrestricted device connectivity (Figure 7.3). Hence, a rogue device is considered under unrestricted device connectivity. Nevertheless, other technical threats such as script kiddies and network disruption can also be considered under unrestricted device connectivity because they are associated with hardware, software and network technology (Ketel & Shumate, 2015).

Social threats represent those threats that relate to the lack of an ICT policy (Figure 7.3). Obsolete security policies and budget shortages can be considered under a lack of an ICT

policy because they are associated with organizations' principles, policies and values (Ifinedo, 2012).

Mobility threats represent those security threats that relate to vulnerable remote devices (Figure 7.3). E-waste and lost or stolen devices are considered under vulnerable remote devices. However, they are not limited to the abovementioned; a defunct device can also be considered under vulnerable remote devices (Kearns, 2016).

Sociotechnical threats represent those security threats that relate to poor access control (Figure 7.3). Hence, WiFi eavesdropping and spamming are considered under poor access control. However, cyber stalking can also be considered under sociotechnical threats because it involves people communicating with one another through the use of network technology rather than the natural world (Appelbaum, 1997; Ostwald, 2017).

Pervasive threats relate to ICT policy violation (Figure 7.3). Sharing of passwords is considered under ICT policy violation. However, other pervasive threats such as data ownership violation and office e-mail violation can also be considered under ICT policy violation (Urry, 2012).

E-commuting threats relate to location-based intrusion (Figure 7.3). Hence, unauthorized location tracking is considered under location-based intrusion. Likewise, Trackmageddon flaws can be considered under location-based intrusion because they occur as a result of work undertaken at a location while using mobile technology (Raffaele & Connell, 2016).

Lack of awareness represents those threats that relate to laxity as a result of organization practices. These include denial of service and data leakage. They are not limited to the above-mentioned security threats as zero-day exploits can also occur as result of software flaws if the organization is not security conscious (Raffaele & Connell, 2016). Likewise, an organization's ignorance and carelessness (Ray, 2015) can be attributed to a lack of awareness.

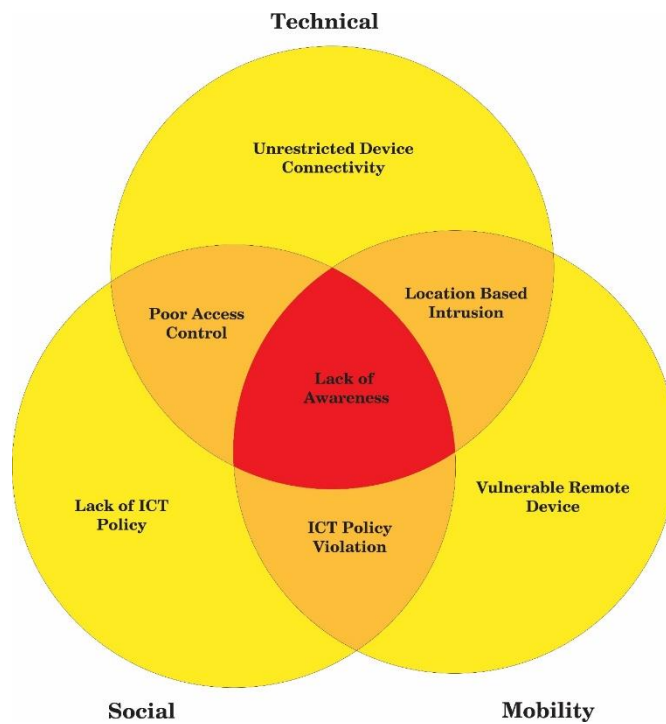


Figure 7.3: Threats-based organization practices

7.5 Solutions for threats arising from individual practices

In this study, the solutions to threats for individual practices are presented under technical, social, mobility, sociotechnical, pervasive, e-commuting and security awareness domains.

The technical solution refers to those security measures that relate to prescriptive device usage (Figure 7.4). This study proffers prescriptive device usage for individuals based on the security threats classified under susceptible device usage for individual practices (section 7.3). Although existing security measures such as firewalls, intrusion detection systems and proxy servers are effective for mobile security, they are not sufficient (Kearns, 2016). Sipponen (2000) laments that organizations are still struggling to reach a point where the workforce would internalize and follow given guidelines; as a result employees are still unaware of policies or they fail to apply them (Kearns, 2016). Thus, this study recommends prescriptive device usage for individuals. Individuals are expected to show full prescriptive commitment by adhering to organization security policies when using mobile devices in the workplace. Prescriptive commitment can take different forms

such as having individuals who will avoid installing unnecessary applications, avoid sharing organization's confidential information especially over unprotected networks, avoid jailbreaking, and have good physical control of mobile devices. This is an additional security measure to the existing security measures which include password authentication, personal firewall and antivirus software (Gui-Hong et al., 2010).

Social solutions refer to those security measures that relate to work agreement (Figure 7.4). This study recommends work agreement for individuals based on the security threats classified under sabotage behaviour for individual practices (section 7.3). According to Johnston et al. (2016), individuals are the "weakest link" in the security environment because they fail to perform specified security behaviours owing to insufficient awareness. Allowing employees to use their mobile devices for work purposes has raised several concerns (Silvergate & Salner, 2011). In a BYOD context, the concerns emphasize addressing the existing policies, regulations and legislations between employers and employees (Lebek et al., 2013). The BYOD philosophy causes violations of working hour regulations because employees are forever connected to jobs, even after working hours (Silvergate & Salner, 2011). Employees are able to access work materials on weekends, even on vacations. Consequently, this can lead to employees' demanding compensation for the expanded working hours (Silvergate & Salner, 2011). However, failure by the organization to compensate employees for the expanded working hours can lead to sabotage, industrial actions or even litigations by employees (to section 7.3). In addition, there is an assumption that employees are concerned about being liable when corporate information gets lost and when employees lose or damage their devices (Lebek et al., 2013). In order to avoid sabotage, industrial actions or even litigation, it is advisable in the interest of industrial harmony that employees request a review of working conditions from employers to accommodate demands which are associated with BYOD.

Mobility solutions refer to those security measures that relate to device protection (Figure 7.4). This study recommends device protection for individuals based on the security threats classified under device misuse for individual practices (section 7.3). Some organizations have introduced policies on individuals' use of mobile devices and data, thereby contributing to specific sections of the organization's handbook (Herath & Rao, 2009). Individual are expected to comply with the stipulated policy guiding the usage of mobile device; failure to do so puts the organization at significant risk (Herath & Rao,

2009). Furthermore, it is very important for individuals to enable mobile device security software such as anti-virus software or malware and personal firewalls. Antivirus software is used as a signature-based detection in a computer system or mobile device to identify, prevent and take action to remove malicious software programs, such as viruses, malware and worms (Friedman & Hoffman, 2008). An anti-virus program is known to scan several files on user's system to identify matches between each file's code and those in the signature database. Such identified matches are flagged as malware (Friedman & Hoffman, 2008). In addition, Friedman and Hoffman (2008) describe the role of a firewall on mobile devices as blocking the use of WiFi, Bluetooth and phone communication. A firewall is a software program or piece of hardware used to protect corporate resources from outside intruders (hackers, viruses, and worms) that try to reach the computer over the Internet (Clark, 2013). Security software has been known to help prevent security threats associated with mobile devices, hence it is advisable that individuals be more security conscious by enabling the security software on their mobile devices. It is also important that they abide by the conditions of use stipulated in the licenses that come with the software.

Sociotechnical solutions refer to those security measures that relate to data protection measures (Figure 7.4). This study recommends data protection measures for individuals based on the security threats classified under data protection violation for individual practices (section 7.3). It is important to protect confidentiality of corporate data on BYODs. Data encryption at rest and in motion helps to prevent data loss in the case of stolen or lost devices (Gui-Hong et al., 2010). Thus, it is recommended that individuals ensure that sensitive data such as passwords, login information and accounts must by no means travel unencrypted over a wireless system. This is to protect the data from hackers as a wireless system can be easily sniffed and thus compromised. Furthermore, the technical procedures and measures used for managing cryptographic keys should be effective (Nunoo, 2013).

Pervasive solutions refer to those security measures that relate to ethical principles (Figure 7.4). This study recommends ethical principles for individuals based on the security threats classified under ethical violation for individual practices (section 7.3). Ethical principles and values shape an organization's definition of acceptable behaviour (Dittrich & Kenneally, 2012). Hence, it is very important for individuals to have a robust

ethics and compliance initiative in a BYOD environment where mobile devices are used to enhance business operations. Some considerations for an individual determining an ethical principle and compliance initiative include being in accordance with the standards or rules for right conduct or practice, especially the standards of a profession (Dittrich & Kenneally, 2012). It also incorporates the values that most people associate with ethical behaviour such as being law abiding, honest and having integrity.

E-commuting solutions refer to those security measures that relate to data obfuscation (Figure 7.4). This study recommends data obfuscation for individuals based on the security threats classified under location-based threats for individual practices (section 7.3). Data obfuscation can help to safeguard confidential data by making it “harder to understand” (Drape, 2004). It is recommended that individuals ensure data security by obfuscating confidential data on their mobile devices. Location-based services collect location-related data and transmit it without the user’s consent or knowledge (Twinomurinzi & Mawela, 2014). This does not only raise concerns about vendor ethics and privacy, but also about what other kinds of sensitive data that applications may be transmitting without the employees’ knowledge or consent (Twinomurinzi & Mawela, 2014). Although location data helps mobile networks route calls faster and more efficiently, employees are going suddenly to find many useful tools are not so useful without location services. Furthermore, most mobile devices come with turn-on location services by default, but they all provide the option to turn them off (Su, 2016). It is advisable that individuals be aware of how applications (apps) use and share data with just a vague click-through agreement during installation (Su, 2016). Apps that are allowed to access communication networks may pose a risk to data security and organizations’ compliance (Gharibi, 2012).

Awareness refers to those security measures that create consciousness. It is very important that every employee should understand and comply with security policies and guidelines laid down by the organization. According to Ehimen and Bola (2010), the issue of non-compliance with security policies is a major challenge to most organizations. CISCO (2015) confirms that 69 per cent of mobile device users do not comply with security policies: this has paved the way for hackers to penetrate and hack into the device. However, Disterer and Kliner (2013) argue that employees’ non-compliance is as a result of their inadequate knowledge of what constitutes a security threat. Hence, having

revealed what constitutes security threats and the various risk levels, it is recommended that employees comply with the proffered solutions to these security threats as discussed in section 7.5. In addition, it is advisable that employees comply with the security policy and guidelines laid down by the organization.

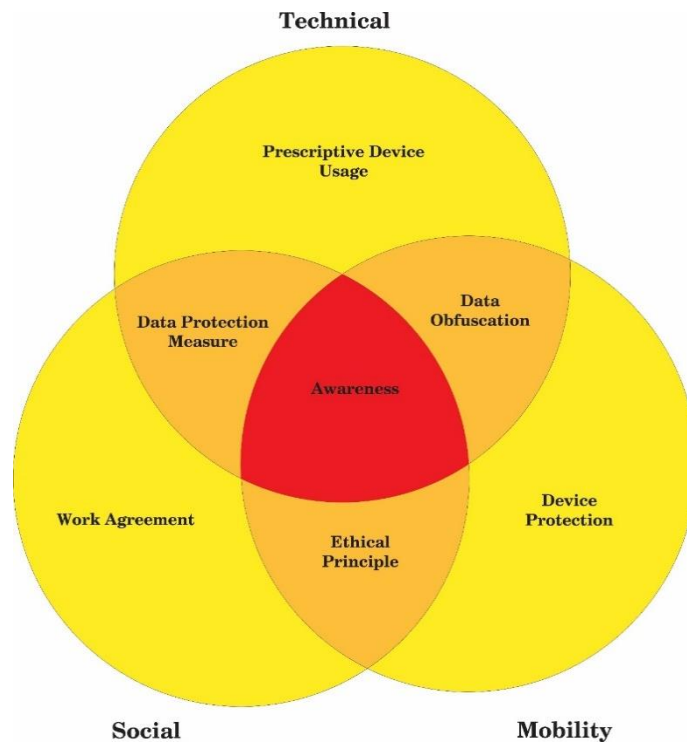


Figure 7.4: Solution for threats based on individual practices

7.6 Solution for threats arising from organization practices

In this study, the solutions to threats for organization practices are presented under technical, social, mobility, sociotechnical, pervasive, e-commuting and security awareness domains.

The technical solution represents those security measures that relate to restricted device connectivity (Figure 7.5). This study recommends restricted device connectivity for the organization as an additional security measure for technical solutions based on the security threats classified under unrestricted connectivity for organization practices (section 7.4). Restricting device connectivity is among the most significant of the security measures as individuals currently enjoy almost unrestrained access to networks and organizations' data at all times (Kearns, 2016). It is essential for organizations to monitor

and reject unauthorized and illegal access of corporate data. Unauthorized access comes from insiders (employees) when they are not supposed to access corporate data (Kearns, 2016). Illegal access comes from outsiders when they want to recover corporate data stored on a device, e.g. malicious users try to steal data from a lost device. Restricting device connectivity can be implemented to ensure each individual can only access information remotely that is consistent with limited privilege. Restricting device connectivity can include the following processes: device identification (e.g. International Mobile Equipment Identity (IMEI)), device ownership and device operating systems. These processes will ensure that rogue mobile devices do not gain unauthorized access. Furthermore, this study recommends a service-oriented approach (SOA) for the organization as an additional security measure. A SOA automatically downloads all the security measures when an employee's 'approved device' is connected to the organization's network and makes it active on the employee's device.

Social solutions represent those security measures that relate to establishing an ICT policy for an organization (Figure 7.5). This study proffers establishing an ICT policy based on the security threats classified under lack of an ICT policy for organization practices (section 7.4). Research findings reveal that organizations lack an ICT policy to insure data protection against threats created by the practice of BYOD (section 5.5.2.1). This lack of an ICT policy exposes the organization to security threats including malware and virus attacks, phishing, data leakage, compromised systems and services, and even criminal liability (Enisa, 2014; Yeh & Chang, 2007). It is important for an organization to create a well-defined ICT policy beyond a formal policy of a simple list of best practices. The policy should be designed to explain policy procedures and protect users from any unacceptable behaviours or mismanagement of these technologies by users. The process of creating an ICT policy should be in line with the Nigerian national policy for information technology and endorsed by the senior management; otherwise compliance will be difficult to maintain or achieved. However, it is not the responsibility of the IT team to create an ICT policy; rather it should be a steering team charged with the responsibility of pinpointing vital areas to address in the policy (Enisa, 2014). The IT team plans and implements the technical controls to follow the policy while the auditors decide whether the controls are compliant or not (Enisa, 2014). Once the policy has been created by the team, it must be enforced and followed (Yeh & Chang, 2007). The penalty for wilful non-compliance should be outlined in the policy and be circulated all over the

organization so employees are aware of it. It is important for an organization to review this policy at regular intervals. Furthermore, it is recommended that the policy encompasses adequate budget availability to update and maintain IT infrastructure. The cost of maintenance of an infrastructure asset can be determined by how well it was designed, its fitness for purpose, the quality of construction, and the materials specified and used and not just by the capacity, nature and size of that infrastructure (Su, 2016).

Mobility solutions represent those security measures that relate to vulnerable remote devices (Figure 7.5). This study proffers remote device management for the organization as an additional security measure for mobility solutions based on the security threats classified under vulnerable remote devices for organization practices (section 7.4). It is essential for every organization to protect devices that contain confidential information of corporate data used within a BYOD environment. In order to protect the device, Su (2016) opines that the organization can remove the native application (app) stores that come with the device operating system and instead provide a company one which only has approved (whitelisted) apps that users can download. This removes issues around licensing as the app store will only feature paid and licensed (where necessary for corporate use) apps. If an unlisted app is required, the administrator (or licensing committee) can consider making it available via to the app store once it has been vetted, tested, approved and licensed for use (Su, 2016).

Furthermore, it is recommended that certain device types that have not been built with tough security levels should not be allowed to contact the corporate network. In addition, mobile device disposal should be properly handled in order to avoid a detrimental effect on the organization (Keys, 2013). The methods used to prepare mobile devices for disposal will either increase or reduce the risks of attacks when they are disposed of (Keys, 2013). It is important that the organization should take absolute precautions when preparing mobile devices for disposal or else it may expose confidential information to unnecessary and entirely preventable security threats. Some of the precautions recommended that can be taken include formatting the storage devices, replacing the hard drive of the device or resetting the device to the factory default setting. It is also recommended that the organization have an e-waste management system put in place. Such a system should deal carefully with measures for mobile device disposal under any circumstances that do not pose a security threat to the organization or the environment.

Furthermore, the organization should endeavour to be updated with the latest scientific knowledge on the safe management of mobile device waste by undertaking more training in e-waste management (Keys, 2013).

Sociotechnical solutions refer to those security measures that relate to access control management (Figure 7.5). This study recommends access control management for the organization as an additional security measure for sociotechnical solutions based on the security threats classified under poor access control for organization practices (section 7.4). It is strongly recommended that organizations should ensure they have access control to the server. The access control involves both insider and outsider users who may want to access organizations' resources (Gui-Hong et al., 2010). Allowing access to organizations' resources should be based on the resources necessary for a user to perform his/her respective tasks while disallowing access to resources that are not relevant to the user. Access control can include the following three processes: authentication, authorization and audit (Gui-Hong et al., 2010). Authentication validates users' identifications (e.g. username and password or multifactor authentication) in order to grant access to resources. Authorization, the second process, permits users' access to the precise servers or applications while the third process, auditing, creates a users' activities trail. This will enable the administrator to analyze the trail and identify abnormalities that might reveal unauthorized access attempts on the users' part or inappropriate access assignment on the part of the administrators.

Pervasive solutions represent those security measures that relate to ensuring ICT policy compliance (Figure 7.5). This study recommends ICT policy compliance for an organization as an additional security measure for pervasive solutions based on the security threats classified under the ICT policy violation for organization practices (section 7.4). It is recommended that the organization should ensure relevant information security training is given to employees and executive management to assist in compliance with terms of policy. They should provide a series of security training tailored to meet the needs of the organization in order to ensure that they maximise the benefits of the IT services and information management systems. Furthermore, it is recommended that the security training should be designed for all employees which include the IT team and the executive managers who need to acquaint themselves with the world of security threats (Broughton et al., 2009).

E-commuting refers to those security measures that relate to location-based device usage control (Figure 7.5). This study proffers location-based device usage control for the organization as an additional security measure for e-commuting solutions based on the security threats classified under location-based intrusion for organization practices (section 7.4). Organizations can ensure location-based device usage control through device freezing, remote wiping and tracking device location. Device freezing ensures the safety of the devices and the important information they contain (Guo, Xu, & Chen, 2017). It allows the organization to remotely control the endpoint so that it can protect endpoint data, enforce best practices and manage the inventory. Device freezing can be used when the organization receives an alert that a suspicious activity has occurred such as a suspicious location, encryption that is not working or a username change (Lee et al., 2009). It can also be used to limit unauthorized roaming and control devices whenever employees are on a trip, as travel often puts devices and the data they contain at risk (Guo et al., 2017). Furthermore, when devices are in transit, they can be frozen until the end user is validated. In addition, many mobile device users have experienced panic whenever their mobile device is missing (Twinomurinzi & Mawela, 2014). The risks are raised even higher when a stolen or lost device is issued by the organization, or when the stolen or lost device is a personal device that an individual use for work purposes and which contains sensitive data (Karen, 2015). However, security can be further fortified with remote “find” and “wipe” capabilities (Friedman & Hoffman, 2008). These can be used to either permanently delete data on a lost mobile device or recover the device.

Before using these functionalities, it is recommended that there should be a policy for this technology asking users to sign a consent form (Karen, 2015). This is because “find me” services can raise privacy concerns while remote wipe could put a user’s personal data at risk (Friedman & Hoffman, 2008). Similarly, the global positioning system (GPS) helps to track the geographical location of mobile devices (Hofmann-Wellenhof, Lichtenegger & Collins, 2012). It calculates the exact longitude, latitude and altitude values which can be used in finding the location of the device (Kaplan & Hegarty, 2005). With GPS technology, the location of anyone carrying a GPS-enabled device can be accurately tracked at any time (Hofmann-Wellenhof et al., 2012). This can therefore be a useful feature for the Nigerian banking sector to track devices or connect with one another. It can also be used to track mobile devices that may be stolen or lost. In addition, this study

recommends switching between mobile device operating modes based on location and also restricting applications and information sharing based on location. This implies that when an employee is at a location other than the organization, the mobile device automatically switches operating mode and restricts applications or information sharing. This further strengthens the security system.

Awareness refers to those security measures that relate to an organization acquiring knowledge and disseminating the knowledge to the employees. The primary goal for organizations in creating an information security awareness programme is to change individuals' attitudes towards information security (Qudaih, Bawazir, Usman & Ibrahim, 2014). Organizations should endeavour to be updated with the latest scientific knowledge on security awareness such as the use of persuasive technology for employees. Persuasive technology can be used to change attitudes by conveying social presence and persuasion (Qudaih et al., 2014). For example, dialogue boxes can be used to persuade users to update software, to stop visiting malicious web sites, and to renew passwords. With all these, users may infer that the computing product is animate in some way to which can lead to their attitudes and their behavioural change.

According to Ferebee (2010), for an awareness programme to be effective and successful, organizations need to target people's behaviours, attitudes or mind-sets towards change. Persuasive technology is fundamentally about learning to automate behaviour change to that which can be effectively encoded in creating experiences that change behaviours in information security awareness in an organization (Fogg, 2009). The tools for creating persuasive products have become very easy to be used in organizations (Fogg, 2009). For example, organizations can design experiences and innovations in social networks, online videos, and presentations that influence people's behaviours by means of technology channels. Hence it is recommended that organizations use the persuasive technology to create awareness and to train their employees regarding information security, which can help employees to change their behaviour. This is an additional security measure to the existing security measures which include training on the acceptable use of ICT policies, information security and enforcement of security policies.

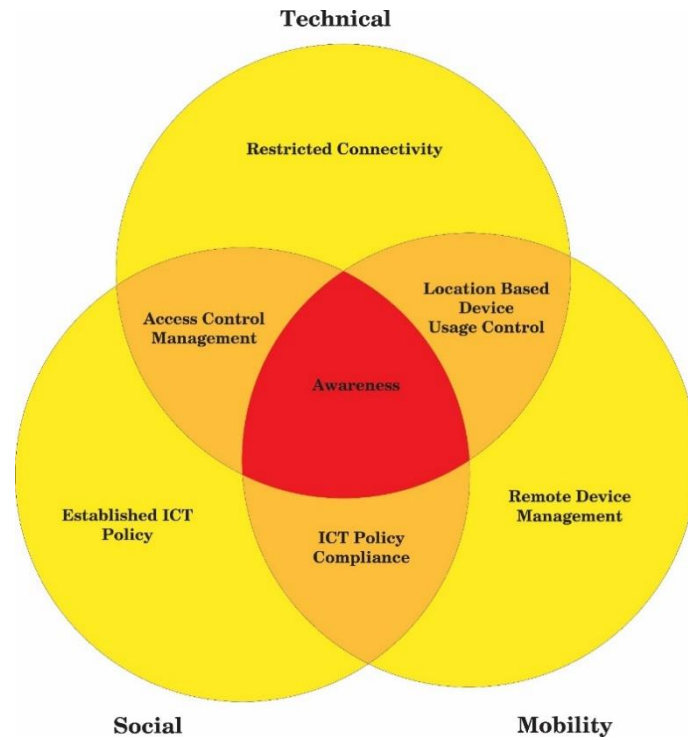


Figure 7.5: Solution for threats based on organization practices

For the purpose of clarity, the threats and solutions for individual practices as indicated in Figures 7.2 and 7.4 are summarized in Figure 7.6, while the threats and solutions for organization practices as indicated in Figures 7.3 and 7.5 are summarized in Figure 7.7.

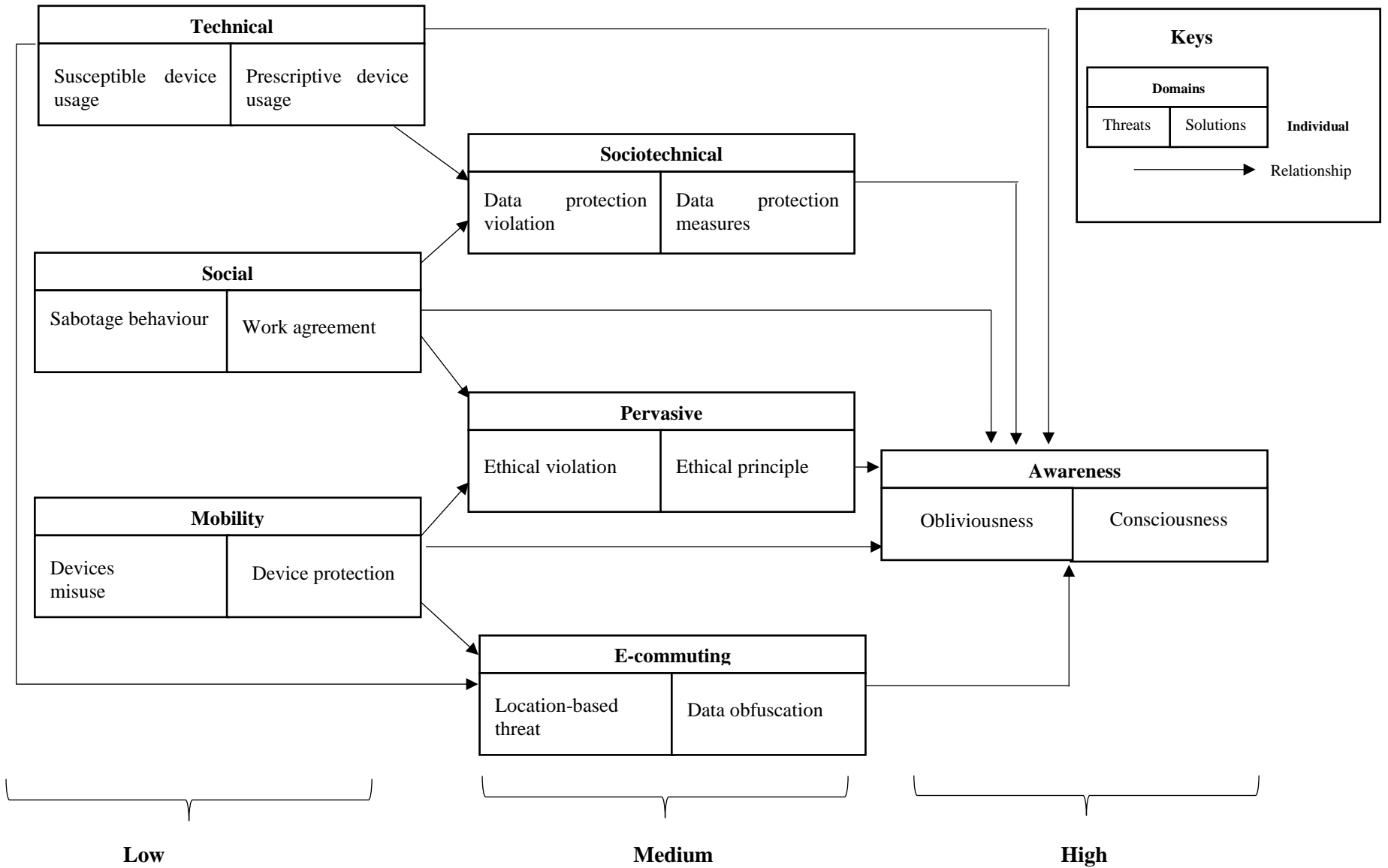


Figure 7.6: Summarized threats and solutions: Individual practices

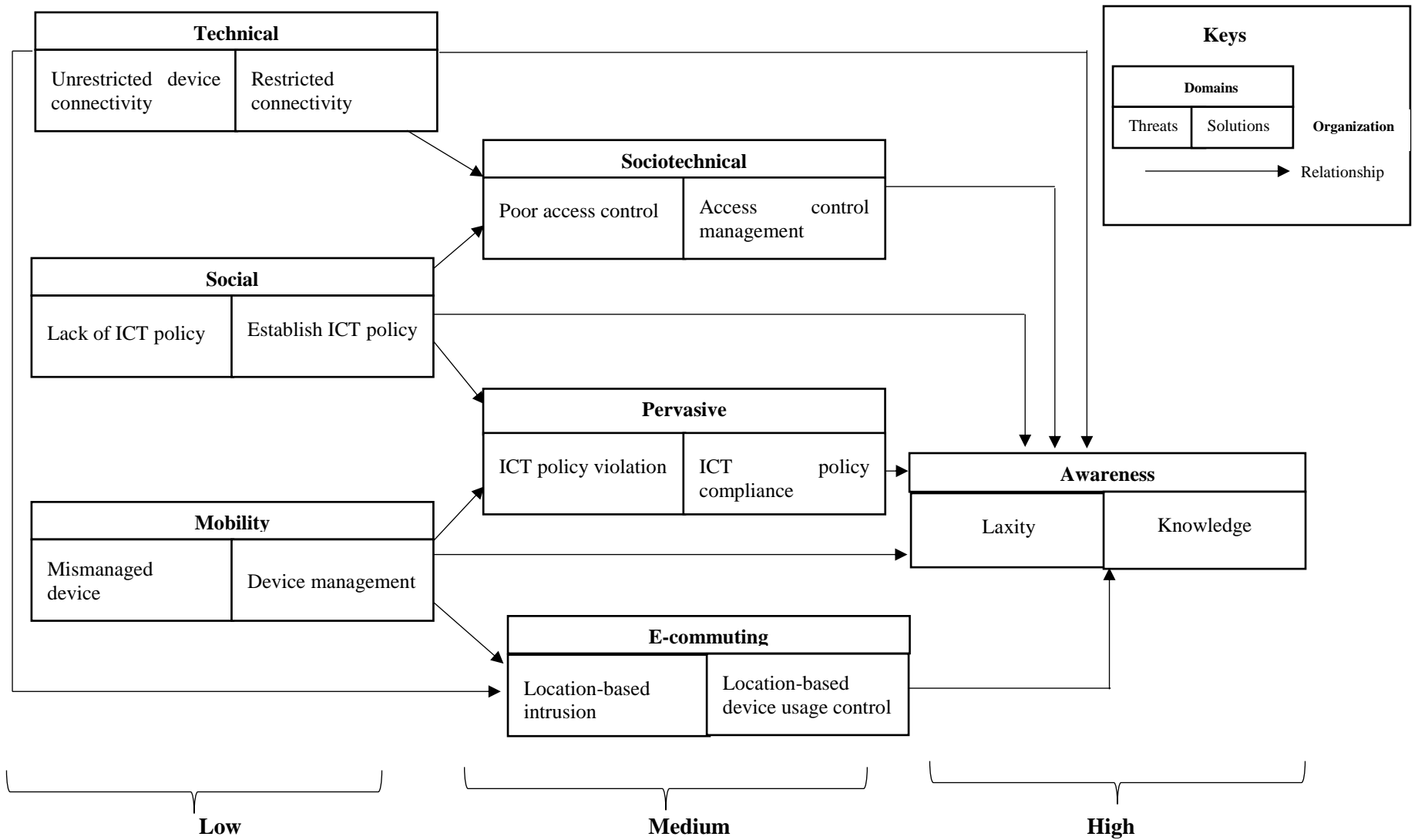


Figure 7.7: Summarized threats and solutions: Organization practices

To guarantee BYOD security, mobile device users must ensure they follow specific processes (Bello et al., 2015). This is essential because most BYOD users do not know how to protect both their devices and the information on them against security threats (Twinomurinzi & Mawela, 2014). Hence, as far as an information security system is concerned, it is imperative for individual and organization to be educated on the stages involved for device management to prevent security breaches (Twinomurinzi & Mawela, 2014). Hence, section 7.7 presents the various stages involved in device management.

7.7 Activities guiding device management

This section discusses the activities guiding device management for both individual and organization practices as they relate to BYOD. The activities are cyclical in nature and ensure a systematic best practice for both individual and organization. It is composed of four parts, namely device acquisition, device monitoring, device maintenance and device disposal. Each part of the processes enforces a connection between individual and organization. Figure 7.8 shows a pictorial representation of the flow of the recommended activities for device management.

7.7.1 Device acquisition

The research findings show that organizations give out mobile devices such as laptops to the employees for official purposes and also allow employees to acquire their own mobile devices such as smartphones, tablets and laptops (section 5.5.2.1). Supporting this finding, Lennon (2012) reveals that prior to the BYOD era, most organizations provided employees with mobile devices (laptops and smartphones). These devices were configured and given the right type of access as stipulated in company policy (Lennon, 2012). As the prices for smartphones started to drop, users started being able to afford them. As a result, advanced devices came out faster than organizations could afford to replace them (Wills, 2013). Wills (2013) further explains that replacing the devices was no longer feasible but organizations were forced to adopt mobile devices from employees, hence the emergence of BYOD. However, the study also confirmed there is no definite policy that guides the use of BYODs (section 5.5.2.1). Thus, organizations must have well-defined ICT policies that encompass device acquisition.

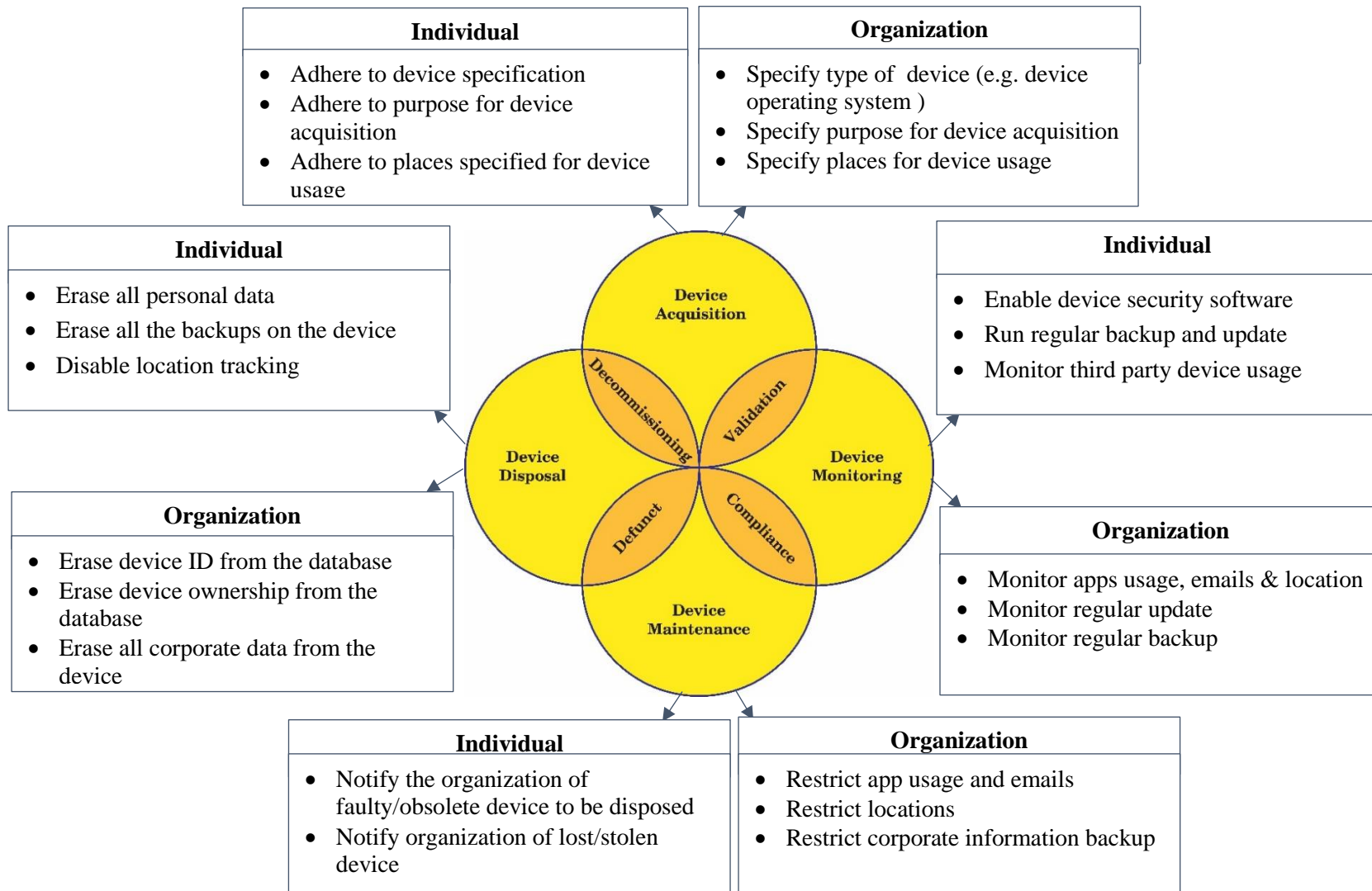


Figure 7.8: Activities guiding device management

In addition, organizations must specify the type of mobile device, the operating system, the purpose for acquisition, and the place where the device can be used. Furthermore, the research findings reveal that organizations do not register employees' mobile devices (section 5.5.1.1.). Bello et al., (2015) argues that it is the responsibility of the organization to register the device users and the device in the organization's database; this includes device identification e.g. International Mobile Equipment Identity (IMEI)), device ownership and the operation system (Twinomurinzi & Mawela, 2014). On the other hand, individuals (i.e. employees) need to adhere to device specification which includes the type of device and type of operating system. Furthermore, individuals are also expected to adhere to the purpose for device acquisition as well as places allowed for device usage.

7.7.2 Device monitoring

As employees are increasingly accessing privileged corporate information and applications, it is important they understand the security implications caused by personal or unknown devices entering the organizational environment (Twinomurinzi & Mawela, 2014). This study identified some security threats relating to the use of mobile devices (section 5.4.3 to 5.4.6). Thus, it is the responsibility of individuals to comply with the stipulated policy guiding the usage of mobile device by familiarising themselves with the terms of policy relating to the use of mobile devices (Enisa, 2014). Furthermore, individuals are expected to show prescriptive commitment (section 7.5) in adhering to organizations' security policies when using mobile devices in the workplace. It is also the responsibility of individuals to monitor and protect corporate data by enabling device security software, running regular updates, running regular backup and monitoring third party device usage (Kearns, 2016).

On the other hand, the study revealed that organizations do not monitor applications and location (section 5.5.2.1). It is advisable for organizations to monitor users' activities on the network such as regular updates, locations and apps usage (section 7.6). For example, the organization can monitor and prevent individuals from running apps that could compromise security such as those that record phone calls or access a user's contacts (Lennon, 2012). It can highlight unnecessary costs, such as excessive data use by certain apps and identify apps that cause direct or indirect licensing issues (section 7.6). This can be done using mobile

device management (MDM), intrusion prevention systems (IPSs), key management and firewalls (Wang et al., 2014).

7.7.3 Device maintenance

It is essential for organizations to restrict device usage relating to applications, e-mails, location and corporate information backup (Kearns, 2016). In addition, an organization can remove the native app stores that come with the device operating system and instead, provide a company one which only has approved (whitelisted) apps that users can download (Su, 2016). If an unlisted app is required, the administrator can consider making it available via the app store once it has been vetted, tested, approved and licensed for use. Furthermore, mobile devices that have not been built with tough security levels should not be allowed to contact the corporate network. On the other hand, it is the responsibility of individuals to notify the organization promptly of any faulty or obsolete device as well as any lost or stolen devices (Kearns, 2016). This guards against unnecessary security threats that can hijack data when a device is missing or sold (Gui-Hong et al., 2010).

7.7.4 Device disposal

From the data analysis, individuals (i.e. employees) have no right to dispose of mobile devices given to them by the organization, except in cases where the organization allows them to dispose of them (section 5.5.2.3). Thus, it is the responsibility of the individuals to protect their devices (section 7.5). Before disposing of the devices, employees must erase all personal data and backup data, and disable the location tracking. On the other hand, it is the responsibility of the organization to have strategies and procedures for device maintenance (section 7.6). Such a system should deal carefully with measures for mobile device disposal under circumstances that do not pose a security threat to the banking system or the environment (Keys, 2013). Before disposing of the devices, organizations must ensure they erase device ID from the databases, erase device ownership from databases and erase all corporate data from the devices. Furthermore, it is the responsibility of the organization to ensure that, if necessary, they should be updated with the latest scientific knowledge on the safe management of mobile device waste by undertaking more training in e-waste

management (Keys, 2013). The methods used to prepare mobile devices for disposal will either increase or reduce the risks of attacks when they are disposed of (Keys, 2013).

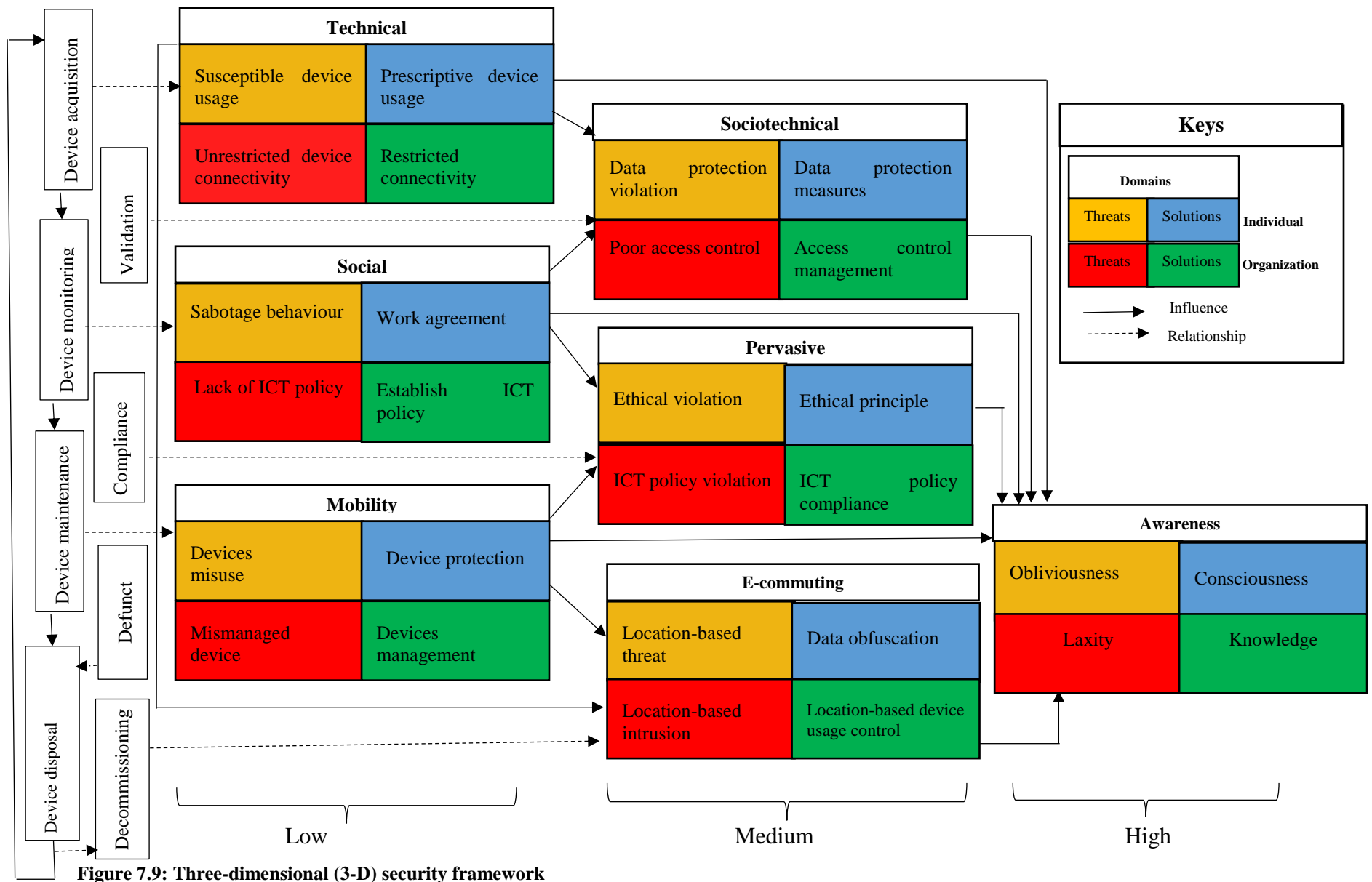
It is evident that risk management is a critical aspect that needs to be addressed when developing a security framework (Matinde, 2015). Therefore, to manage risk, individuals and organizations must understand the probability of the occurrence of security threats and their impact on the organization (NIST, 2018). This understanding gives the organizations the capability to determine the risk level which is expressed by its risk threshold (NIST, 2018). Furthermore, this information also gives the organization the capacity to prioritize their security activities (NIST, 2018).

7.8 Three-dimensional (3-D) security framework

This section presents a 3-D security framework that could be initiated in BYOD-enabled banking institutions where mobile devices are used by both individuals and the organization. It is important to note that this security framework is driven by the data collected for the threat identification of the study. The framework is composed of three parts: Firstly, ‘threats and solutions for individual practices’; secondly, ‘threats and solutions for organization practices’; and lastly, ‘the activities guiding the device management’. When these three parts are combined, it gives a strategic approach to managing the risk levels associated with each category of security threats as it relates to both individual and organization practices respectively.

The ‘threats and solution categories for individual practices’ and the ‘threats and solution categories for organization practices’ form the context in which an individual and an organization understand the security threats’ categories and the processes established to manage them. The activities guiding device management spell out the interconnectivity and the alignment of the procedure that guides the framework. The various activities can be used to pinpoint areas for mitigating the security threats by comparing the threats associated with each domain (e.g. technical, social, mobility) with the solutions to the threats as they relate to both individual and organization practices.

As presented in Figure 7.9, device acquisition has a direct relationship with the technical domain. Similarly, device monitoring has a focus on the social domain, while device maintenance has a focus on the mobility domain (Figure 7.9). However, device disposal has a direct link with device acquisition. It is an iterative process that goes back to device acquisition after device disposal (Figure 7.9). Furthermore, there are intermediate relationships such as validation, compliance, defunct and decommissioning. The intermediate relationship has a link with socio-technical, pervasive and e-commuting domains, except for defunct which has a direct link with device disposal. Both individual and organization need to be aware of the security threats and security solutions for all these domains and take proactive steps for device acquisition, device monitoring, device maintenance and device disposal as stated in sections 7.7.1, 7.7.2, 7.7.3 and 7.7.4 respectively. It is important to note that the interrelations among these domains as investigated in the study provide the synthesis guiding device management which leads to the security framework as shown in Figure 7.9. This approach gives both individual and organization the ability to distinguish threats in such a way that can easily be detected and mitigated without affecting other assets of the organization (NIST, 2018).



7.9 Summary

This chapter presented a 3-D security framework for BYOD-enabled banking institutions in Nigeria. The framework describes the link between individual and organization practices in exploring BYOD security threats and their security solutions under three major domains, namely technical, social and mobility. Wang et al. (2014) assert that owing to the type of transactions and sensitive information processed within the banking system, risk management is a critical aspect that must be addressed when developing a security framework. Similar empirical studies by Matinde (2015) and Bello et al. (2015) affirm that the magnitude of BYOD challenges will always intensify as long as business models continuously evolve. This necessitates the review of existing relevant security frameworks with a view to strengthening them for better performance. However, none of these security frameworks reviewed (section 2.6) have been able to sufficiently address the significance of individual and organization practices as they relate to BYOD security threats. Hence, based on the findings of this study, a security framework comprising threats, solutions and the activities guiding device management for both individual and organization practices was presented in Figure 7.9. The framework spelt out the interconnectivity between the three major domains (technical, social and mobility) as well as the processes and their sustainability to ensure optimal delivery in meeting the sector's needs. It concludes by sending the developed security framework (Figure 7.9) for evaluation. The reason for sending out the security framework for evaluation is to determine whether it is feasible, implementable and whether it meets the expected security requirements.

This is important because evaluating a security framework offers significant insight regarding the functionality of the system which can result in a measure of confidence that the system meets the required expectations (Asheri et al., 2012). Hence, the outcome of the evaluation and the interpretation were used to answer the fifth research question (chapter 8).

CHAPTER 8: EVALUATION OF THREE-DIMENSIONAL (3-D) SECURITY FRAMEWORK FOR BYOD ENABLED BANKING INSTITUTIONS IN NIGERIA

8.1 Introduction

Evaluating a security framework is a process by means of which the evidence for assurance is identified, assembled and analyzed against criteria for security functionality and guarantee level (Asheri, Louise & Stewart, 2012). In other words, it is a process by means of which evidence that a particular system meets its security requirements is presented. This understanding can result in a measure of confidence that shows how well the system meets particular security targets or objectives (Asheri et al., 2012). Hence, to evaluate the confidence or assurance level that the 3-D security framework for BYOD-enabled banking institutions in Nigeria meets the security functionality, the unified perceptions of the participating banks' executives (i.e. ICT department personnel and executive managers) and the academic experts in information security were sought. The evaluation results help to answer the fifth research question which is stated as follows:

How do the recommended security measures help to mitigate the security threats?

The evaluation follows the mixed-methods research design. The quantitative and qualitative data components are used to provide a complete understanding of the realization and sustainability of the security framework. As explained in the research methodology (chapter 4), twelve participants were involved in the evaluation. This includes eight executive management staff from the four participating banks (i.e. one ICT department person and one executive manager each from the four banks) and four academic experts in information security from four different universities (i.e. one academic staff member each). Closed and open-ended questions were employed, and a questionnaire was distributed to the twelve participants via e-mail. The twelve questionnaires were all completed and returned. The success recorded in retrieving the questionnaires may be attributed to the small number of participants which made the follow up easier. The evaluation analysis is presented in two sections – descriptive analysis and thematic analysis.

8.2 Descriptive analysis

A descriptive analysis was carried out on the security framework's appropriateness, adequacy, feasibility, flexibility and intention to use. The results of the analysis are presented as follows:

8.2.1 Appropriateness

Participants were asked to assess the criteria presented in item 1 of the evaluation questions (Appendix E) to determine the appropriateness of the security framework. The outcome of the assessment is illustrated in Figures 8.1 to 8.3.

Figure 8.1 show that 16.7 per cent of the participants strongly agreed, while 33.3 per cent agreed and 41.7 per cent slightly agreed that the security framework aligned with the policies and strategies of the bank. Contrariwise, 8.3 per cent of the participants slightly disagreed with this statement. This result has found out that the vast majority (91.7 per cent) of the participants believed that the security framework aligned with the policies and strategies of the bank. According to Vanderlinde, Dexter and Van Braak (2012), policies are shaped by coalescing the various requirement of top managers, IT executives and key users within the organization. It is from the combination of executive managers' and IT executives' perspectives in evaluating the information systems framework that the appropriateness of the framework emerges (Torres, Sarriegi, Santos & Serrano, 2006).

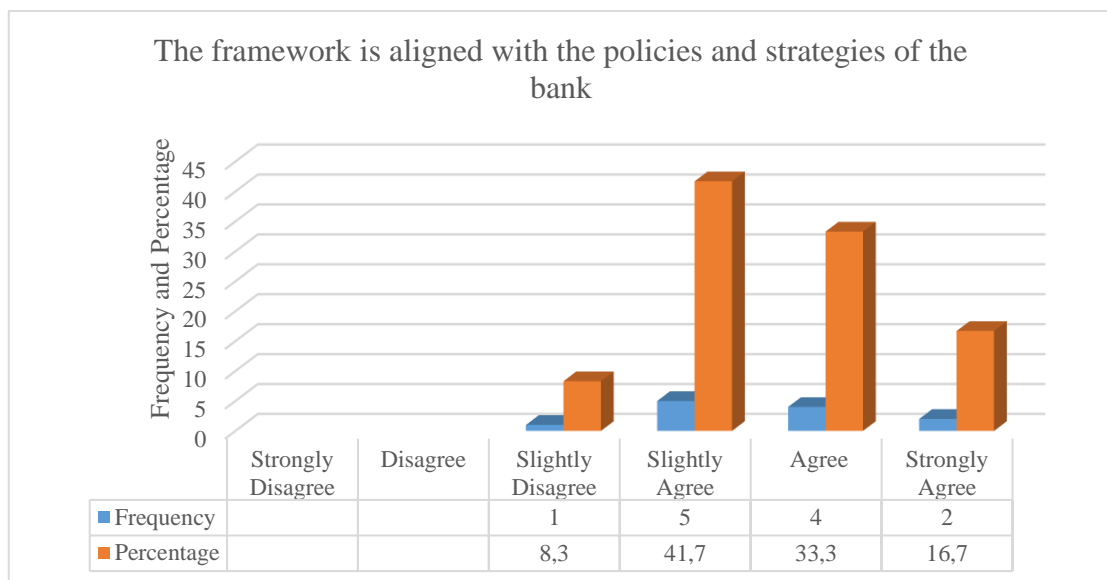


Figure 8.1: The framework is aligned with the policies and strategies of the bank

Again, the results in Figure 8.2 shows that 25 per cent of the study participants strongly agreed, while 41.7 per cent agreed and 33.3 per cent slightly agree that the security framework enhances the effectiveness of the bank’s data security. This result shows that all of the participants (100 per cent) believed that the security framework enhances the effectiveness of the bank’s data security. Supporting this finding, Cameron and Whetten (2013) claim that the primary task for any investigator of effectiveness lies in determining whether it boosts the organization’s information security system. Effective information security focuses on identifying the essential success factors for information security implementation which include how organizations could align information security system with business goals, security strategies, policies’ enforcement and investments (Torres et al., 2006).

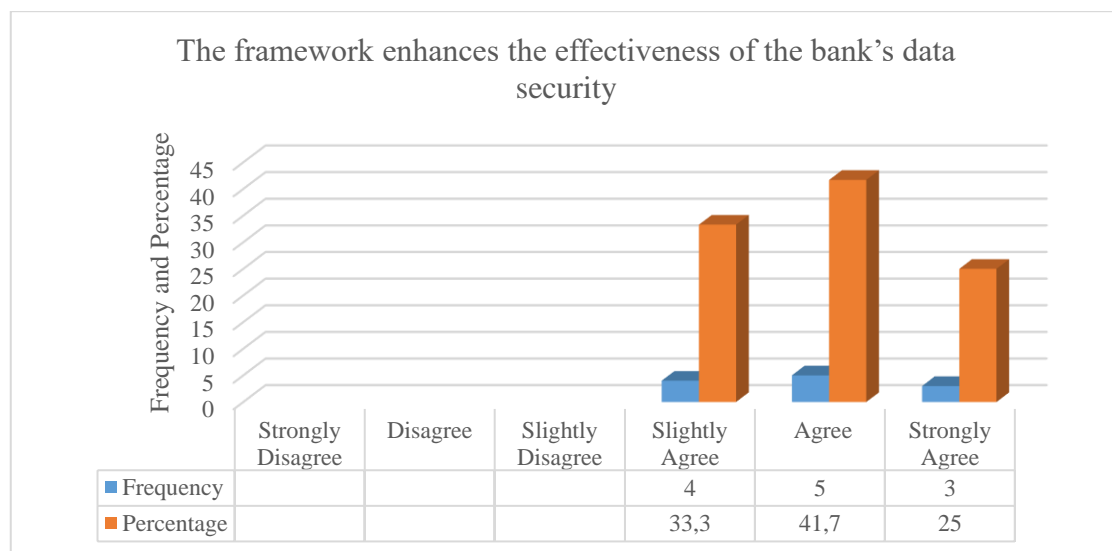


Figure 8.2: The framework enhances the effectiveness of the bank’s data security

Likewise, Figure 8.3. clearly shows that 16.7 per cent of the participants strongly agreed that the security framework could contribute towards the efficiency of the bank operations while 58.3 per cent and 16.7 per cent agreed and slightly agreed respectively. Conversely 8.3 per cent slightly disagreed. This result shows that the vast majority (91.7 per cent) of the participants believed that the security framework could contribute towards the efficiency of the bank operations. This implies that the efficiency of the security framework is credible. Kamatchi and Modi (2016) assert that the efficiency of a security system lies in its ability to be utilized with minimal maintenance. Furthermore, a security framework is considered efficient if it can identify and minimize risk when handling information (Torres et al., 2006).

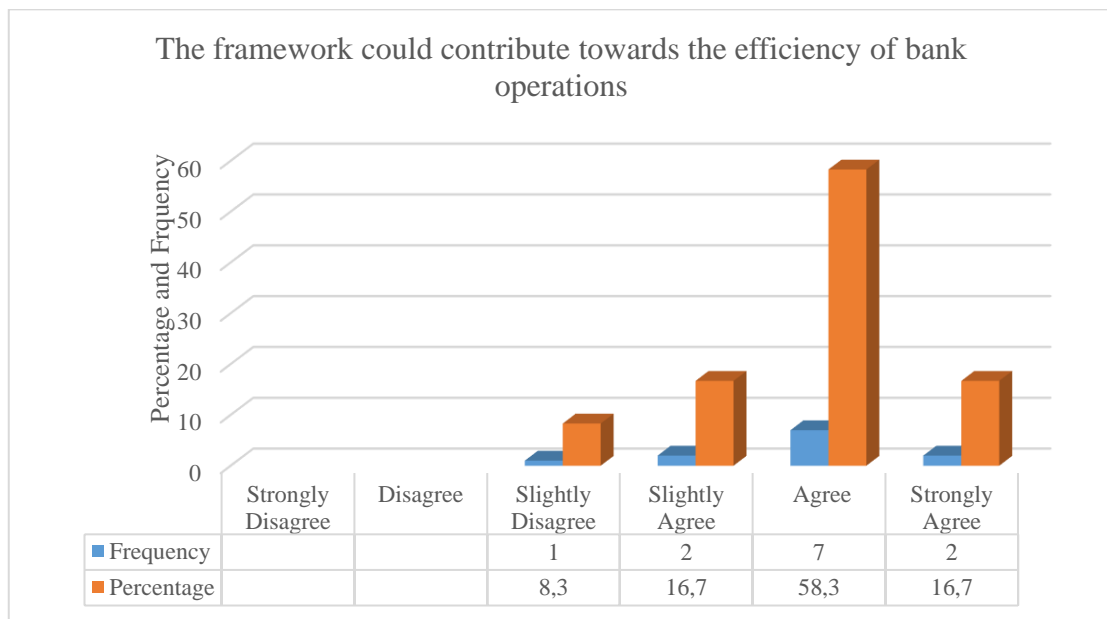


Figure 8.3: The framework could contribute towards the efficiency of the bank operations

8.2.2 Adequacy

Participants were asked to assess the criteria presented in item 2 of the evaluation questions (Appendix E) to determine the adequacy of the security framework. The outcome of the assessment is illustrated in Figures 8.4 to 8.6.

Figure 8.4 reveal that 16.7 per cent of the participants strongly agreed, while 66.7 per cent agreed and 8.3 per cent slightly agreed that the security framework could address all the technical threats identified. The remaining 8.3 per cent of the participants slightly disagreed with this statement. This clearly shows that majority of the participants (91.7 per cent) believed the security framework could address all the technical threats identified. This implies that the confidentiality of the banks' information is protected against any technical security threats as identified in the data analysis chapter (i.e. chapter 5). In support of this finding, Pratt Jr and Jones (2013) assert that it is important that the technical security threats are addressed because by their very nature, they can be harmful if the right security measures are not put in place to the extent that they can be exposed to other security threats that require separate security management.

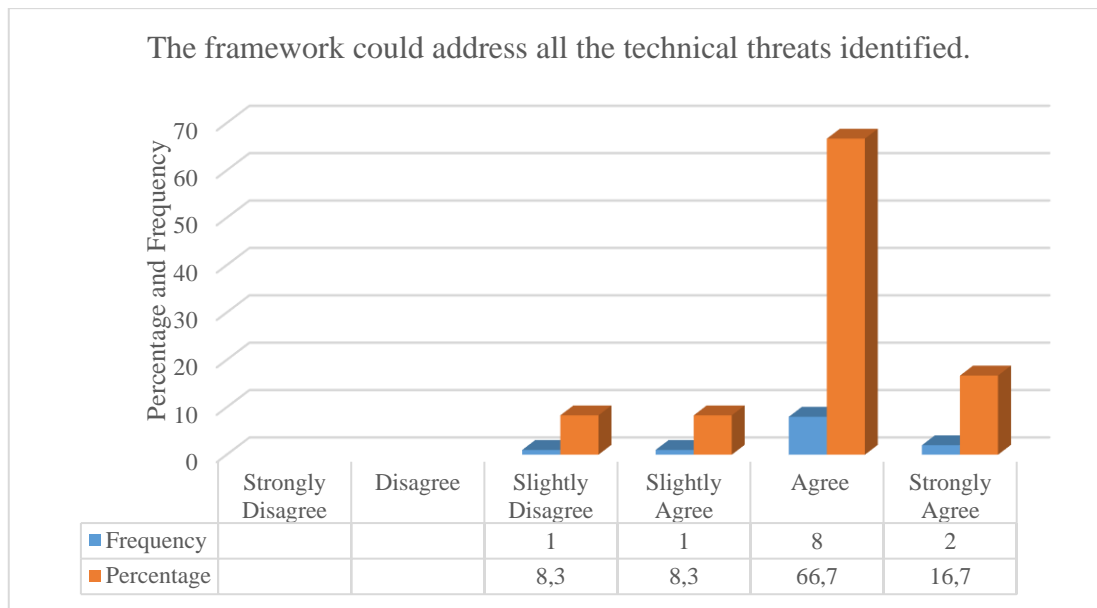


Figure 8.4: The framework could address all the technical threats identified

Again, the results in Figure 8.5 show that 16.7 per cent of the participants strongly agree, while 33.3 per cent agree and 33.3 per cent slightly agree that the security framework could address all the social threats identified. Conversely, the remaining 16.7 per cent of the participants slightly disagreed with this statement. This result has found that the vast majority (83.3 per cent) of the participants believed that the security framework could address all the social threats identified. These social security threats are threats from employees' attitudes and organizations' norms, principles, policies and values as revealed in the data analysis chapter (i.e. chapter 5). Bello et al. (2015) opine that organizations should recognise the influence of these security threats and address them accordingly.

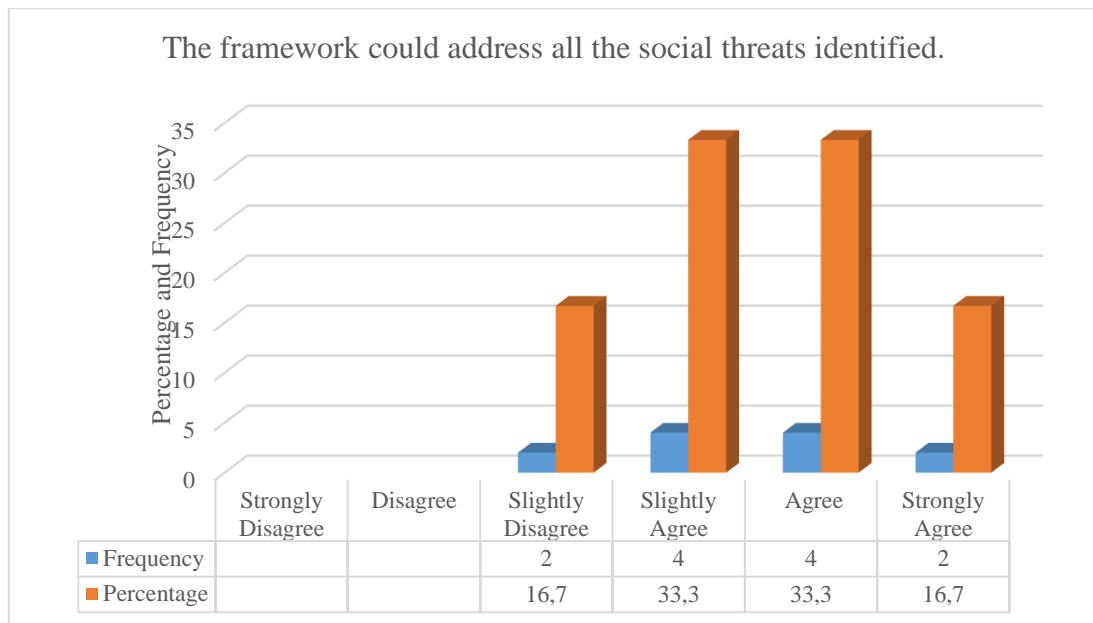


Figure 8.5: The framework could address all the social threats identified

Similarly, Figure 8.6 reveals that 16.7 per cent of the study participants strongly agreed, while 66.7 per cent agreed that the security framework could address all the mobility threats identified. Contrariwise, 16.7 per cent slightly disagreed with the statement. This result has found that a vast majority (83.3 per cent) of the participants believed that the security framework could address all the mobility threats identified. It is important that organizations integrate a security framework into management systems that substantially improves their ability to respond to various information security threats (Astani et al., 2013). In addition, Wolden, Valverde and Talla (2015) maintain that vulnerabilities can be dealt with through security measures that can be created via a security framework.

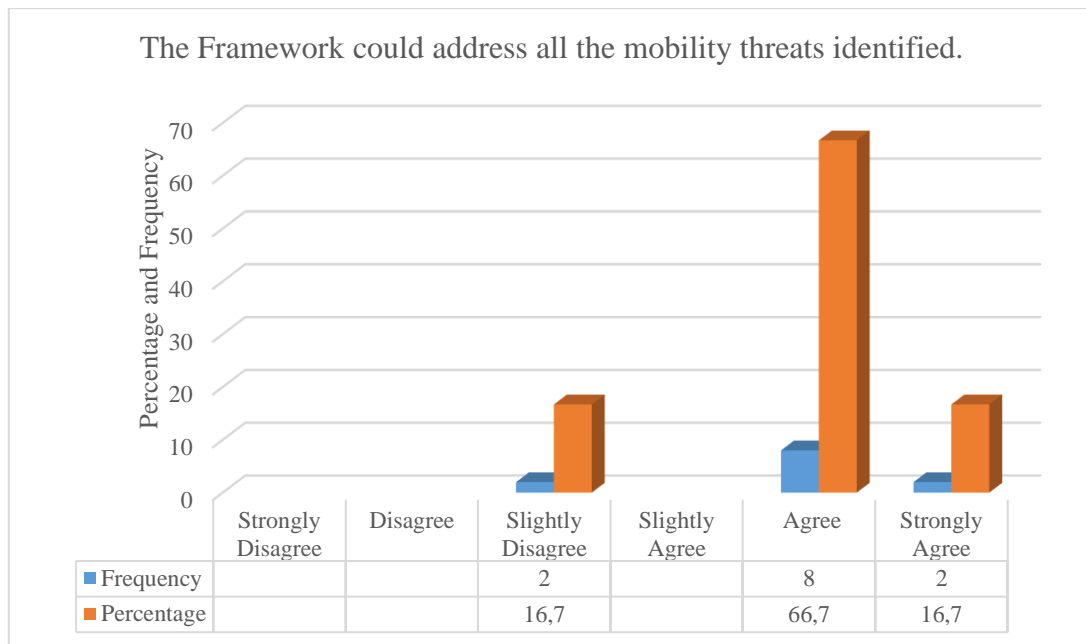


Figure 8.6: The framework could address all the mobility threats identified

8.2.3 Feasibility

Participants were asked to assess the criteria presented in item 3 of the evaluation questions (Appendix E) to determine the feasibility of the security framework. The outcome of the assessment is illustrated in Figures 8.7 to 8.9.

Figure 8.7 reveals that 25 per cent of the study participants strongly agreed, while 33.3 per cent agreed and 25 per cent slightly agree that the security framework could be cost effective. However, 8.3 per cent slightly disagree and 8.3 disagree with the statement. This clearly show that a vast majority (83.3 per cent) of the participants affirm that the security framework could be cost effective. This implies that the security framework could be implemented with minimal cost. Asheri et al. (2012) affirm that the three most cited measures of information system performance are cost, budget performance and return on investment. The cost of maintenance of an infrastructure asset can be determined by how well it was designed, its fitness for purpose, the quality of construction, materials specified and used and not just by the capacity, nature and size of that infrastructure (Su, 2016). However, 16.6 per cent of the participants disagreed that the security framework could be cost effective. This is as a result of budget constraints which were identified in section 5.5.2.2. Hence there is a need to consider the availability of funds. Hong (2013) maintains that the feasibility of a system or business could be

determined by forecasting and analysing the resources and cash-flows as well as other financial tests.

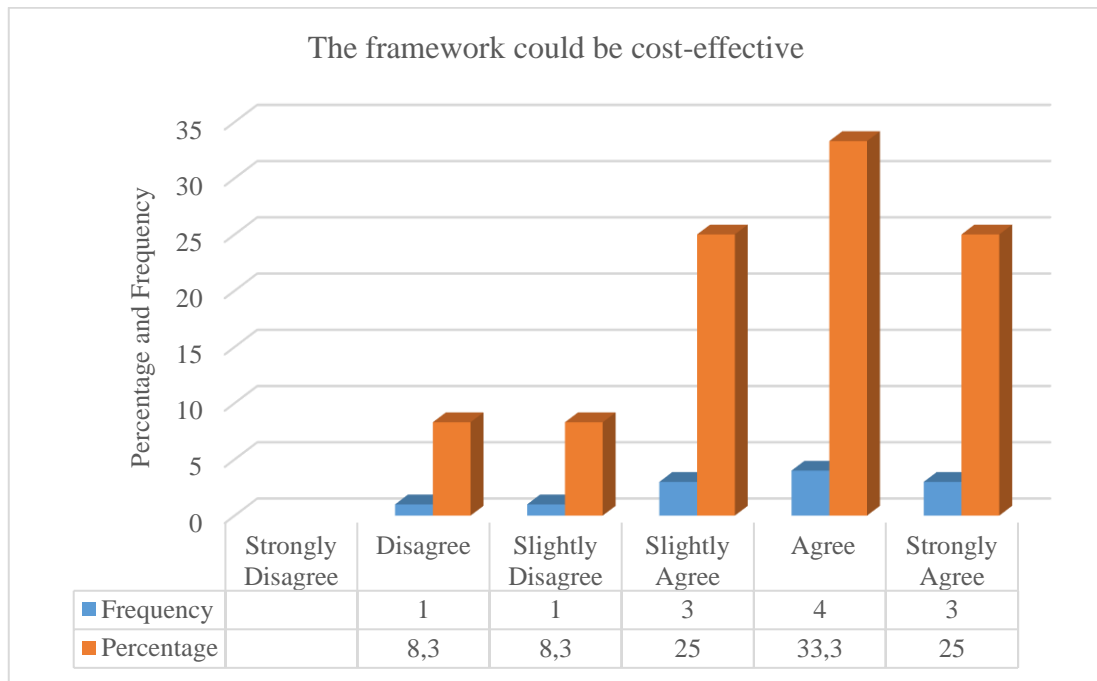


Figure 8.7: The framework could be cost-effective

Again, the results in Figure 8.8 show that 33.3 per cent of the study participants strongly agreed, while 33.3 per cent agreed and 16.7 per cent slightly agree that the security framework could be implemented within a short period of time. However, 16.7 per cent disagreed with the statement. This infers that a vast majority (83.3 per cent) of the participants confirm that the security framework could be implemented within a short period of time. In addition, this implies that the organization has the necessary infrastructure to implement the security framework within a short time frame. Supporting this finding, Cameron and Whetten (2013) affirm that timeline feasibility is important to determine whether the organization can implement the framework within a specified period. In addition, Hong (2013) emphasizes the need for an organization to have the required resources and capabilities to implement the framework within a time frame. However, 16.7 per cent of the participants disagreed that the security framework could be implemented within a short period of time. This is also attributed to budget constraints (section 5.5.2.2). Hence it is noted as one of the limitations of this study.

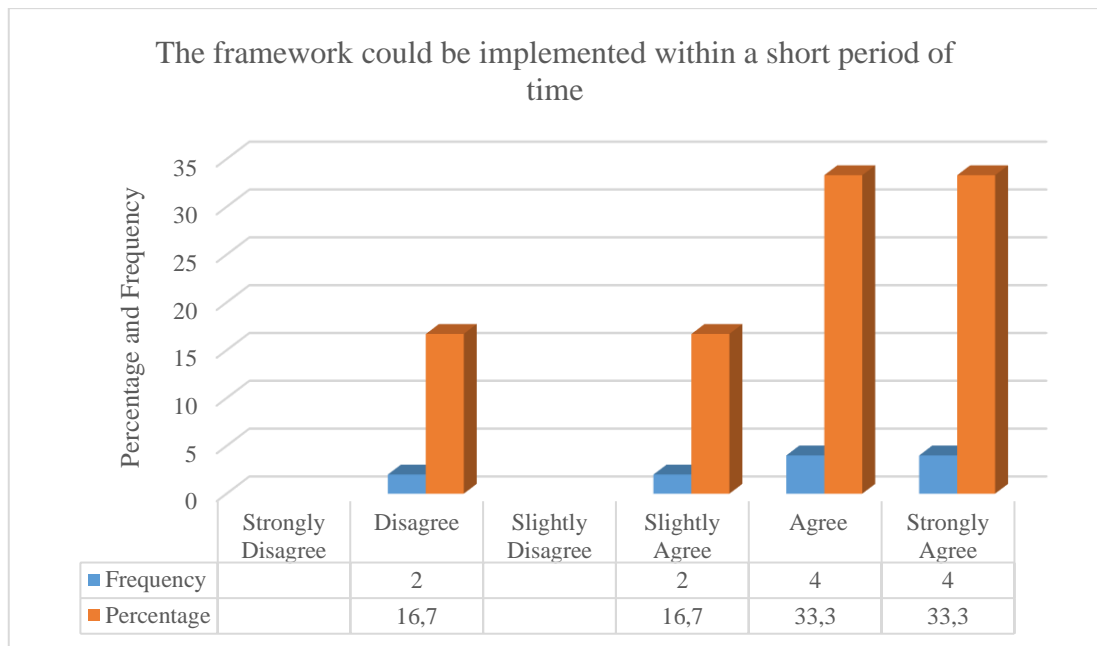


Figure 8.8: The framework could be implemented within a short period of time

Likewise, Figure 8.9 shows that 8.3 per cent of the study participants strongly agreed, while 50 per cent agreed and 16.7 per cent slightly agree that the security framework could be implemented with the available resources of the bank. Contrariwise, 8.3 per cent slightly disagree and 16.7 per cent disagreed with the statement. This implies that a vast majority (75 per cent) of the participants believed that the security could be implemented with the available resources of the bank. Supporting this finding, Vateva-Gurova, Luna, Pellegrino and Suri (2014) assert that the feasibility of implementing a security framework depends on the organization's available resources and capabilities to support the process of implementation. However, 25 per cent of the participants did not believe that the security framework could be implemented with the available resources of the bank. This implies that the available resources at hand are insufficient for the implementation of the framework. This is also considered as one of the limitations of this study as the resources available for each bank is not the same for framework implementation.

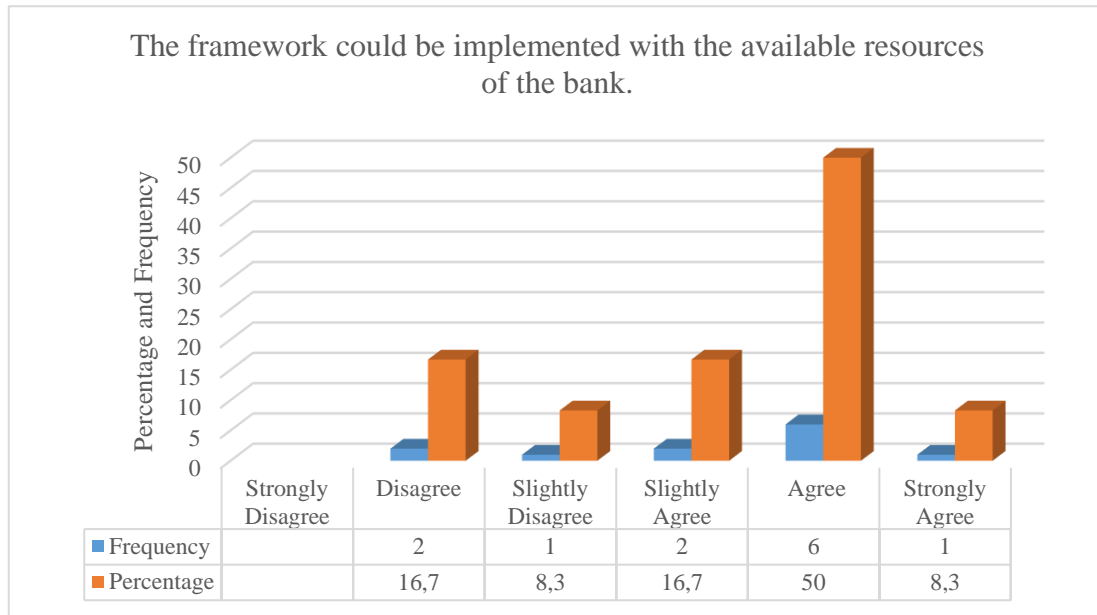


Figure 8.9: The framework could be implemented with the available resources of the bank

8.2.4 Flexibility

Participants were asked to assess the criteria presented in item 4 of the evaluation questions (Appendix E) to determine the flexibility of the security framework. The outcome of the assessment is illustrated in Figures 8.10 to 8.13.

Figure 8.10 reveals that 8.3 per cent of the study participants strongly agreed, while 41.7 per cent agreed and 25 per cent slightly agree that the security framework could be easily adopted with changing policies. Conversely, 25 per cent slightly disagree with the statement. This infers that a vast majority (75 per cent) of the participants confirm that the security framework could be easily adopted with changing policies. According to Ifinedo (2012), change is a major part of our lives, whether it is change in social policies or technologies policies. “Policy change occurs through interactions between wide external changes and the success of the ideas in the coalitions, which may cause actors in the advocacy coalition to shift coalitions” (Cerna, 2013). However, 25 per cent of the participants disagreed somewhat that the security framework could be adopted with changing policies. This is owing to inconsistency in terms of ICT policy across the bank (Downer & Bhattacharya, 2015). Hence, an ICT policy guideline is required for each bank: this was not considered in this research.

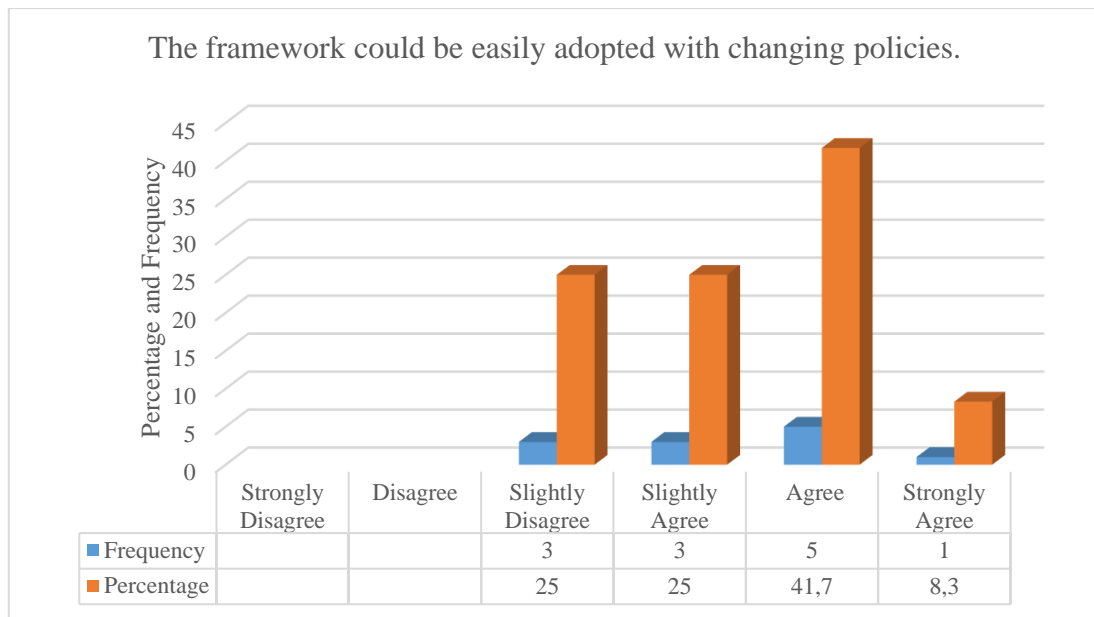


Figure 8.10: The framework could be easily adopted with changing policies

Again, the results in Figure 8.11 reveal that 8.3 per cent of the study participants strongly agreed, while 58.3 per cent agreed and 33.3 per cent slightly agree that the security framework could be adopted for mitigating security threats within different branches of the bank. This shows that 100 per cent of the participants opine that the security framework could be adopted for mitigating security threats within different branches of the bank. Vateva-Gurova et al. (2014) maintain that a business must have the capacity to withstand tempestuous occasions and to ride out sudden hard blows. This implies that the business ought to be sufficiently adaptable to deal with both the unforeseen dangers and opportunities posed by an indeterminate future and unstable environment.

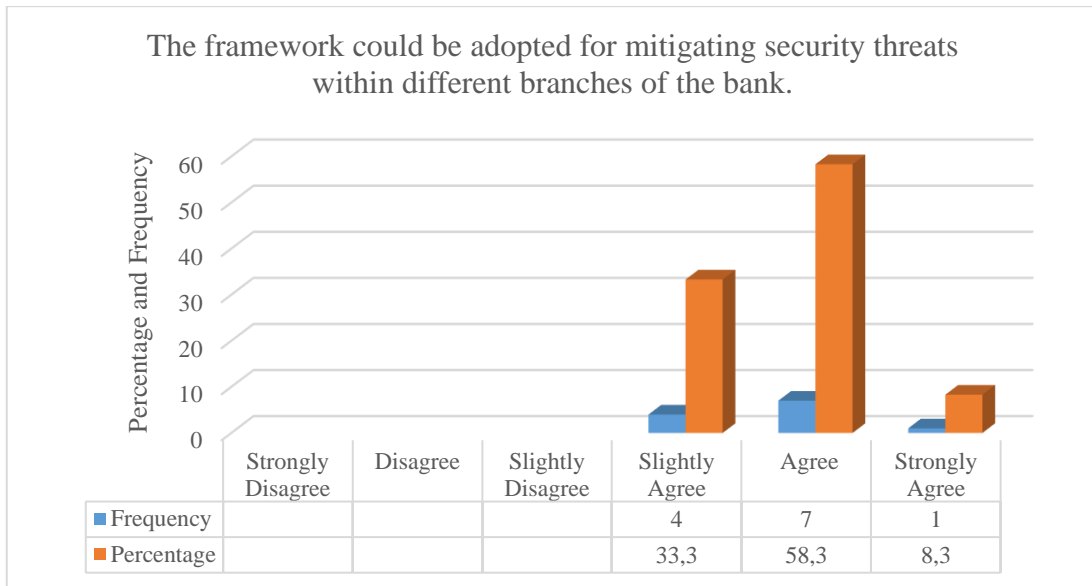


Figure 8.11: The framework could be adopted for mitigating security threats within different branches of the bank

Similarly, Figure 8.12 shows that 8.3 per cent of the study participants strongly agreed, while 25 per cent agreed and 41.7 per cent slightly agree that the security framework could be adopted for mitigating security threats across different banks. However, 16.7 per cent slightly disagree and 8.3 per cent disagree with the statement. This infers that a vast majority of the participants (75 per cent) believed that the security framework could be adopted for mitigating security threats across different banks. This finding is consistent with the literature that indicates that the more adaptable companies become, the better they can respond to security risks ranging across companies (Cameron & Whetten, 2013). However, the remaining 25 per cent of the participants do not believe that the security framework could be adopted for mitigating security threats across different banks. This can also be attributed to inconsistency in terms of ICT policy across the banks (Downer & Bhattacharya, 2015). Hence an ICT policy guideline is required across the banks, a factor which was not considered in this study: hence it is noted for recommendation.

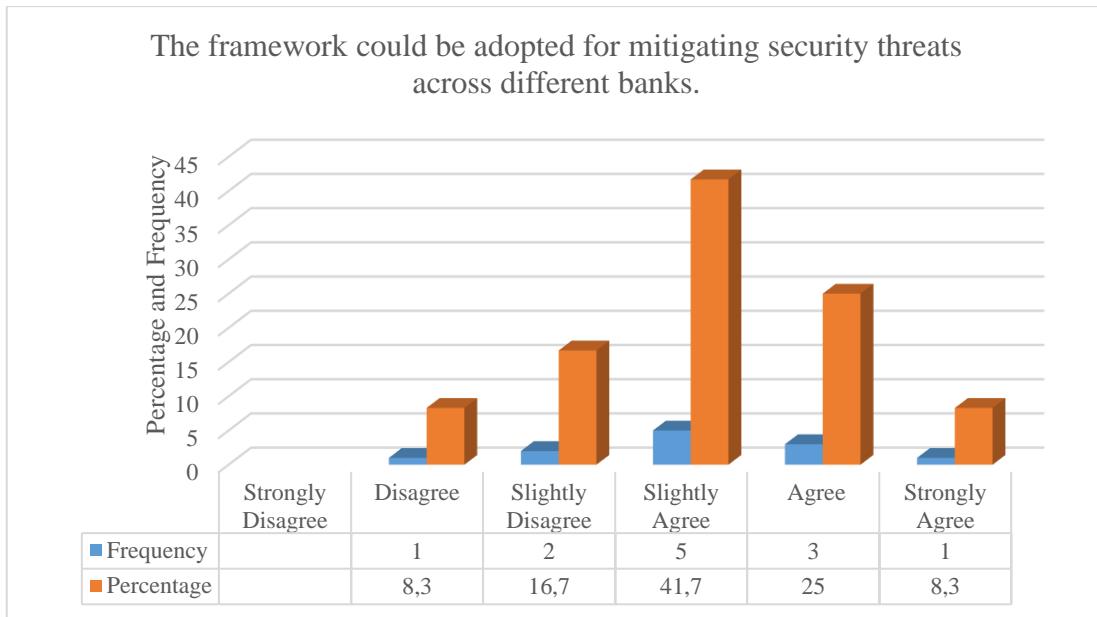


Figure 8.12: The framework could be adopted for mitigating security threats across different banks

8.2.5 Intention to use

Participants were asked to assess the criteria presented in item 5 of the evaluation questions (Appendix E) to determine the intention to use the security framework. The outcome of the assessment is presented in Figures 8.13 to 8.15.

Figure 8.13 reveals that 91.7 per cent of the participants are willing to implement the framework as it is. This implies that participants are happy and comfortable with implementing the security framework. The findings may also be consistent with the literature, which indicated that organization are more comfortable with implementing a security framework if it addresses the security concerns of the organization (Wolden et al., 2015).

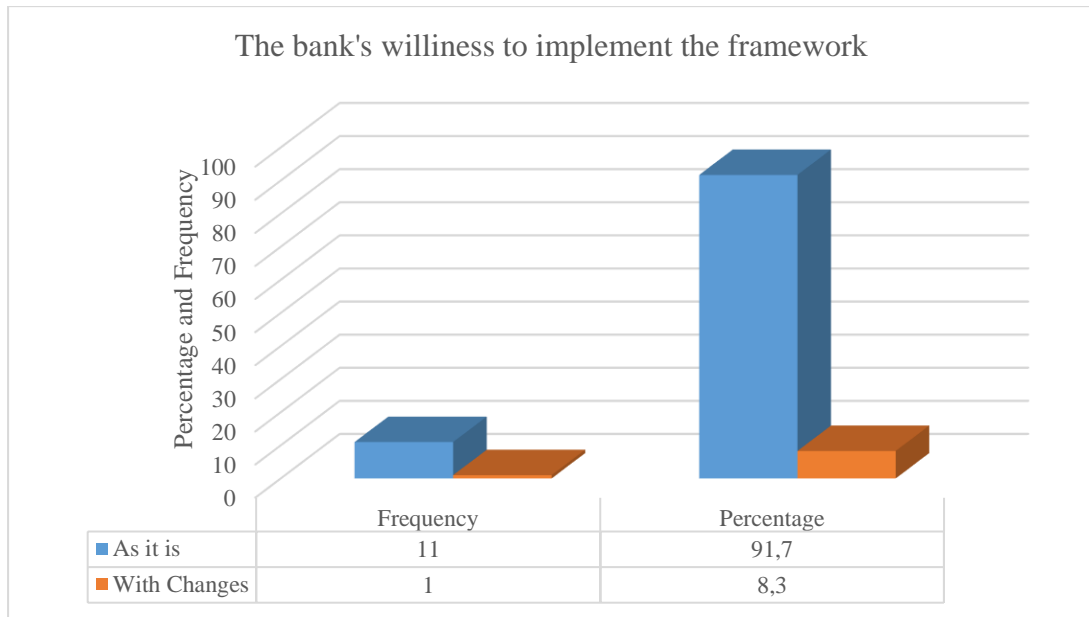


Figure 8.13: The bank's willingness to implement the framework

Again, the results in Figure 8.14 reveal that 75 per cent of the participants are willing to adopt the security framework immediately. This implies that participants are satisfied with adopting the security framework straight away. Cameron and Whetten (2013) claim that organizations that adopt a framework will probably be a function of the framework's flexibility, and efficiency. This suggests that acceptability in the organization is innate in these characteristics. However, 25 per cent of the participants were of the opinion that adopting the framework should take place in the future. This may also be attributed to budget constraints as identified in section 5.5.2.2.

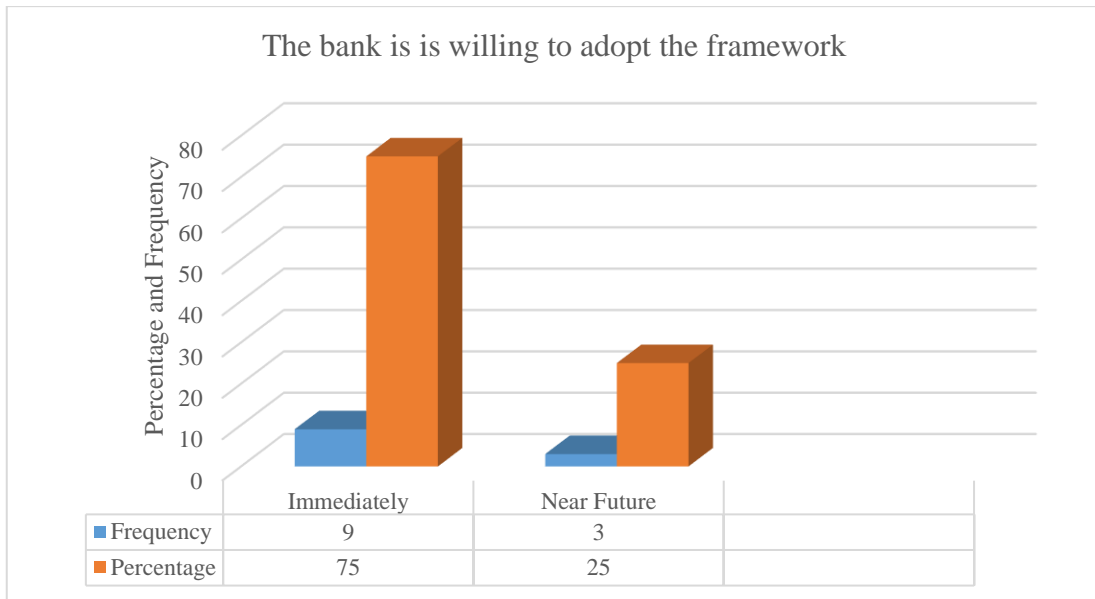


Figure 8.14: The bank willingness to adopt the framework

Similarly, Figure 8.15 shows that 91.7 per cent of the participants affirmed that the use of the security framework by employees could be easy. According to Cameron (2014), since a framework is result driven, it empowers versatility. It is this flexibility that enables the framework to be easily used by organizations (Stouffer et al., 2008).

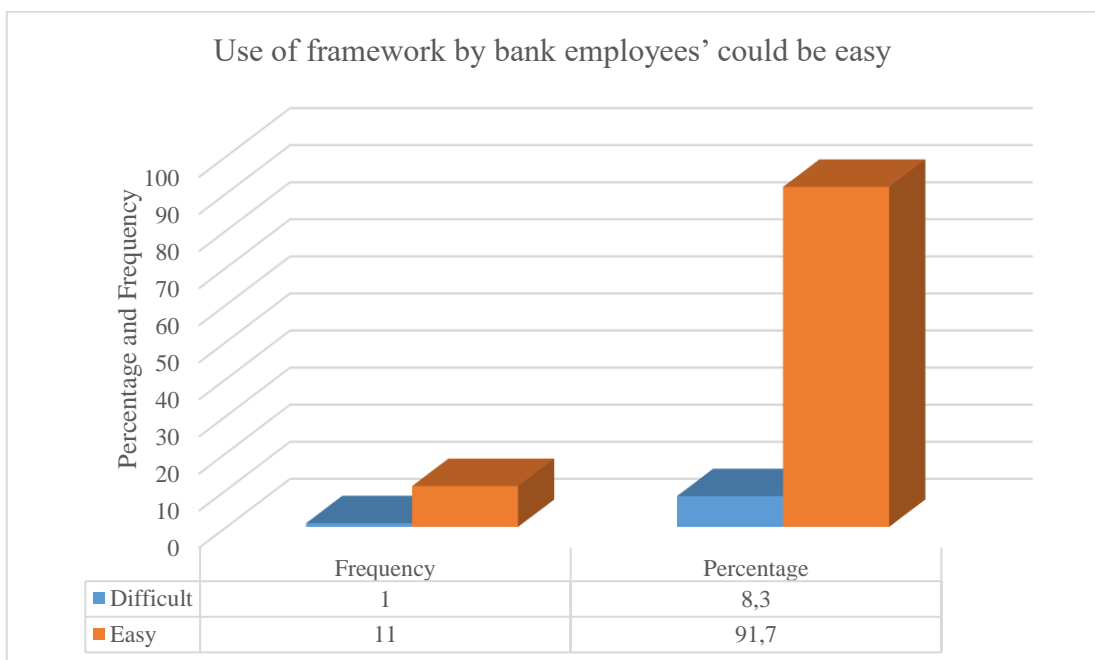


Figure 8.15: Use of framework by bank employees' could be easy

This section of the study presents the closed-ended data analysis obtained from the evaluation. The quantitative data was gathered via responses from the closed-ended

questions to validate the security framework using Likert-scale measures. The outcome of the analysis affirms the security framework validity. The next section presents the qualitative data that was obtained from the open-ended questions. The open-ended questions were included in order to obtain detailed information on any data that maybe missed if only closed-ended questions were used. The result is analysed using thematic analysis.

8.3 Thematic analysis

This section presents the analysis of the open-ended data collected at the evaluation phase. The data in this phase was coded and analysed using thematic analysis. A thematic analysis technique was considered to be suitable because it enables researchers to determine the relationship between various concepts and relate them alongside other replicated data (Vaismoradi et al., 2013). The themes that emerged in the open-ended questions were subsequently classified into three (3) major categories, namely recommendation for threats and solutions that are not considered in the framework, implementation comments and general comments. This is illustrated in Table 8.1.

Table: 8.1: Categories and themes that emerged in the open-ended questions

Categories	Major Themes
1. Recommendation for threats and solutions that are not considered in the framework	1. Training 2. Credit card encryption
2. Implementation comments	1. Possibility for changes at the implementation stage 2. Budget constraint
3. General Comments	1. Acceptability of the security framework

8.3.1 Recommendations for threats and solutions not considered in the framework

Participants gave recommendations for solutions that were not considered in the security framework. The following threats and solutions were recommended:

Training

Two participants recommended training as a solution that was not covered in the security framework. The statement below is a comment from one participant:

“Training should be included in the security framework”

Another participant remarked:

“Provide more training and awareness programmes piloting before roll out”

This implies that the participants identified training as a vital need to be considered for a successful security framework. This finding is consistent with those of other studies that suggest the need for ICT programmes and formal training for employees as key organisational aspects to provide knowledge of security awareness (Bulgurcu et al., 2010). According to Downer and Bhattacharya (2015), the primary goal of organizations in conducting information security training is to disseminate adequate knowledge which will eventually change individuals’ attitudes towards information security. Shaw, Chen, Harris and Huang (2009) maintain that the major reason for training is to ensure awareness of risks and convey how to maintain good practices.

However, it is important to note that training was considered in the previous security framework, but it was made implicit (Figure 7.9). Hence, in order to make a better presentation, the security framework is revised to make ‘training’ explicit (Figure 8.16). In addition, it can be recalled (Figure 7.9) that knowledge and consciousness were solutions recommended for organizations and individuals respectively under the high risk region. Hence, it is important to note that training encompasses both knowledge and security consciousness. In other words, the training will be used to provide the relevant knowledge for organization as well as creating a security consciousness for employees. According to Keys (2013), organizations should endeavour to be updated with the latest scientific knowledge on security awareness by attending information security training. This training can be in form of workshops, conferences or seminars (Kearns, 2016).

Similarly, individuals should be trained on how to be more security conscious when using their mobile devices (Keys, 2013). Such training may include how to run regular updates, regular backups, avoid installing unnecessary applications, avoid sharing organizations’ confidential information especially over unprotected networks, avoid jailbreaking and have good physical control of mobile devices (Kearns, 2016). Hence, while incorporating these changes in the high risk region, the awareness domain (Figure 7.9) was also revised

to obscure interaction domain (Figure 8.16). This is because the interaction of the three domains (i.e. technical, social and mobility) makes it the most vulnerable to security flaws which can be obscure in nature. Apelbaum (2007) argues that obscure interaction may have theoretical or actual security vulnerabilities; however, its flaws are not visible, hence it gives room for successful attack. Thus, there is a need for training to create security awareness for both organization and individual.

Furthermore, it is important to note that training can be a meaningful driver of an effective and strong cybersecurity culture that helps the organization to actively respond to new threats and technologies as well as changing their goals, processes and structures (Enisa, 2017). According to Abawajy (2014), building a strong cybersecurity culture through consistent training, awareness and promotion will ensure that employees are well informed of cybersecurity policies thus improving resilience against all cyber threats. Alfawaz (2010) suggests that organization should draft out cyber security strategy and policy using guidelines from other cyber security documentations or standards that is informed by best practices. This will help organizations to regularly measure and evaluate employees' opinions on cybersecurity, which can heighten awareness and enhance culture (Enisa, 2017). "This approach moves employees from risk factor to security advocate, and employees may even proactively protect the business as they become more cognizant of cybersecurity practices" (Alfawaz, 2010).

Credit card encryption

Similarly, one participant recommends credit card encryption as a solution that was not covered in the framework. The statement below is a suggestion from the participant, and it reads:

"Credit card numbers should be encrypted with one master card"

From the excerpt above, it can be deduced that the participant expected the security framework to capture smart cards, which include credit and debits cards. However, it can be recalled from the threat identification (section 5.4.2.1) that a descriptive analysis was carried out on the categorized four types of mobile devices (smartphones, laptops, tablets and other devices). The 'other devices' options give the respondents ample opportunity to specify other types of mobile devices used that may have been omitted (e.g. smart

cards). However, an insignificant number of respondents specified other types of mobile devices. Hence, the 3-D security framework for BYOD-enabled banking institutions in Nigeria was based on the threat identification findings where a significant number of respondents specified smartphones, laptops and tablets. This implies that the security framework does not capture smart cards which include credit and debit cards. However, this is one of the limitations of this security framework and it is noted for recommendation for future research.

8.3.3 Implementation comments

Participants made general remarks regarding the implementation of the security framework. These are presented as follows:

Possibility for changes at implementation stage

Two participants remarked that the framework is subject to change at the implementation stage. The statement below is a response from one of the participants:

“To the best of my knowledge, the basic threats have been identified and solutions proffered. Other possible issues will be tackled at the implementation stage”
(Participant 16).

Another participant notes:

“I think the framework is well detailed but there is possibility for changes at the implementation stage”.

From the excerpt above, it can be deduced that the participant believed that the framework is well detailed to tackle the security threats and if peradventure there is any issue at the implementation stage it can easily be tackled to incorporate any changes.

Budget constraint

Two out of the twelve participants maintain the willingness to use the security framework in the near future is due to financial constraints. The statement below is a response from one of the participants:

“The framework can be implemented in future due to budgetary reasons”
(Participant 11).

Again, another participant notes:

“The framework is subject to management approval for implementation which may be delayed due to budgetary reasons” (Participant 2).

The foregoing suggests that only two participants foresee financial constraint as a challenge to implement the security framework immediately. This result corroborates the ideas of Su (2016) which asserts that for an organization to have effective IT infrastructure, adequate budget must be made available by the organization to update and maintain the IT infrastructure. However, this is one of the limitations of this security framework and it is noted for recommendation for executive managers.

8.3.4 General comments

Participants made general remarks regarding the acceptability of the security framework. These were presented as follows:

Acceptability of the security framework

Seven participants commented via e-mail that they are satisfied with the security framework as it addresses the important areas of the security threat. The responses of the participants are stated as follows:

“Great work! I endorsed the framework as a realistic and pragmatic intervention that can secure banks in general from any security threats”
(Participant 2).

“We believe this framework will go a long way to address any threats that jeopardize our operation as a bank”. (Participant 8).

“We have evaluated your security framework and we are satisfied that it captures the essential aspects of security threats”. (Participant 11).

“The framework will accelerate the knowledge process on BYOD security”.
(Participant 13).

“I can say that it is a very comprehensive framework that has been well researched and conceptually sound, and which encompasses several dimensions of inquiry” (Participant 14).

“The security framework gives a clearer indication on the security awareness for BYODs” (Participant 15).

“This security framework is pivotal to maintain data security while employees use their mobile devices” (Participant 16).

It can be inferred from the above statements that participants are delighted with the security framework. These results validate the concepts of Stouffer et al. (2008) who declared that having a security framework in a business enterprise promotes greater sensitivity to whatever constitutes a security threat to the enterprise's assets, improves trust in relationships among individuals and groups and supports greater consistency in the standards and quality of products. This implies that the acceptability of the security framework is positive. Thus, the main objective of this chapter, which is to validate the 3-D security framework for BYOD-enabled banking institutions in Nigeria, has been met.

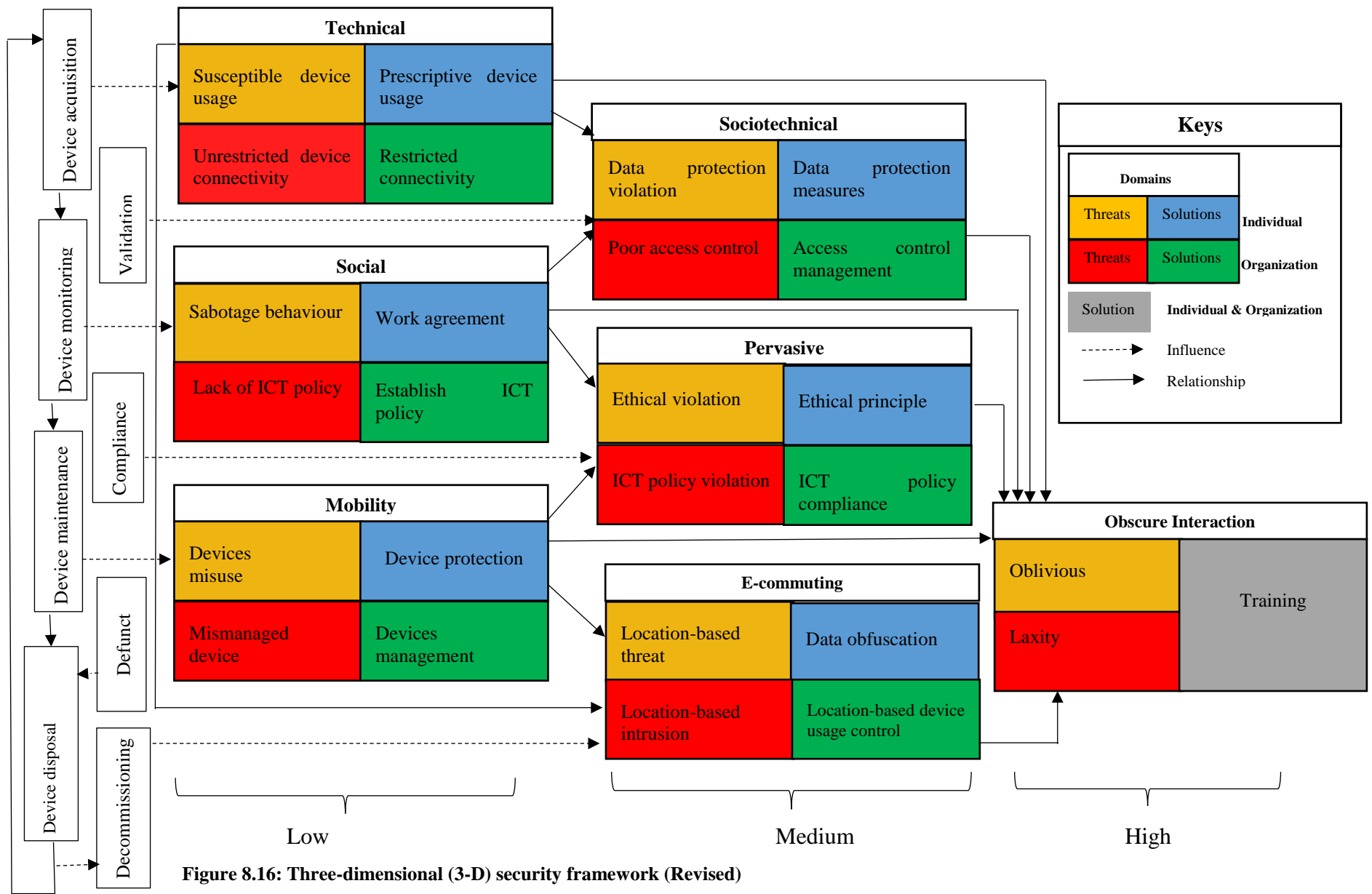


Figure 8.16: Three-dimensional (3-D) security framework (Revised)

8.4 Summary

This chapter presented the empirical findings obtained from the analysis of quantitative and qualitative data that evaluates the 3-D security framework for BYOD-enabled banking institutions in Nigeria. The quantitative results indicate the level of acceptance of the security framework which largely depends on the framework's appropriateness, adequacy, feasibility, flexibility and intention to use. These findings are fully supported by the qualitative data where themes such as training and acceptability of framework also emerged. This indicates that training and acceptability of the framework also account for the credibility of the security framework. However, it is important to note that training was implicit in the previous framework (Figure 7.9) but has now been made explicit based on the evaluation responses in the revised framework (Figure 8.16).

In addition, the framework was endorsed as a realistic and pragmatic intervention that can secure Nigerian banks in general from any security threats. The findings may also be consistent with the literature, which indicated that organizations are more comfortable to implement a security framework if it addresses the security concerns of the organization (National Institute of Standards Technology, 2014). This justifies the credibility and acceptability of the 3-D security framework for BYOD-enabled banking institutions in Nigeria.

The next chapter presents the summary of the study. This is followed by the contribution of the thesis to the body of knowledge, the limitations of the study and recommendations for further study. Lastly, the research conclusion is drawn.

CHAPTER 9: SUMMARY OF FINDINGS, DISCUSSIONS AND RECOMMENDATIONS

9.1 Introduction

This chapter presents a summary of the study and its major findings. The chapter then discusses the contribution of the study to the body of knowledge. The limitations of the study and some useful recommendations on the way forward also form part of the chapter.

It is important to note that the essence of the study was to develop a security framework that will address BYOD security threats in the Nigerian banking sector. In order to develop this security framework, ways of addressing BYOD security threats were explored. The literature reviews provided information regarding BYOD security threats as well as ways to tackle the security threats, particularly ways in which other researchers have tackled similar security threats. Similarly, the threat identification findings (chapter five) from the study explain the link between individual and organization practices in exploring BYOD security threats under three major domains, namely technical, social and mobility. In addition, the influence of these security threats on the Nigerian banking sector also emerged from the threat identification findings. These findings were used in the development of a security framework with each of the domains having a specific research question and a unique objective to be achieved. Thereafter, the viability of the security framework was investigated in the framework evaluation.

Section 9.2 presents the summary of the major findings from the literature review. Section 9.3 discusses the summary of the major findings from the threat identification; Section 9.4 presents the summary of the major findings from the framework evaluation; Section 9.5 presents the contribution to body of knowledge; Section 9.6 discusses the limitation of the study; Section 9.7 outlines the recommendations while section 9.8 presents the summary.

9.2 Findings from the literature

It was revealed from the literature that individual and organization practices have to be re-defined and policies have to be drawn up to provide guidelines that accommodate the BYOD

trend in the banking sector, especially in developing countries which include Nigeria (Mphahlele, 2016). In addition, the literature revealed that organization practices, which include allowing employees to use their mobile devices from home or public places, create security risks. Similarly, individual practices such as employees connecting their mobile devices to unregulated networks result in security threats which include data leakage (Bello et al., 2015). The individual practices would have been stopped but most organizations have adopted this practice because of the profound benefits they derived from BYOD (Bello et al., 2015).

Furthermore, it was revealed that BYOD security threats could be considered under three major domains, namely technical, social and mobility domains (Ofusori et al., 2018). Technical security threats include phishing, keystroke logging, rogue devices, jailbreaking, data interception, network exploitation and unregulated public networks (Bello et.al, 2015). Social security threats include malicious insiders, data privacy violations, data ownership violations, user policy violations and disgruntled employees (Shumate & Ketel, 2014). Finally, mobility security threats include lost or stolen devices, e-waste, sharing mobile devices, and WiFi eavesdropping (Juniper Network, 2011; Karen, 2015).

The literature revealed the existing security measures as they relate to each domain (i.e. technical, social and mobility). For the technical domain, the existing mitigating measures include password authentication, encryption, firewalls, anti-virus/malware software, anti-phishing, hardware tokens, encrypted cookies and Windows Defender (Bello et.al, 2015). The mitigating measures for social include training on the acceptable use of an ICT policy, training on information security and enforcement of security policies (Shumate & Ketel, 2014). Similarly, the mitigating measures for mobility include mobile device management, intrusion detection services and tracking devices (Wang et al., 2014). A review of these existing security measures indicates they are effective for mobile security but are not sufficient as they all have their limitations (Bello et al., 2015). Hence, it is vital for organizations to understand and address the implications caused by unknown devices entering the organizational environment (Twinomurinzi & Mawela, 2014).

The study also identified related security frameworks from the literature. These frameworks come in various degrees of complexity and are used to build an information security programme to reduce vulnerabilities and manage risks. This includes ISO/IEC 2700 series (Granneman, 2013), PCI DSS (Al-Ahmad & Mohammad, 2012), COBIT (ISACA, 2011), NIST SP 800 series (NIST, 2012), CISCO security control framework and IBM security framework (Buecker et al., 2010). Following the review of these frameworks, the limitations identified are a deterrent to the Fourth Industrial Revolution (Schwab, 2016).

In addition, a review of the application of relevant theories was carried out in the study. From the review and analysis of the existing theories, it is clear that there is no single theory or model that sufficiently explains the variables (constructs) surrounding the BYOD phenomenon and its interrelationship with organization and individual practices (Yang et al., 2013). Hence, the researcher combined the three theories, namely organization theory, mobility theory and socio-technical theory so as to hypothesise the conceptual framework for the Nigerian banking sector which will eventually add to the body of knowledge.

It is obvious from the literature that not much research has been carried out to investigate or explain these domains (i.e. technical, social and mobility) surrounding the BYOD phenomenon and its interrelationship with organization and individual practices. Furthermore, a security framework that takes into account the peculiarity of the study context and one that also highlights security awareness indicators was lacking. As a result of these gaps, this study explains the link between individual and organization practices in exploring BYOD security threats with a view to developing a security framework.

9.3 Findings from threat identification

The threat identification phase of the study identified the security threats associated with the technical, social and mobility domains. To achieve this objective, the explanatory sequential mixed-methods approach was followed. In this case, the quantitative approach was first used to explore individual practices in identifying BYOD security threats. Thereafter, the influence of these security threats on the Nigerian banking sector was investigated. The qualitative technique was then used to elicit more information regarding organization

practices in exploring BYOD security threats. The major findings from the threat identification are presented as follows:

9.3.1 General practices

Using descriptive analysis of the categorized four types of mobile devices (smartphones, laptops, tablets and other devices), the study generally revealed that the majority of the respondents have used smartphones and laptops for both work and personal purposes. These were measured based on ‘Yes’ or ‘No’ answers. Again, for each type of mobile device, the chi-square goodness-of-fit was used to test whether any of the response options are selected significantly more or less often than the others. It was found that a significant number of the respondents indicated that they use smartphones and laptops for work and personal usage. This finding was considered significant as it clearly showed that both smartphones and laptops are used for both work and personal purpose.

9.3.2 Technical security threats

It can be recalled that a bivariate analysis was carried out to determine whether there is a significant relationship between technical practices and BYOD security threats (section 5.4.3). The four major technical practices that were considered for quantitative study were firstly, “*allowing software on device to manage login credentials*” (section 5.4.3.1); secondly, “*saving work documents from laptop to a free cloud storage*” (section 5.4.3.2); thirdly, “*updating mobile device on public network*” (section 5.4.3.3) and lastly, “*not adhering to security measures*” (section 5.4.3.4). It was revealed that these technical practices have given rise to the following security threats; data leakage, data ownership violation WiFi eavesdropping, unauthorized location tracking, phishing, viruses, malware and jailbreaking. Furthermore, the qualitative study for the ICT department personnel identifies “*keystroke logger*” and “*rogue device*” as a technical security threat (section 5.5.1.1).

On the other hand, the qualitative study for the executive managers acknowledged three major organization practices that lead to three technical security threats. Firstly, “*there is no definite policy guiding the use of BYODs*” (section 5.5.2.1); secondly, “*the organization*

provides laptops to individuals' for official purpose as well as allowing employees to personally acquire their own mobile but the organization does not monitor nor maintain this device" (section 5.5.2.1); and lastly, *"the organization does not have a specific operating system approved to be used"* (section 5.5.2.1). For each of these practices it was found that security threats such as malware, phishing, jailbreaking and data leakage are inevitable (Bello et al., 2015). This confirms four out of the other security threats identified for the quantitative study.

9.3.3 Social security threats

A bivariate analysis was carried out to determine whether there is a significant relationship between social practices and BYOD security threats (section 5.4.4). Three major social practices were considered for the quantitative study: Firstly, *"Clicking on links, advertisement and videos/audios"* (section 5.4.4.1); secondly, *"attaching customer bank statement to e-mail/instant messages"* (section 5.4.4.2); and lastly, *"sharing of password with colleagues or friends/family"* (section 5.4.4.3). These three major social practices have given rise to the following security threats: data leakage, spamming, jailbreaking, malware, viruses, spyware and WiFi eavesdropping.

However, the qualitative findings for ICT department personnel differed slightly from one of the quantitative findings, namely *"the banks do not allow employees to use social media"* (section 5.5.1.2). This is in contrast with the quantitative findings on social media (section 5.4.4.1) where individuals (i.e. employees) acknowledged that they click on links, advertisement and videos and audios on social media. However, Aula (2010) asserts that organizations' information that is made available on the social media can be stolen and used to commit security breaches, referred to as *"data privacy violation"*. In addition, the qualitative findings regarding the ICT department personnel have revealed that *"backups are allowed on laptops as well as the bank's server"* (section 5.5.1.2). This is line with the quantitative results (section 5.4.3.3) whereby employees admitted saving work documents on laptops before uploading them to a free cloud storage. However, while the portability of these mobile devices allows continuous access to work-related functions and personal information from any location, it also leads to incidences of theft or loss (Karen, 2015).

Similarly, the interviews conducted with ICT department personnel reveal “*employees’ non-compliance to security policies*” (section 5.5.1.2) which has resulted in “*loss of confidential information*”.

On the other hand, the qualitative study for the executive managers acknowledged three major organization practices that lead to social security threats. Firstly, “*there is no specified interval for reviewing security policies*” (section 5.5.2.2); secondly, “*disgruntled employees are only being monitored by their action*” (section 5.5.2.2); and lastly, “*there is budget shortages in developing a security framework*” (section 5.5.2.2). For each of these practices the study found the following security threats, namely obsolete security policies, disgruntled employees and budget shortages for a security framework.

9.3.4 Mobility security threats

A bivariate analysis was carried out to determine whether there is a significant relationship between the mobility practices and BYOD security threats (section 5.4.5). For the quantitative study, three major mobility practices were considered; firstly, “*methods used to prepare mobile device for disposal*” (section 5.4.5.1); secondly, “*methods employees used to dispose obsolete/faulty devices*” (section 5.4.5.2); and lastly, “*sharing mobile devices with colleagues and friends/family*” (section 5.4.5.3). These practices have given rise to the following security threats, namely WiFi eavesdropping, data leakage, viruses and phishing. However, contrary to the quantitative findings on the sharing of mobile devices (section 5.4.5.3) where employees admitted they share mobile devices, the interviews conducted with the ICT department personnel have revealed that “*employees’ are not allowed to share their mobile devices*” (section 5.5.1.3). Furthermore, qualitative findings have revealed that there have been cases of “*lost/stolen devices*” that were reported but not recovered (5.5.1.3). Additionally, the findings revealed that the banks were unable to address security issues caused by lost or stolen devices (section 5.5.1.3). Lastly, the qualitative findings from the ICT department personnel revealed that “*employees are allowed to dispose of their faulty or obsolete devices by themselves*” (section 5.5.1.3). These findings are in agreement with the qualitative findings from the executive managers, namely that “*there is no policy guiding employees’ disposal of mobile devices*” (section 5.5.2.3).

9.3.5 The influence of technical, social and mobility security

The study adopted the threat classification technique in exploring the influence of technical, social and mobility security threats on the Nigerian banking sector (section 7.2). It was revealed that the classified security threats gave rise to four other security threats domains which include 'socio-technical', 'e-commuting', 'pervasive' and 'lack of awareness'. This led to sorting out the security threats that are peculiar to either one, two and three domains respectively based on research findings as well as the literature. The outcome of the classification shows that technical, social and mobility domains can be regarded as low risk (LR) domains because the security threats are only peculiar to a particular domain; they do not affect more than one domain at a time (Yang & Yao, 2009). On the other hand, 'sociotechnical', 'pervasive' and 'e-commuting' domains can be regarded as medium risk (MR) domains because the security threats are only peculiar to two domains and can bring down the two domains at the same time if the right security measures are not put in place (Ghosh et al., 2013).

However, 'lack of awareness' is considered as a high risk (HR) domain because it affects the three domains at the same time which can be very harmful to the organization (Ghosh et al., 2013). Kathleen (2015) argues that a lack of awareness is a major factor contributing to most security threats. Hence, LR are security threats that are harmful but not to the same extent as the other two risks, namely MR and HR (Ghosh et al., 2013) while MR are security threats that are harmful but not to the same extent as the HR but are more harmful than LR. However, an HR security threat is considered the most harmful because it affects the three domains at the same time and can bring the organization down at once. This risk levels informs the type of security framework that was developed.

9.3.6 Existing security measures

This study identified the security measures put in place such as firewalls, antivirus software,, antispyware, proxy servers and intrusion detection systems (section 5.5.1.1) which are effective for mobile security but are not sufficient and may not address employees' and organizations' lack of awareness. Furthermore, the findings reveal areas that need more security focus which include the banks' network systems and customer databases (section

5.5.1.1). This also emphasises the fact that the existing security measures are not sufficient, hence giving rise to the development of a security framework. The developed 3-D security framework for BYOD-enabled banking institutions in Nigeria was evaluated and the findings are summarized in section 9.4.

9.4 Findings from the framework evaluation

It was revealed from the descriptive analysis that the appropriateness of the 3-D security framework aligns with the policies and strategies of the bank. Additionally, it could enhance the effectiveness of the bank data security and could contribute towards the efficiency of the bank operations. Similarly, in evaluating the adequacy of the security framework it was revealed that it could address all the technical, social and mobility threats identified from the study. Furthermore, the feasibility evaluation of the security framework indicates that it is cost effective, it can be implemented in a short period of time and it can be implemented with the available resources. Likewise, the flexibility evaluation of the security framework shows that it could be easily adopted with changing policies and could be used for mitigating security threats within or across different branches of the bank. Again, evaluating the intention to use the security framework reveals that the bank is willing to use the security framework as it is and also to adopt the framework immediately. Also, it was revealed that using the framework by the employees will be easy. Additionally, the thematic analysis corroborates the descriptive analysis as the participants affirm their satisfaction with the security framework. This implies that there is a degree of uptake in terms of implementation.

However, the security framework was revised based on some recommendations from the participants to incorporate their suggestions (Figure 8.16).

9.5 Contribution to body of knowledge

Firstly, the study provides a contribution to literature by explaining the link between individual and organization practices in exploring BYOD security threats under three major domains, namely technical, social and mobility. Although there is considerable research on BYOD trends, to the researcher's knowledge there has been no study of BYOD in the specific context of the Nigerian banking sector.

Secondly, another contribution relates to the theoretical and methodological approaches used in the study. The combination and adaptation of the organization theories, socio-technical theory and mobilities theory has been used uniquely to hypothesise the conceptual framework for the Nigerian banking sector which eventually adds to the body of knowledge.

The third major contribution is the development of a 3-D security framework for BYOD-enabled banking institutions in Nigeria that will help the banking sector to mitigate BYOD security threats in the Fourth Industrial Revolution. In addition, the security framework provides a basis on which banks in developing countries can enhance their security while supporting their employees in using their personal devices in executing their duties as employees of the bank. Hence, the security framework is an innovative contribution within the context of information security for the BYOD phenomenon in the Nigerian banking sector.

Lastly, the study enlightens individuals (employees) and organizations on the different security threats caused by using personally owned devices and also highlights the importance of educating employees who are constantly using personal devices to access corporate data.

9.6 Limitations of the study

It is important to note that the solutions for security breaches will keep changing because cybercriminal are adaptive and given time, will usually find ways to by-pass such security solutions. However, this research has identified some limitations which can be considered for future research.

Firstly, the security framework developed in this study is exclusively for Nigerian banking sector and it only considers individual and organizations practices and does not include the third party in tackling threats arising from technical, social and mobility domains. The developed security framework is applicable to Nigeria because of the following reasons: firstly, threats were identified through data collected from the Nigerian banks, hence the result cannot be generalized. Secondly, the banking technology used in Nigeria is not the same as the other countries. Lastly, the framework evaluation for acceptance was done by the

bank's officials in Nigeria; hence, the framework may not be applicable to other African banks. However, to be able to generalize the result, the researcher has made a recommendation for future research to extend its samples to other banking institutions in different countries.

Secondly, the resources available for each bank are not the same. This limitation was identified from the framework evaluation (Figure 8.9) where three participants disagreed that the framework could be implemented with the available resources. This implies that the available resources at hand are insufficient for the implementation of the security framework. According to Downer and Bhattacharya (2015), it is imperative to implement security measures to protect all devices' hardware and software as well as maintaining secure and stable connections for all devices connected to the network. This is because extra resources are needed to maintain the required level of security (Lindström & Hanken, 2018). Hence, this limitation is noted for recommendation.

A third limitation of this study was discovered from the framework evaluation (Figure 8.10) where three participants disagreed that the framework could be adopted with the changing of policies. In addition, another three participants (Figure 8.12) also disagreed that the framework could be adopted for mitigating security threats across different banks. This is because of the inconsistency in terms of ICT policy across the banks (Downer & Bhattacharya, 2015). Hence, a separate ICT policy guideline is required for each bank: this was not considered in this research.

Fourthly, two participants from the framework evaluation phase (Figure 8.7) disagreed that the framework could be cost-effective. In addition, another two participants (Figure 8.8) also disagreed that the framework could be implemented within a short period of time. This is as a result of budget constraints which were identified by the respondents in section 5.5.2.2. According to Hong (2013), every organization needs to have an adequate budget set apart for security framework implementation at any point in time. Hence, this limitation is noted for recommendation.

Fifthly, the scope of the research is limited to BYOD, hence smart cards which include credit and debits cards were not considered. This limitation was based on the responses received from the participants in section 8.3.1 where a respondent suggested credit card encryption.

Lastly, this research does not focus on employees' privacy, or that of customers or account holders, hence there is a need for further research that focuses on employees' privacy as well as that of customers and account holders.

9.7 Recommendations

In general, this study recommends a periodic review of the framework for effective security. This is because with the emerging trends of technology, the possibilities of new mobile devices may emerge, and the pattern of usage may change.

9.7.1 Recommendations for employees

Based on the research findings, this study recommends the following for the bank employees:

Firstly, this study recommends that employees comply with security policies and guidelines laid down by the organization. This is in line with the research findings that revealed that employees do not comply with security policies (section 5.5.1.2). Compliance with security policies will help to guide against security breaches (Disterer & Kliner, 2013).

Secondly, employees should endeavour to monitor third party device usage. This recommendation is based on the research findings that confirm that most employees share their mobile devices with colleagues, friends or family (section 5.4.5.3). "Sharing of mobile device can lead to cases of lost or stolen devices, which endangers the device as the security can be compromised" (Karen, 2015).

Thirdly, it is recommended that employees promptly notify the appropriate authorities (e.g. ICT department) of any case of lost or stolen devices. This recommendation is based on the research findings that revealed that there are cases of lost or stolen devices (section 5.5.1.3). Reporting such cases will help the organization to take prompt action to avoid security breaches (Karen, 2015).

Fourthly, employees should endeavour to notify the appropriate authorities of their obsolete or faulty devices before disposal. This recommendation is in line with the research findings that revealed that “employees have no right to dispose of mobile devices given to them by the organization, except if the organization allows them to do so” (section 5.5.2.3).

Fifthly, employees should always maintain regular data backups on the server. This recommendation is in line with the study findings that revealed “saving work documents from laptop to a free cloud storage” leads to “data leakage” (section 5.4.3.3).

Lastly, it is recommended that employees maintain an effective organizational cybersecurity culture by making information security considerations an integral part of their job, attitude, habits and conduct in their day-to-day activities (Enisa, 2017). “Organizational cybersecurity culture helps to shape the security thinking of all employees, thus improving resilience against all cyber threats” (Enisa, 2017).

9.7.2 Recommendations for ICT department personnel

This study recommends the following for the ICT departments’ personnel based on the research findings:

Firstly, it is recommended that the ICT department personnel register every personal mobile device as well as the owner of the device in the organization’s database; this includes device identification (e.g. International Mobile Equipment Identity [IMEI]), device ownership and the operating system (Twinomurinzi & Mawale, 2014). This recommendation is given based on the research findings that confirm that employees are allowed to acquire their own mobile devices (section 5.5.2.1) as well as rogue devices connecting to the organization network (section 5.5.1.1).

Secondly, this study recommends a service-oriented approach (SOA) for the ICT department as an additional security measure for mobile device management (Valilai & Houshmand, 2013). The SOA automatically downloads all the security measures when an employee’s

'approved device' is connected to the organization network and makes it active on the employee's device (Valilai & Houshmand, 2013).

Thirdly, this study recommends the setting up of security alerts. This will help the ICT department to be aware of what is happening on the network (Green & Basil, 2013), for example, "get an alert whenever employees download unapproved application or mobile device sign-in or logout" (Green & Basil, 2013). This recommendation was given based on a study that identified data leakage and rogue devices as two of the security threats (section 5.4.3.1 and 5.5.1.1).

Fourthly, it is recommended that the ICT department employ the use of mobile device management to restrict application usage by providing a list of approved applications and disallowing the installation of unapproved applications. It can also be used to ensure that employees enable the security measures provided by denying a sign-in attempt if a security measure has not been enabled (Ortbach, Brockmann & Stieglitz, 2014). This recommendation was given based on the research findings that revealed that some employees do not use some of the security measures (section 5.4.3.4).

Fifthly, it is the responsibility of the ICT department's personnel to ensure that they are updated with the latest scientific knowledge on the safe management of mobile device waste by undertaking more training in e-waste management (keys, 2013). This recommendation is given based on the research findings that identified obsolete or faulty devices and lost or stolen devices as two of the security threats (section 5.4.5.2 and 5.5.2.3).

Sixthly, it is recommended that organizations use persuasive technology to create awareness and training for employees regarding information security, which can help employees to change their behaviour. Persuasive technology can be used to change attitudes by conveying social presence and persuasion (Qudaih et al., 2014). For example, dialogue boxes can be used to persuade users to update software, to stop visiting malicious web sites, and to renew passwords. This recommendation is given based on the research findings that identified employees' non-compliance as one of the security threats (section 5.5.1.2).

Seventhly, this study recommends a separate ICT policy guideline for each bank; this is a factor that was not considered in this study. According to Downer and Bhattacharya (2015), there is inconsistency in terms of ICT policy across the banks (Downer & Bhattacharya, 2015).

Lastly, the study recommends an effective cybersecurity culture to be introduced and nurtured within the wider organizational culture in collaboration with employees, rather than imposed, if the value of cybersecurity is to be accepted by all members (Enisa, 2017).

9.7.3 Recommendations for executive managers

This study recommends the following for the executive managers of the bank based on research findings:

The study recommends that executive managers develop ICT policy guidelines that support BYOD. In addition, this policy should be reviewed at regular intervals. According to Vanderlinde et al. (2012), an ICT policy plays an important role in leveraging security threats that may emerge as a result of using BYODs. However, based on the research findings, it is obvious that the existing ICT policy does not support the BYOD trend because the policies were developed prior to the emergence of BYOD (The Ministry Of Communication Technology, 2012). This recommendation was given based on the research findings that identify obsolete security policies as one of the security threats (section 5.5.2.2).

Secondly, it is recommended that adequate budget and resources are allocated for security framework implementation. This recommendation is in line with the research findings that identified budget constraints as one of the limitations for framework development (section 5.5.2.2). According to Hong (2013), every organization needs to have adequate budget set aside for security framework implementation at any point in time.

Thirdly, the study recommends a well-defined disciplinary procedure in case of breach of organizational IT policies. This policy will outline the process that will be used to discipline any employee that fails to comply with or maintain the required standards (Bulgurcu et al.,

2010). This recommendation is based on the research findings that identified “lack of regulations guiding employees’ interaction” (e.g. disgruntled employees) as one of the security threats (section 5.5.2.2). This disciplinary procedure is to ensure that employees are acquainted with the guiding principle that governs their conduct (Bulgurcu et al., 2010).

Lastly, the study suggests that the executive managers organize periodic security training for employees. The primary goal of organizations in conducting information security training is to give adequate knowledge which will eventually change individuals’ attitudes towards information security (Downer & Bhattacharya, 2015). This will ensure awareness of risks and convey information on how to maintain good practices.

9.7.4 Recommendation for future research

Based on the limitations of the study, the following areas of research are therefore suggested for further studies:

Further study can be done to include third party support in addition to individual and organization practices in tackling threats arising from technical, social and mobility domains.

Future research should extend its samples to other banking institutions in different countries in order to generalise results based on large samples. Furthermore, the scope of BYOD should be extended to include smart cards (credit and debit cards). This recommendation is based on the responses received from the respondents in section 8.3.1 where a respondent suggested credit card encryption.

In addition, further research should focus on employees’ privacy while using their mobile devices in a BYOD-enabled environment. According to Deasy et al. (2018), employees are concerned with the issue of data privacy because their personal information is at the disposal of their employer. Privacy invasion arises when an employer tries to access employees’ devices and such action can result in lawsuits when not handled properly (Lebek et al., 2013).

Lastly, the framework developed in this study may be further explored to include customers and account holders. This is because while customer and account holders are using their mobile devices to surf the Internet, hackers can easily steal their login credentials and use the credentials to access the bank's server without their knowledge (Ofusori et al., 2018).

9.8 Summary

This study explored individual and organizational practices in identifying BYOD security threats under three major domains, namely technical, social and mobility domains. In addition, threat classification was used to explore the influence of these security threats on the banking sector. Three risk levels emerged as a result of this classification which include low risk, medium risk and high risk. This led to the development of a three-dimensional security framework for BYOD-enabled banking institutions in Nigeria. Hence, all the objectives of the study were achieved.

Furthermore, this study combined three theories, namely organization, socio-technical and mobility theory so as to hypothesise the conceptual framework for the Nigerian banking sector which will eventually add to the body of knowledge. Additionally, the research onion informs the research process and procedures used in this study. Research onion was used to explain different research methodologies before adopting the most suitable one for this study. In addition, the developed three-dimensional security framework for BYOD-enabled banking institutions in Nigeria was sent out for evaluation and the result of the evaluation suggests that it is implementable. Hence, by implication, the continuity of BYODs in the Nigerian banking sector is guaranteed.

Finally, since this study is limited to Nigerian banks; all other banks in other countries are excluded. This also means that the results cannot be generalized to other banks outside Nigeria. Hence, it is recommended that future research should extend its samples to other banking institutions in different countries in order to generalise results based on large samples.

REFERENCES

- Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248.
- Acar, T., Belenkiy, M., & Küpçü, A. (2013). Single password authentication. *Computer Networks*, 57(13), 2597-2614.
- Adeniran, A. I. (2008). The internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology*, 2(2), 368-381.
- Akbari, S., & Land, F. (2011). Theories used in IS research: Socio-technical theory. Retrieved from <http://www.istheory.yorku.ca/sociotechnicaltheory.htm>
- Al-Ahmad, W., & Mohammad, B. (2012). Can a single security framework address information security risks adequately? *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 2(3), 222-230.
- Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science*, 2(2), 28-43.
- Alade, S. O. (2013). Quality statistics in banking reforms for national transformation. *CBN Journal of Applied Statistics*, 3(2), 127-142.
- Alawatugoda, J., Stebila, D., & Boyd, C. (2015). Protecting encrypted cookies from compression side-channel attacks. *Financial Cryptography and Data Security* (pp. 86-106): Springer.
- Alexandrou, A., & Chen, L.-C. (2015). *A security risk perception model for the adoption of mobile devices in the healthcare industry*. Pace University.
- Alfawaz, S., Nelson, K., & Mohannak, K. (2010). 'Information security culture: A Behaviour Compliance Conceptual Framework', 8th Australasian Information Security Conference, Brisbane, Australia.
- Amer, S. H., & Hamilton, J. A. (2010). Intrusion detection systems (IDS) taxonomy-a short review. *Defense Cyber Security*, 13(2).
- Andrew, H., & Kyle, G. (2015). Departing employees and data theft. *Digital Workplace*. Grand Valley State University, Michigan, USA.
- Appelbaum, S. H. (1997). Socio-technical systems theory: An intervention strategy for organizational development. *Management Decision*, 35(6), 452-463.

- Anti-Phishing Working Group (APWG, 2013). Phishing activity trends report, 2nd Quarter 2013: Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.
- Aribake, F. O. (2015). Impact of ICT tools for combating cyber crime in Nigeria online banking: A conceptual review. *International Journal of Trade, Economics and Finance*, 6(5), 272.
- Arregui, D. A., Maynard, S. B., & Ahmad, A. (2016). Mitigating BYOD information security risks. Australasian Conference on Information Systems 2016. Wollongong, Australia, pp. 1–11, 05-07 December 2016.
- Asheri, C. J., Louise, Y., & Stewart, K. (2012). Security metrics and evaluation of information systems security. Department of Computer and Systems Sciences, Stockholm University/KTH Forum 100, 164 40 Kista, Sweden
- Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems*, 14(2), 195-201.
- Atallah, M., & Hopper, N. (2010). Privacy enhancing technologies. *Proceedings of the 10th International Symposium, PETS 2010*, July 21-23, 2010, Berlin, Germany. (Vol. 6205): Springer.
- Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership*, 38(6), 43-49.
- Badke, W. (2004). Research strategies: Finding your way through the information fog, iUniverse. Retrieved from <https://books.google.co.za/books?hl=en&lr=&id=b0DDDgAAQBAJ&oi=fnd&pg=PT13&dq=Finding+your+way+through+the+information+fog&ots=0G-4Hhlxtt&sig=sj-3Yaehz9piryFg3O8ewqokASM#v=onepage&q=Finding%20your%20way%20through%20the%20information%20fog&f=false>
- Bakshi, A., & Yogesh, B. (2010). Securing cloud from ddos attacks using intrusion detection system in virtual machine. *Paper presented at the Second International Conference*

- on Communication Software and Networks, 2010, (ICCSN'10).pp. 260-264. IEEE. June 29-July 1, 2010. Hong Kong.*
- Balachandran, A., Voelker, G. M., & Bahl, P. (2005). Wireless hotspots: Current challenges and future directions. *Mobile Networks and Applications, 10*(3), 265-274.
- Balogun, V. F., & Obe, O. O. (2010). E-crime in Nigeria: Trends, tricks, and treatment. *The Pacific Journal of Science and Technology, 11*(1), 343-355.
- Barlette, Y., & Fomin, V. V. (2010). The Adoption of information security management standards. *Information Resources Management: Concepts, Methodologies, Tools and Applications: Concepts, Methodologies, Tools and Applications* (pp. 69-90). IGI Global
- Basole, R. C. (2004). The value and impact of mobile information and communication technologies. *Paper presented at the Proceedings of the IFAC Symposium on Analysis, Modeling & Evaluation of Human-Machine Systems* (Vol. 9, pp. 1-7). Atlanta, Georgia USA.
- Bello, A. (2014). *A review of the regulatory & legal framework of public sector accounting in Nigeria.* Retrieved from https://www.academia.edu/13054899/A_Review_of_the_Regulatory_and_Legal_Framework_of_Public_Sector_Accounting_In_Nigeria
- Bello, G. A., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARNP Journal of Engineering and Applied Sciences, 10*(3), 1279-1287.
- Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective, part II: The application of socio-technical theory. *MIS Quarterly, 11*-28.
- Bowen, B. M., Salem, M. B., Hershkop, S., Keromytis, A. D., & Stolfo, S. (2009). Designing host and network sensors to mitigate the insider threat. *IEEE Security & Privacy, 7*(6), 22-29.
- Brace, I. (2018). *Questionnaire design: How to plan, structure and write survey material for effective market research.* New York, USA. Kogan Page Publishers.
- Broomhead, S. (2013). *Gartner says BYOD is disruptive.* Retrieved from <https://books.google.co.za/books?id=w9ZdDwAAQBAJ&pg=PA228&lpg=PA228&dq=Gartner+says+BYOD+is+disruptive.&source=bl&ots=e6ibck4ehg&sig=xCOB>

CnIPJfgbNeVoC-

ZPuVrD_P0&hl=en&sa=X&ved=2ahUKEwijoN3koaHfAhVTt3EKHaLnBmQQ6A
EwBXoECAAQAQ#v=snippet&q=broomhead&f=false

- Broughton, A., Higgins, T., Hicks, B., & Cox, A. (2009). *Workplaces and social networking - The implications for employment relations*. Brighton: Institute for Employment Studies.
- Bryman, A., & Bell, E. (2015). *Business research methods*. USA, NY: Oxford University Press.
- Buecker, A., Borrett, M., Lorenz, C., & Powers, C. (2010). Introducing the ibm security framework and ibm security blueprint to realize business-driven security: *International Technical Support Organization*. IBM Corp., Vol. 4528 No. 1, pp. 1-96.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Bunn, C. (2016). Is Decision. Retrieved from <https://www.isdecisions.com/>
- Cameron, K. S., & Whetten, D. A. (2013). *Organizational effectiveness: A comparison of multiple models*. United Kingdom, NYCity: Academic Press.
- Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). Challenges for securing cyber physical systems. *Paper presented in Workshop on future directions in cyber-physical systems security: The Department of Homeland Security (DHS)'s Science and Technology Directorate*. Newark, New Jersey, USA. July 22-24, 2009.
- Carmine, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment* (Vol. 17): Sage publications
- Catherine, L. A., & Ritu, A. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-644.
- Cerna, L. (2013). The nature of policy change and implementation: A review of different theoretical approaches. Geneva, Switzerland: *Organisation for Economic Cooperation and Development (OECD) report*.

- CERT insider threat. (2015). *Insider threat blog*. Retrieved from www.insights.sei.cmu.edu/insider-threat/2015/07/handling-threats-from-disgruntled-employees.html
- Chanda, R., & Zaorski, S. (2013). Social media usage in the financial services industry: Toward a business-driven compliance approach. *Journal of Taxation and Regulation of Financial Institutions*, 26(5), 5-20.
- Chen, C.-M., Chen, Y.-H., Lin, Y.-H., & Sun, H.-M. (2014). Eliminating rouge femtocells based on distance bounding protocol and geographic information. *Expert Systems with Applications*, 41(2), 426-433.
- Cherns, A. (1976). The principles of sociotechnical design¹. *Human Relations*, 29(8), 783-792.
- Chomeya, R. (2010). Quality of psychology test between Likert scale 5 and 6 points. *Journal of Social Sciences*, 6(3), 399-403.
- CISCO. (2009). CISCO security control framework (SCF) model. Retrieved from <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/CiscoSCF.html>
- Clark, P. G. (2013). Firewall policy diagram: Novel data structures and algorithms for modeling, analysis, and comprehension of network firewalls. Doctoral dissertation, University of Kansas. Retrieved from <https://kuscholarworks.ku.edu/handle/1808/11462>
- Cohen, D., & Crabtree, B. (2006). Qualitative Research Guidelines Project. Retrieved from <http://www.qualres.org/>
- Copeland, R., & Crespi, N. (2012). Analyzing consumerization-Should enterprise business context determine session policy? *Paper presented at the 16th International Conference on Intelligence in Next Generation Networks (ICIN)*. Berlin, Germany.
- Council Payment Card Industry. (2010). Payment Card Industry Council (PCI-Council), PCI DSS 2.0. USA: PCI Council Publication
- Creswell. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, California: Sage Publications.
- Czarniawska, B. (1999). *Writing management: Organization theory as a literary genre*. Oxford: Oxford University Press.

- Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, 48, 281-297.
- De las Cuevas, P., Mora, A., Merelo, J. J., Castillo, P. A., Garcia-Sanchez, P., & Fernandez-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications*, 68, 83-95.
- Deasy, S., Meyer, R., Newell, C., Emil, S., Wisner, P., Furodet, D., & Strudel, F. (2018). Controlling use of a business environment on a mobile device: Google Patents. Retrieved patents.google.com/patent/US9247042B2/en
- Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE handbook of qualitative research (3rd ed.)*. Thousand Oaks, CA, : Sage Publications.
- Dick, B. (1993). *You want to do an action research thesis*. Retrieved from <http://www.aral.com.au/resources/arthesis.html>
- Dimensional Research. (2013). *The impact of mobile devices on information security: A survey of professionals*. Retrieved from www.dimensionalsearch.com
- Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. Retrieved from www.dx.doi.org/10.1016/j.protcy
- Dittrich, D., & Kenneally, E. (2012). The Menlo Report: Ethical principles guiding information and communication technology research. *US Department of Homeland Security*. Retrieved from http://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/
- Dittrich, D., Reiher, P., & Dietrich, S. (2004). *Internet denial of service: Attack and defense mechanisms*. NJ, USA: Pearson Education.
- Dobson, I., & Hietala, J. (2011). *Risk management: The open group guide*. United Kingdom: Van Haren Publishing.
- Downer, K., & Bhattacharya, M. (2015). BYOD security: A new business challenge. *Paper presented at the IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*: Chengdu, China. December 19-21, 2015.
- Drape, S. (2004). *Obfuscation of abstract data types*. Doctoral thesis: University of Oxford.

- Du, H., & Zhang, C. (2006). Risks and risk control of WiFi network systems. Retrieved from https://www.researchgate.net/publication/268053793_Risks_and_Risk_Control_of_WiFi_Network_Systems
- Dunnett, R. (2012). *Information security, mobile security and internet of things. BYOD-Bring your own device*. Retrieved from <http://www.bringyourownit.com/2012/06/25/byod-bring-your-own-device/>
- Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, (3)1,93-98.
- Ehrenfeld, J. M. (2017). WannaCry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems*, 41(7), 104.
- El-Moussa, F. (2018). *Method and system for malicious code detection: Google patents*. Retrieved from <https://patents.justia.com/patent/9954889>
- Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P. and Sheth, A. N. (2014). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2), 5.
- European Union Agency for Network and Information Security (Enisa). (2017). Cybersecurity culture in organizations. Retrieved from <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>
- European Union Agency for Network and Information Security (Enisa). (2014). *Network and information security in the finance sector: Regulatory landscape and industry priorities*. Retrieved from <https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector>
- Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices*. Chicago, Illinois, USA
- Ferebee, S. S. (2010). Successful persuasive technology for behavior reduction: Mapping to fogg's gray behavior grid. *Paper presented at the International Conference on Persuasive Technology*. Springer, Berlin, Heidelberg

- Fogg, B. J. (2009). *A behavior model for persuasive design*. *Proceedings of the 4th International Conference on Persuasive Technology*. Claremont, California, USA
- Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information, Knowledge, Systems Management*, 7(1-2), 159-180.
- Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security*, 11(1), 38-54.
- Gartner. (2014). *Gartner says 75 percent of mobile security breaches will be the result of mobile application misconfiguration* [Press release]. Retrieved from <https://www.gartner.com/newsroom/id/2753017>
- Geldenhuys, K. (2016). WhatsApp scams - read before you click. *Servamus Community-based Safety and Security Magazine*, 109(11), 24-26.
- Gerić, S., & Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and Organizational Sciences*, 31(1), 51-61.
- Gharibi, W. (2012). *Some recommended protection technologies for cyber crime based on social engineering techniques -- phishing*. Retrieved from arXiv preprint arXiv:1201.0949.
- Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *International Journal of Global Research in Computer Science (UGC Approved Journal)*, 4(4), 62-70.
- Goguen, A., Stoneburner, G., & Feringa, A. (2017). Risk management guide for information technology systems and underlying technical models for information technology security. Retrieved from <https://www.amazon.com/Management-Information-Technology-Underlying-Technical/dp/0756731909>
- Golde, N., Redon, K., & Borgaonkar, R. (2012). Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. *Paper presented at the Network and Distributed System Security (NDSS)*. San Diego, USA.
- González, E. P., Tapiador, D. J. M. E., & Garnacho, D. A. R. (2008). Content authentication and access control in pure peer-to-peer networks. *Universidad Carlos Iii De Madrid*. Doctoral thesis.

- Goodyear, P., & Retalis, S. (Eds.). (2010). *Technology-enhanced learning*. Rotterdam, Netherlands: Sense Publishers.
- Goulding, C. (2002). *Grounded theory: A practical guide for management, business and market researchers*. Thousand Oaks California: Sage publications.
- Goverdhan, R., & Sammulal, P. (2013). Machine learning approach to anomaly detection in cyber security with a case study of spamming attack. *International Journal of Computer Engineering & technology*, 4(3), 113-122.
- Goyal, V., Ishai, Y., Sahai, A., Venkatesan, R., & Wadia, A. (2010). Founding cryptography on tamper-proof hardware tokens. *Theory of Cryptography* (pp. 308-326). Berlin, Heidelberg: Springer.
- Grand, J. (2000). Attacks on and countermeasures for USB hardware token devices. *Proceedings of the Fifth Nordic Workshop on Secure IT Systems*. Reykjavik, Iceland, October 12-13, 2000, pp 35-57
- Granneman, J. (2013). IT security frameworks and standards: Choosing the right one. *TechTarget Network*. Retrieved from <http://searchsecurity.techtarget.com/IT-security-frameworks-and-standards-Choosing-the-right-one>.
- Green, R. M., & Basil, N. J. (2013). Mobile device controller application for any security system: Google Patents. Retrieved from <https://patents.google.com/patent/US8489065B2/en>
- Gregory, K. (2011). The importance of employee satisfaction. *The Journal of the Division of Business & Information Management*. Retrieved from <https://www.managementstudyguide.com/importance-of-employee-satisfaction.htm>
- Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. *Paper presented at the Security and Privacy Workshops (SPW)*. 2014 IEEE. San Jose, CA, USA
- Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied thematic analysis*. Thousand Oaks, California : Sage.
- Gui-Hong, L., Hua, Z., & Gui-Zhi, L. (2010). Building a secure web server based on OpenSSL and Apache. *Paper presented at the 2010 International Conference on E-*

- Business and E-Government. 2010 International Conference on* (pp. 1307-1310).
IEEE. Guangzhou, China
- Guo, Y., Xu, Y., & Chen, X. (2017). Freeze it if you can: Challenges and future Directions in benchmarking smartphone performance. *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications* (pp. 25-30). ACM. Sonoma, CA, USA
- Gustav, A., & Kabanda, S. (2016). BYOD adoption concerns in the South African financial institution sector. In *CONF-IRM* (p. 59).
- Hammer, M., & Mangurian, G. E. (1987). SMR Forum. The changing value of communications technology. *Sloan Management Review (1986-1998)*, 28(2), 65.
- Hannam, K., Sheller, M., & Urry, J. (2006). Editorial: Mobilities, immobilities and moorings. *Mobilities*, 1(1), 1-22.
- Hanson, W. E., Creswell, J. W., Clark, V. L. P., Petska, K. S., & Creswell, J. D. (2005). Mixed methods research designs in counseling psychology. *Journal of Counseling Psychology*, 52(2), 224.
- Hartley, J. (2014). Some thoughts on Likert-type scales. *International Journal of Clinical and Health Psychology*, 14(1).
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*. 18(2), 106-125.
- Hofmann-Wellenhof, B., Lichtenegger, H., & Collins, J. (2012). *Global positioning system: Theory and practice*, 2nd ed., New York: Springer-Verlag Wien
- Hong, H. L. (2013). Feasibility study on incorporating IEC/ISO27001. *Information Security Management System (ISMS) Standard in IT Services Environment*. Universiti Teknologi Malaysia.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
- International Labour Organization. (2012). Rate of job creation insufficient to tame unemployment in Nigeria. *The International Labour Organization Publication*.

- Information Systems Audit and Control Association (ISACA). (2011). COBIT 4.1. Retrieved from www.isaca.org
- International Organization for Standardization (ISO).(2005). Information technology – Security techniques – Code of Practice for Information Security Management. ISO.
- James, D., & Philip, M. (2012). A novel anti-phishing framework based on visual cryptography. *Paper presented at the International Conference on Power, Signals, Controls and Computation (EPSCICON)*. 2012 International Conference on (pp. 1-5). IEEE. Thrissur, Kerala, India
- Johnson, B. (2013). Toward a new classification of nonexperimental quantitative research. *Educational Researcher*, 30(2), 3-13.
- Johnson, R.B. & Onwuegbuzie, A. J. (2004). Mixed-methods research: A research paradigm whose time has come. *Educational researcher*, 33(7), 14-26.
- Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, 25(3), 231-251.
- Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.
- Juniper Network. (2011). *Mobile device security- Emerging threats, essential Strategies*. Retrieved from www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj60-6g5oDKAhWMWBoKHWjtASwQFggyMAA&url=http%3A%2F%2Fwww.bytes.co.uk%2Fdownload_file%2Fview%2F943%2F537%2F&usg=AFQjCNGVmC_t7GmVQqdw36AgYtv9orttwg
- Kahate, A. (2013). *Cryptography and network security*. New Delhi: Tata McGraw-Hill Education.
- Kakihara, M., & Sørensen, C. (2001). Expanding the 'mobility'concept. *ACM SIGGroup Bulletin*, 22(3), 33-37.
- Kamatchi, A., & Modi, C. (2016). An efficient security framework to detect intrusions at virtual network layer of cloud computing. *Paper presented at the 19th conference on Innovations in Clouds, Internet and Networks (ICIN)*. March 1-3, 2016, Paris.

- Kaplan, E., & Hegarty, C. (2005). *Understanding GPS: Principles and applications*. Norwood, MA, USA: Artech House.
- Karen, T. (2015). *Device debacles – Lost, stolen, and neglected data risks*. Retrieved from <https://www.allclearid.com/blog/device-debacles-lost-stolen-and-neglected-data-risks>
- Kathleen, R. (2015). *Lack of cybersecurity awareness linked to CIOs*. Retrieved from www.searchsecurity.techtarget.com/opinion/Lack-of-cybersecurity-awareness-linked-to-CIOs
- Kearns, G. S. (2016). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, 8(1).
- Kelliher, F. (2011). Interpretivism and the pursuit of research legitimisation: An integrated approach to single case design. *Leading Issues in Business Research Methods*, 1, 45.
- Ketel, M., & Shumate, T. (2015). Bring your own device: Security technologies. *Paper presented at the SoutheastCon 2015*. Fort Lauderdale, FL, USA
- Keys, A. (2013). *Smartphone financial transactions: Security risks and control options*. University of Oregon.
- Khan, A. A. (2013). Preventing phishing attacks using one time password and user machine identification. *International Journal of Computer Applications*, 68(3),7-11
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, 30(3), 607-610.
- Kumar, R. (2011). *Research Methodology - A step-by-step for beginners* (3rd ed.). London: Sage Publications.
- Ladakis, E., Koromilas, L., Vasiliadis, G., Polychronakis, M., & Ioannidis, S. (2013). You can type, but you can't hide: A stealthy GPU-based keylogger. *Proceedings of the 6th European Workshop on System Security (EuroSec)*. Institute of Computer Science, Foundation for Research and Technology: Hellas, Greece Columbia University, USA.
- Lani, D. (2011). *Chi-square goodness of fit test*. Retrieved from <https://www.statisticssolutions.com/wp-content/uploads/kalins-pdf/singles/chi-square-goodness-of-fit-test.pdf>

- Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago Retrieved from <https://eprints.qut.edu.au/105686/>
- Lee. (2015). Cyber attacks, prevention, and countermeasures *Counterterrorism and Cybersecurity* (pp. 249-286). Switzerland: Springer.
- Lee, Park, J.-H., Chung, N., & Blakeney, A. (2012). A unified perspective on the factors influencing usage intention toward mobile financial services. *Journal of Business Research*, 65(11), 1590-1599.
- Lee, G. A., Yang, U., Kim, Y., Jo, D., Kim, K.-H., Kim, J. H., & Choi, J. S. (2009). Freeze-set-go interaction method for handheld mobile augmented reality environments. *Proceedings of the 16th ACM Symposium on Virtual Reality Software and Technology*. Kyoto, Japan: November 18 - 20, 2009
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 71-90.
- Lin, P.-C., Lin, P.-H., Chiou, P.-R., & Liu, C.-T. (2013). Detecting spamming activities by network monitoring with Bloom filters. *Paper presented at the 15th International Conference on the Advanced Communication Technology (ICACT)*. PyeongChang, South Korea, January, 2013.
- Lindström, J., & Hanken, C. (2018). Wearable computing: Security challenges, BYOD, privacy, and legal aspects. *Wearable Technologies: Concepts, Methodologies, Tools, and Applications* (pp. 1043-1067). Information Resources Management Association, USA: IGI Global.
- Lorch, M., Basney, J., & Kafura, D. (2004). A hardware-secured credential repository for Grid PKIs. Paper presented at the IEEE International Symposium on cluster computing and the gridCCGrid 2004: Chicago, IL, USA. April 2004
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469-479.
- Madzima, K., Dube, E. L., & Mashwama, P. M. (2013). ICT Education in Swaziland Secondary Schools: Opportunities and Challenges.

- Makimoto, T., & Manners, D. (1997). *Digital nomads*. Chichester: John Willey and Sons.
- Margaret, R. (2013). *Risk map*. Retrieved from <http://searchcompliance.techtarget.com/definition/risk-map>
- Mark, O. (2014). *Bring your own internet of things*. Retrieved from www.bringyourowninternetofthingscomingtobusinessin2015/
- Mathew, S., Upadhyaya, S., Ha, D., & Ngo, H. Q. (2008). Insider abuse comprehension through capability acquisition graphs. *Paper presented at the 11th International Conference on Information Fusion: Cologne, Germany. 30 June-3 July 2008*
- Matinde, V. (2015). *The rise of BYOD and corporate data threats*. Retrieved from: <http://www.idgconnect.com/abstract/9313/africa-the-rise-byod-corporate-threats>.
- Matthew, L. (2013). *Securing mobility: Developing a framework to assist in the development, implementation and enforcement of mobile device security policy*. A dissertation submitted for a Master's degree, College of St. Scholastica, Duluth, Minnesota.
- McBurney, D., & White, T. (2009). *Research methods*. Belmont, CA, USA: Cengage Learning.
- McHugh, M. L. (2013). The chi-square test of independence. *Biochemia Medica*, 23(2), 143-149.
- Miradore Management Suite (2016). *Device lifecycle management*. Retrieved from <https://mms.miradore.com/resource/device-lifecycle-management/>
- Moavenzadeh, J (2016). The fourth industrial revolution: Reshaping the future of production. Retrieved 20 November, 2017, from https://www.eiseverywhere.com/file_uploads/fe238270f05e2dbf187e2a60cbcd68e_2_Keynote_John_Moavenzadeh_World_Economic_Forum.pdf
- Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 2012(12), 5-8.
- Mphahlele, P. (2016). *The impact of bring-your-own-device on work practices in the financial sector*. University of Cape Town. Masters Dissertation
- Mulligan, P., & Gordon, S. R. (2002). The impact of information technology on customer and supplier relationships in the financial services. *International Journal of Service Industry Management*, 13(1), 29-46.

- National Bureau of Statistics. (2012). *Annual abstract of statistics*. Retrieved from http://www.nigerianstat.gov.ng/pdfuploads/annual_abstract_2012.pdf
- National Bureau of Statistics. (2017). *Use of financial services in Nigeria, Abuja*. National Bureau of Statistics Publication.
- National Institute of Standards Technology. (2014). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology Gaithersburg, MD.
- Nazar, A., Seeger, M. M., & Baier, H. (2011). Rooting Android – Extending the ADB by an auto-connecting WiFi-accessible service. *Paper presented at the Nordic Conference on Secure IT Systems*. Berlin, Heidelberg: Springer.
- Needham, R., & Lampson, B. (2008). Network Attack and Defense. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 383-390.
- Ngoqo, B., & Flowerday, S. V. (2015). Information security behaviour profiling framework (ISBPF) for student mobile phone users. *Computers & Security*, 53, 132-142.
- Nguyen, L., Tian, Y., Cho, S., Kwak, W., Parab, S., Kim, Y., Tague, P., and Zhang, J. (2013). UnLocIn: Unauthorized location inference on smartphones without being caught. *Paper presented at the International Conference on Privacy and Security in Mobile Systems (PRISMS)*: Atlantic City, NJ, USA. June 2013.
- NIST. In full. (2012). *Guide for conducting risk assessments*. NIST Special Publication 800-30, Revision 1. Retrieved from www.nist.org
- Norušis, M. J. (2006). *SPSS 14.0 guide to data analysis*. Upper Saddle River, NJ.: Prentice Hall.
- Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. *Paper presented at the Proceedings of the Seventh Australasian Conference on Information Security- Volume 98*: Wellington, New Zealand, January 2009.
- Nunoo, E. M. (2013). Smartphone information security risks. Retrieved from <http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1019739&dswid=-7869>
- Ofusori, L. O., Dlamini, N. N. J., & Prabhakar, R. S. (2018). Optimized three-dimensional security framework to mitigate risks arising from BYOD-enabled business environment. *In Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 205-233): IGI Global.

- Ojeka, S., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber Security in the Nigerian banking sector: An appraisal of audit committee effectiveness. *International Review of Management and Marketing*, 7(2), 340-346.
- Okonjo-Iweala, N., & Osafo-Kwaako, P. (2007). Nigeria's economic forum: Progress and challenges. *Bookings Global Economy and Development Working Paper 6*.
- Olalere, M., Abdullah, M. T., Mahmud, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *Sage Open*, 5(2), 2158244015580372.
- Olasanmi, O. O. (2010). Computer crimes and counter measures in the Nigerian banking sector. *Journal of Internet Banking and commerce*, 15(1), 1.
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1), 1.
- Ortbach, K., Brockmann, T., & Stieglitz, S. (2014). Drivers for the adoption of mobile device management in organizations. Retrieved from <https://aisel.aisnet.org/ecis2014/proceedings/track16/10/>
- Osterman Research. (2012). *The BYOD (Bring your own device) trend- Putting IT in control of BYOD*. Retrieved from <http://www.hyperoffice.com/byod-whitepaper/>
- Ostwald, T. (2017). Threat modeling data analysis in socio-technical systems. *arXiv preprint arXiv:1712.10243*.
- Parvizi, R., Oghbaei, F., & Khayami, S. R. (2013). Using COBIT and ITIL frameworks to establish the alignment of business and IT organizations as one of the critical success factors in ERP implementation. *Paper presented at the 5th Conference on Information and Knowledge Technology (IKT): Shiraz, Iran. May 2013*.
- Peltier, T. R. (2010). *Information security risk analysis*. New York. Auerbach Publications.
- Pfeifer, P. (2008). Chi-square goodness-of-fit test. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1284265
- Pratt Jr, D. E., & Jones, B. K. (2013). Mobile device management in the DoD enterprise network. *Practice*, 44(3), 179-196.
- Putri, F. F., & Hovav, A. (2014). Employees compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. Retrieved from <https://aisel.aisnet.org/ecis2014/proceedings/track16/2/>

- Qudaih, H. A., Bawazir, M. A., Usman, S. H., & Ibrahim, J. (2014). Persuasive technology contributions toward enhanced information security awareness in an organization. *arXiv preprint arXiv:1405.1157*.
- Queiroz, A. A., & De Queiroz, R. J. (2010). Breach of internet privacy through the use of cookies. *Paper presented at the Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments*. Samos, Greece 2010, ACM. NY, USA
- Raffaele, C., & Connell, J. (2016). Telecommuting and co-working communities: What are the implications for individual and organizational flexibility? *Flexible Work Organizations* (pp. 21-35) New Delhi: Springer.
- Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2006). Research methodology. *arXiv preprint physics/0601009*.
- Ray, J. R. (2014). *Training programs to increase cybersecurity awareness and compliance in non-profits*. Retrieved from <https://scholarsbank.uoregon.edu/xmlui/handle/1794/19638>.
- Reisman, D., Englehardt, S., Eubank, C., Zimmerman, P., & Narayanan, A. (2014). *Cookies that give you away: Evaluating the surveillance implications of web tracking*: Florence, Italy. ACM.
- Ribadu, N. (2007). Cybercrime and commercial fraud: A Nigerian perspective. *Paper presented at the Congress celebrating the Fortieth Annual Session of the UNCITRAL*, Vienna, Austria. July 2007.
- Rice, R. A. (2017). *How to write a literature review*. Retrieved from <https://www.tandfonline.com/doi/abs/10.1080/10511253.2012.730617>
- Rogers. (1975). A protection motivation theory of fear appeals and attitude change¹. *The Journal of Psychology*, *91*(1), 93-114.
- Rogers, K. (2012). Jailbroken: Examining the policy and legal implications of iPhone jailbreaking. *Journal of Technology Law and Policy*.(13)1. University of Pittsburgh, USA.
- Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security*, *2014*(1), 13-15.

- Ross, R. S. (2011). Guide for conducting risk assessments. *NIST Special Publication*, 800-830.
- Sanusi, L. S. (2012). Banking reform and its impact on the Nigerian economy. *CBN Journal of Applied Statistics*, 2(2), 115-122.
- Saunders, Lewis, P., & Thornhill, A. (2009). Understanding research philosophies and approaches. *Research Methods for Business Students*, 4, 106-135.
- Saunders, Lewis, P., & Thornhill, A. (2011). *Research methods for business students*. 5th ed. The University of Surrey, United Kingdom. Pearson Education India.
- Scheidell, M. (2009). Intrusion detection system: Google Patents. Retrieved from <https://patents.google.com/patent/US6405318B1/en>
- Schwab, K. (2016). Navigating the fourth industrial revolution. . *BIZNEWS*. Retrieved from <http://www.biznews.com/wef/davos-2016/01/20/Klaus-schwab-navigating-the-fourth-industrial-revolution/>
- Sekaran, U., & Bougie, R. (2009). *Research Methods of Business-A Skill-Building Approach*.
- Serianu. (2016). *Nigeria cyber security report*. Retrieved from <http://www.serianu.com/downloads/NigeriaCyberSecurityReport2016.pdf>
- Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100.
- Shazmeen, S. F., & Prasad, S. (2012). A practical approach for secure internet banking based on cryptography. *International Journal of Scientific and Research Publications*, 2(12), 1-6.
- Sheu, J.-J., Chu, K.-T., Li, N.-F., & Lee, C.-C. (2017). An efficient incremental learning mechanism for tracking concept drift in spam filtering. *PloS one*, 12(2), e0171518.
- Shumate, T., & Ketel, M. (2014). Bring your own device: Benefits, risks and control techniques. *Paper presented at the Southeastcon 2014, IEEE*. Lexington, KY, USA. November 2014.
- Silvergate, S., & Salner, D. (2011). Smartphones and the Fair Labor Standards Act. *For the Defense—Legal Magazine*, 41-44.

- Sipior, J. C., Bierstaker, J., Chung, Q., & Lee, J. (2017). A bring-your-own-device case for use in the classroom. *Communications of the Association for Information Systems*, 41(1), 10.
- Smith, A. R., Colombi, J. M., & Wirthlin, J. R. (2013). Rapid development: A content analysis comparison of literature and purposive sampling of rapid reaction projects. *Procedia Computer Science*, 16, 475-482.
- Soiferman, L. K. (2010). *Compare and contrast inductive and deductive research approaches*. Online submission. Retrieved from <https://eric.ed.gov/?id=ED542066>
- Soludo, C. C. (2004). Consolidating the Nigerian banking industry to meet the development challenges of the 21st century. *An address delivered to the special meeting of Bankers' Committee-CBN, Abuja*. July 2004.
- Stouffer, K., Falco, J., & Scarfone, K. (2008). NIST SP 800-115: Technical Guide to Information Security Testing and Assessment. *National Institute of Standards and Technology (September, 2008)*.
- Su, K. (2016). *Managing mobile device usage agreement*. Retrieved from www.snowsoftware.com/int/blog/2016/10/06/managing-mobile-device-usage-agreements
- Tambotoh, J. J., & Latuperissa, R. (2014). The application for measuring the maturity level of information technology governance on Indonesian government agencies using COBIT 4.1 Framework. *Intelligent Information Management*. 6(01), 12.
- The Ministry Of Communication Technology. (2012). *National Information and Communication Technology (ICT) Policy*. Retrieved from <http://nitda.gov.ng/wp-content/uploads/2016/06/National-ICT-Policy.pdf>
- Thielens, J. (2013). Why APIs are central to a BYOD security strategy. *Network Security*, 2013(8), 5-6.
- Thilagavathi, M. S., & Saradha, A. (2014). Impact Analysis of Dos & DDos Attacks. *IOSR Journal of Computer Engineering (IOSR-JCE)*. 16(6), 24-33
- Thurrott, P. (2009). *Microsoft Security Essentials Public Beta*. Retrieved from Paul Thurrott's SuperSite for Windows: Retrieval from <https://www.itprotoday.com/windows-server/microsoft-security-essentials-40>

- Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing information systems security: critical success factors and indicators to measure effectiveness. *Paper presented at the International Conference on Information Security*. (pp. 530-545): Berlin, Heidelberg. Springer.
- Treiman, D. J. (2014). *Quantitative data analysis: Doing social research to test ideas*. San Francisco, CA, USA: John Wiley & Sons.
- Trochim, W. M., & Donnelly, J. P. (2001). Research methods knowledge base. Retrieved from <http://www.anatomyfacts.com/research/researchmethodsknowledgebase.pdf>
- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506-517.
- Tuli, P., & Sahu, P. (2013). System monitoring and security using keylogger. *International Journal of Computer Science and Mobile Computing*, 2(3), 106-111.
- Tung, L. (2017). *IoT devices will outnumber the world's population this year for the first time*: ZDNet. Retrieved from <https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/>
- Twinomurinzi, H., & Mawela, T. (2014). Employee perceptions of BYOD in South Africa: Employers are turning a blind eye? *Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT Empowered by Technology*. (p. 126). Centurion, South Africa. ACM.
- University of California Santa Cruz (UCSC). (2015). *Security breach Examples and practices to avoid them*. University of California Santa Cruz. Retrieved from <https://its.ucsc.edu/security/breaches.html>
- Urry, J. (2012). *Sociology beyond societies: Mobilities for the twenty-first century*: Routledge.
- Uz, A. (2014). The effectiveness of remote wipe as a valid defense for enterprises implementing a BYOD policy. Doctoral dissertation.
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, 15(3), 398-405.

- Val, S., Sam, F., & Jim, E. (2014). *Mobile financial services; Raising the bar on customer engagement*. Deloitte University Press.
- Valilai, O. F., & Houshmand, M. (2013). A collaborative and integrated platform to support distributed manufacturing system using a service-oriented approach based on cloud computing paradigm. *Robotics and Computer-Integrated Manufacturing*, 29(1), 110-127.
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3), 190-198.
- Vanderlinde, R., Dexter, S., & Van Braak, J. (2012). School-based ICT policy plans in primary education. *School-based ICT policy planning in a context of curriculum reform*, 145. Doctoral dissertation.
- Vateva-Gurova, T., Luna, J., Pellegrino, G., & Suri, N. (2014). Towards a framework for assessing the feasibility of side-channel attacks in virtualized environments. *Paper presented at the 11th International Conference on Security and Cryptography (SECRYPT)*: Vienna, Austria, August 2014.
- Venkatesh, V, Brown, S A, & Bala, H (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in Information Systems. *MIS Quarterly*, 37(1), 21-54.
- Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science*, 50, 511-516.
- Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science*, 9(6), 479-499.
- Walters, P. (2012). The risks of using portable devices. *Carnegie Mellon University. Produced for US-CERT, a government organization*. Retrieved from <http://www.us-cert.gov>.
- Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer*(12), 52-58.

- Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. *Paper presented at the 11th Consumer Communications and Networking Conference (CCNC): Las Vegas, NV, USA. 2014 IEEE*
- Wilson, J. (2014). *Essentials of business research: A guide to doing your research project*. Thousand Oaks, California: Sage.
- Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine, 48(3)*, 1846-1852.
- Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.
- Wu, X. (2009). SIP on an overlay network. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.707.1759&rep=rep1&type=pdf>
- Xie, M., Han, S., Tian, B., & Parvin, S. (2011). Anomaly detection in wireless sensor networks: A survey. *Journal of Network and Computer Applications, 34(4)*, 1302-1325.
- Yadav, S. K. (2010). *Some problems in symmetric and asymmetric cryptography*. Doctoral dissertation, department of mathematics, Ambedkar University.
- Yang, Liu, H.-M., & Wang, X.-X. (2013). Organization theories: From classical to modern. *Journal of Applied Sciences, 13(21)*, 4470-4476.
- Yang, & Yao, S.-Z. (2009). Risk assessment method of information security based on threat analysis. *Computer Engineering and Applications, 45(3)*, 94-96.
- Yayla, A. A., & Hu, Q. (2014). The effect of board of directors' IT awareness on CIO compensation and firm performance. *Decision Sciences, 45(3)*, 401-436.
- Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management, 44(5)*, 480-491.
- Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security, 55*, 81-99.
- Zhang, S. (2017). Fraud detection on a communication network: Google Patents. Retrieved from <https://patents.google.com/patent/US9729727B1/en>

APPENDIX A: ETHICAL CLEARANCE APPROVAL LETTER



05 June 2019

Ms Lizzy Oluwatoyin Ofusori (214584651)
School of Management, IT & Governance
Westville Campus

Dear Ms Ofusori,

Protocol reference number: HSS/0111/016D

New project title: Three-dimensional security framework for Byod enabled Banking Institutions in Nigeria

Approval Notification – Amendment Application

This letter serves to notify you that your application and request for an amendment received on 30 May 2019 has now been approved as follows:

- Change in Title

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form; Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for period of 3 years from the date of original issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful completion of your research protocol.

Yours faithfully

.....
Dr Shamila Naidoo (Deputy Chair)

/ms

Cc Supervisor: Dr Rontala Subramaniam Prabhakar
cc Academic Leader Research: Professor Brian McArthur
cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee

Dr Rosemary Sibanda (Chair)

Westville Campus, Govan Mbeki Building

Postal Address: Private Bag X54001, Durban 4000

Telephone: +27 (0) 31 260 3587/8350/4557 Facsimile: +27 (0) 31 260 4609 Email: ximbap@ukzn.ac.za / shvmanm@ukzn.ac.za / mohung@ukzn.ac.za

Website: www.ukzn.ac.za



100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville

APPENDIX B: QUESTIONNAIRE FOR THREAT IDENTIFICATION



UKZN HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE (HSSREC) APPLICATION FOR ETHICS APPROVAL

Researcher: Lizzy Oluwatoyin Ofusori, +27 621623285

Supervisor: DR. Prabhakar Rontala Subramaniam, +27 33 260 5643

Research Office: Mariette Synman, +27 312608350

Greetings,

My name is Lizzy Oluwatoyin Ofusori a Doctoral student in Information System & Technology at University of KwaZulu-Natal, Durban, South Africa (lizzyofusori@yahoo.co.uk).

You are invited to participate in a study that involves investigating the security threats associated with BYOT trends in the financial institutions, specifically with regards to vulnerabilities and threats against portable mobile technology used by employees of the Nigeria banking sector. The aim and purpose of this research is to develop a security framework that could protect the bank from security threats associated with mobile devices such as smartphones, laptop, and tablets. This study collects data from 360 participants employed in four commercial banks in Lagos State, Nigeria. The questionnaire will be distributed to all employees of the selected bank branches in Lagos State. It requires at most 20minutes of your time to complete this questionnaire.

I hope that the study will be of great benefit to the selected banks as it will provide a basis through which the banks can enhance security while encouraging the employees to use their mobile devices in executing their official duties. In addition, I hope the study will contribute towards policy development discourses to extrapolate new ways of curbing vulnerabilities and threats associated mobile devices.

In the event of any problems or concerns or questions you may contact the researcher at lizzyofusori@yahoo.co.uk or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office, Westville Campus

Govan Mbeki Building

Private Bag X 54001

Durban 4000 KwaZulu-Natal, SOUTH AFRICA

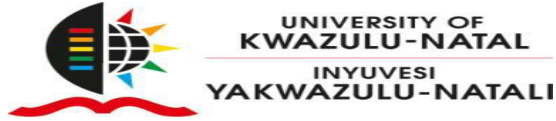
Tel: 27 31 2604557- Fax: 27 31 2604609

E-mail: HSSREC@ukzn.ac.za

Your participation in the study is voluntary and by participating, you are granting the researcher permission to use your responses. You may refuse to participate or withdraw from the study at any time with no negative consequence. There will be no monetary gain from participating in the study. **Your anonymity** will be maintained by the researcher and the School of Management, I.T. & Governance and your responses will not be used for other purpose out of this study. All data, both electronic and hard copy will be securely stored during the period of study and archived for 5 years. After this time, all data will be destroyed

Sincerely

Miss Ofusori Lizzy Oluwatoyin.



University of KwaZulu-Natal, Durban, South Africa

School of Management, IT and Governance

Researcher: Lizzy Oluwatoyin Ofusori, +27621623285

Supervisor: DR. Prabhakar Rontala Subramaniam, +2733 260 5643

Research Office: Mariette Synman, +27312608350

CONSENT TO PARTICIPATE

I have read the informed consent letter shown above and hereby confirm that I understand the content of this document and the nature of the research project, and I consent to participate in the research project.

I declare that my participation in this study is voluntary and that I may withdraw at any time.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher at lizzyofusori@yahoo.co.uk.

I hereby provide consent to participate in the questionnaire: YES / NO

Signature of Participant

Date

Instruction to respondents

- Please sign the letter of informed consent, giving me permission to use your responses.
- Please be honest in your responses.
- Please tick the appropriate option

This questionnaire is concerned about collecting data to design a security framework for banking sector in Lagos State, Nigeria in support of Bring your own technology (BYOT). BYOT is a trend that allows employees to bring their personal mobile devices to the work place. They have the freedom to use mobile devices (such as laptops, tablets or smartphones) for work related purpose.

Given below are the descriptions of different types of known threats

- **Cross-Site Request Forgery (CSRF)** is a type of malicious attack of a website where unauthorized commands are transmitted from a user that the **website** trusts.
- **Data breach** can be defined as a form of security breach in which confidential data is stolen by an unauthorized individual.
- **Data interception** is the obstruction of data transmission to and from the device and remotely altering the messages
- **Denial-of-service (DoS) attack** is an attempt to make a machine or network resource unavailable to its intended users, such as suspending or interrupting services of a host connected to the internet.
- **Eavesdropping attack** is an unauthorized interception of a private communication such as phone call, instant messaging or videoconference
- **Identity theft** occurs when an individual pretends to be another person in order to retrieve vital information
- **Location tracking** occurs when a software application is installed on user's mobile device in order to obtain the device or data location
- **Malware/spyware attack** can be described as any software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems
- **Man in the middle attack** happens when attackers position himself/herself as a relay/proxy into a communication between parties or system
- **Phishing** can be described as an attempt to obtain sensitive information such as credit card details, usernames and passwords often for malicious reasons.
- **Spamming** can be described as a fraudulent practice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers online.
- **Virus attack** can be described as a malicious software that are downloaded and it replicates by making copies of itself
- **Worm:** It is a software that can copy itself from one PC to another without human interaction. A worm can send copies of itself to every contact in your e-mail or contact address books.

Finally, this questionnaire also aims at exploring any new threats that may emanate from regular work practice. The respondent are requested to contribute about any new threats by describing sufficiently in the appropriate space provided (others (specify).....)

QUESTIONNAIRE

SECTION A: Demographic Data

1. Gender

Male	Female

2. Marital Status

Single	Married	Divorced/Separated	Widowed

3. Age group

Up to 20 years	21-25years	26-30years	31-35years	36-40years	>40years

4. Department

Employees					Executives	
Operations	Marketing	Human Resource	Customer service	Others (specify)	ICT	Executive Managers

5. Educational Qualification

School Cert.	National Diploma	Higher National Diploma/ Bachelor of Science	Master Degree	PhD

6. Employment Status

Contract/Temporal	Probation	Permanent	Outsourced (3 rd party)	Others (specify)

7. Work Experience

Up to 5years	6-10years	11-15years	16-20years	>20years

Section B: General practice

This section focuses on the general practices of banks' employees in relation to using mobile devices

Note: The mobile devices referred to in this questionnaire include those owned by yourself or by the bank

Q1. Which of the following mobile device(s) do you to use and for what purpose? **Please tick all that apply**

		Work purposes only	Personal purposes only	Work and personal purposes	Do not use
1.1	Smartphone(s)				
1.2	Laptop(s)				
1.3	Tablet(s)				
1.4	Other devices (specify) _____				

Q2. From which of the following places does the bank allow you to use **each** mobile device for work purposes?

		Smartphone(s)	Laptop(s)	Tablet(s)	Other devices
2.1	Home				
2.2	Office				
2.3	Public place (e.g. hotel, airport)				

Q3. For how long have you been using **each** mobile device?

		Up to 6 months	Up to 1year	Up to 2years	Up to 3years	More than 3years
3.1	Smartphone(s)					
3.2	Laptop(s)					
3.3	Tablet(s)					
3.4	Other devices					

Section C: Technical

Q4. Indicate whether you use the following methods to connect **each** mobile device to the internet

	Connection methods	Smartphone(s)	Laptop(s)	Tablet(s)	Other devices
4.1	Office wireless connection				
4.2	Home wireless connection				
4.3	Office wired connection				
4.4	Home wired connection				
4.5	Mobile router or USB modem				
4.6	Mobile network				

Q5. Which of the following practices do you use to configure **each** mobile device to connect to wireless network?

	Practice	Smartphone(s)	Laptop(s)	Tablet(s)	Other devices
5.1	Manually				
5.2	Automatically				

Q6. Do you save your login credentials on any of your devices?

Yes	No

Q7. If answer to Q6 is Yes, how do you manage the saved details on **each** device

		Smartphone(s)	Laptop(s)	Tablet(s)	Other devices
7.1	I allow browsers to save the login credentials				
7.2	I allow security software on my device to manage the credentials				
7.3	I write them in text files and save on the device				

Q8. For **each** device, indicate the type of applications (apps) you install (**Tick all that apply**)

		Smartphone(s)	Laptop(s)	Tablet(s)	Other devices
8.1	Instant messaging (eg				
8.2	Social media (e.g. Facebook)				
8.3	News/magazines (e.g. Weather)				
8.4	Entertainment (e.g. Video,				
8.5	Travel related (Google map,				
8.6	Mobile banking				

8.7	Security software (Anti-virus)				
8.8	Video conference (e.g. Skype)				
8.9	Storage drive (e.g. Google)				
8.10	Shopping (e.g. eBay)				
8.11	E-mail (e.g. yahoo mail, Gmail)				
8.12	Others				

Q9. Do you update any of your mobile devices operating system and applications regularly?

Yes	No

Q10. If the answer to Q9 is No, what are your reasons for not updating your mobile device(s)?

		Yes	No
10.1	I do not receive update notifications		
10.2	I do not pay attention to update notifications		
10.3	The manufacturer of the operating system no longer supports the device and has stopped sending update notifications		

Q11. If the answer to Q9 is Yes, from which network do you update your mobile device(s)?

		Always	Sometimes	Never
11.1	Office network			
11.2	Home network			
11.3	Public network (e.g. restaurant, airport)			
11.4	Mobile network			

Q12. For each device, indicate where you save work documents

		Smartphone(s)	Laptop(s)	Tablet(s)	Other devices
12.1	Office owned server				
12.2	Office hired cloud storage				
12.3	Personal hired cloud storage				

12.4	A free cloud storage (eg dropbox)				
12.5	Personal owned devices (e.g. external drive, laptop)				
12.6	Internal memory of the device				

Q13. Do any of your mobile devices come with preinstalled security software (e.g. Antivirus)?

Yes	No	Don't know

Q14. If the answer to Q13 is Yes, do you use the preinstalled security software on any device?

Yes	No

Q15. Indicate whether the following security measures are in use for any of your mobile devices

		Yes	No	Not sure
15.1	Password authentication			
15.2	Biometric authentication			
15.3	Anti-virus			
15.4	Anti-Malware			
15.5	Firewall			
15.6	Encryption			
15.7	Proxy server			
15.8	Hardware token			

Q16. In your experience, are you aware of the following incidences in your bank?

		Yes	No
16.1	Transfer of money from a dormant account to personal account		
16.2	Transfer of money from a general ledger account to a fictitious account		
16.3	The use of a customer identity to create a credit card		
16.4	The use of customers' bank cards retained by the ATM machine for cash withdrawal by employees'		
16.5	Customers' bank cards (debit or credit card) cloned by employees		

16.6	Employees' setting up online banking for customers without their knowledge		
16.7	Employees credentials stolen by hackers and used to access the bank's network		

Section D: Social

Q17. Indicate your usage of the following social interactive networks

		Work purposes only	Personal purposes only	Work and personal purposes	Do not use
17.1	Instant messaging (e.g. WhatsApp, BBM)				
17.2	Social media (Facebook, Twitter, LinkedIn)				
17.3	Video conference (e.g. Skype)				
17.4	E-mail (e.g. yahoo mail, Gmail)				
17.5	Entertainment (e.g. video, music,				
17.6	Shopping (e.g. eBay)				
17.7	Mobile banking				
17.8	Travel related (e.g. Google map, GPS, Uber)				

Q18. From the messages you receive on the social media listed in Q17, do you ever click on any of the following? **(Tick all that apply)**

		Yes	No
18.1	Links (e.g. shortened links)		
18.2	Images (e.g. pictures)		
18.3	Advertisement		
18.4	Videos/Audios		
18.5	Games		

Q19. What type of confidential document(s) do you attach to e-mails or instant messages? **(Tick all that apply)**

		Yes	No
19.1	Customers bank statement		
19.2	Customers credentials details (e.g. phone numbers)		
19.3	Employees expense report		
19.4	Customer deposit slip		
19.5	Payroll documents		
19.6	Auditor's report		
19.7	Minutes of meetings		

19.8	Bank financial statements		
19.9	General ledger		

Q20. In your experience, are you aware of the following incidences in your bank? (**Tick all that apply**)

		Yes	No
20.1	Unauthorized access to the bank's network by an employee who no longer works for the bank		
20.2	Stealing of co-employee login credentials by an employee who logs in with the credentials, visiting questionable websites in order to discredit the co-employee		
20.3	A contract employee revealing confidential information (e.g. bank financial statement) to an outsider in return for some money/reward		
20.4	Misuse of data by an outsourced employee		

Q21. For **each** of the following security threats, please indicate your level of awareness

		I know about it	Heard about it, but don't know what it's all about	Never heard about it
21.1	Cross-Site Request Forgery			
21.2	Data interception			
21.3	Denial of service (DoS)			
21.4	Eavesdropping			
21.5	Hacking			
21.6	Location tracking			
21.7	Malware/spyware/virus/worm			
21.8	Phishing			

Q22. If you know about the security threats listed in Q21, indicate what precautions you took to avoid or curb them (**Tick all that apply**)

		Precautions										
	DON'T KNOW ABOUT THIS THREAT	Strong Password	Hardware authentication	Regular update of software and apps	Anti-malware/virus	Backup	Encryption	Firewall	turn off location app	I don't enter sensitive data on a site that doesn't begin with 'Https' or a lock icon	I don't respond to unsolicited e-mails	I check the web address (URL) before clicking site

22.1	Cross-Site Request Forgery (CSRF)												
22.2	Data interception												
22.3	Denial of service												
22.4	Eavesdropping												
22.5	Hacking												
22.6	Location tracking												
22.7	Malware/spyware/vir												
22.8	Phishing												

Q23. With whom do you share your password? (Tick all that apply)

23.1 Colleague(s)	23.2 Family /Friend(s)	23.3 Nobody

Section E: Mobility

Q24. Indicate whether you use the following methods to prepare your mobile device(s) for disposal

		Yes	No	Not sure
24.1	Permanently delete data from the recycle bin to get rid of critical information			
24.2	Format the storage devices to get rid of critical information			
24.3	Replace the hard drive of the device to get rid of the critical information			
24.4	Reset the devices to factory default settings to get rid of the critical information			

Q25. Indicate whether you use the following methods to dispose of your obsolete/faulty device(s)

		Yes	No	Not sure
25.1	Put it up for sale			
25.2	Give it to family/friends			
25.3	Throw away the faulty device			
25.4	Destroy the faulty device			

Q26. With whom do you normally share your mobile device(s)? (Tick all that apply)

26.1 Colleague(s)	26.2 Family/Friend(s)	26.3 Nobody

Q27. Do you use a pre-owned mobile device(s)?

Yes	No

Section F: Security threats

Q28 Please indicate whether you have ever experienced any the following security threats on your mobile device

		Yes	No	Not sure
28.1	Unauthorized modification of confidential information (e.g. customer's bank statement)			
28.2	Unauthorized login into your storage account (e.g. Office server,			
28.3	Unauthorized access to your social interactive network (e.g. Facebook, WhatsApp, BBM, WeChat)			
28.4	Unauthorized access to your bank account			
28.5	Unauthorized interception of private communication such as a phone call, instant message e.t.c.			
28.6	Unavailable network during the cause of interaction			
28.7	Personal information on your mobile device such as private photo, login credentials were used without your knowledge			
28.8	Data leakage (Confidential data were sold out to the bank's			
28.9	Malicious messages were sent to your contact list without your			
28.10	Confidential information were deleted without your knowledge (e.g. customer credential details)			
28.11	Software keeps making copies of itself on your device			
28.12	You saw a number in your dialing list that you haven't dialed			
28.13	You received messages that you have won a prize and should call a number to redeem the prize			
28.14	You received messages that you have won a prize and should click a link to redeem the prize			
28.15	You received e-mail request to update your personal information (e.g. login credentials)			
28.16	You received an access request to device resources as part of terms & conditions to install			

Thank you for participating

APPENDIX C: INTERVIEW FOR ICT DEPARTMENT PERSONNEL (THREAT IDENTIFICATION)



UKZN HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE (HSSREC) APPLICATION FOR ETHICS APPROVAL

Researcher: Lizzy Oluwatoyin Ofusori, +27621623285

Supervisor: DR. Prabhakar Rontala Subramaniam, +2733 260 5643

Research Office: Mariette Synman, +27312608350

Greetings,

My name is Lizzy Oluwatoyin Ofusori a Doctoral student in Information System & Technology at University of KwaZulu-Natal, Durban, South Africa (lizzyofusori@yahoo.co.uk).

You are invited to participate in a study that involves investigating the security threats associated with BYOT trends in the financial institutions, specifically with regards to vulnerabilities and threats against portable mobile technology used by employees of the Nigeria banking sector. The aim and purpose of this research is to develop a security framework that could protect the bank from security threats associated with mobile devices such as smartphones, laptop, and tablets. The study is expected to include 8 respondents (2 each) from the four participating banks in Lagos State, Nigeria. The interview will be carried out with the IT Personnel across the selected banks in Lagos State. The duration of your participation is expected to be 20minutes.

The interview will be recorded and I hope that the study will be of great benefit to the selected banks as it will provide a basis through which the banks can enhance security while encouraging the employees to use their mobile devices in executing their duties. In addition, I hope the study will contribute towards policy development discourses to extrapolate new ways of curbing vulnerabilities and threats associated mobile devices.

In the event of any problems or concerns/questions you may contact the researcher at lizzyofusori@yahoo.co.uk or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office, Westville Campus

Govan Mbeki Building

Private Bag X 54001

Durban 4000 KwaZulu-Natal, SOUTH AFRICA

Tel: 27 31 2604557- Fax: 27 31 2604609

E-mail: HSSREC@ukzn.ac.za

Your participation in the study is voluntary and by participating, you are granting the researcher permission to use your responses. You may refuse to participate or withdraw from the study at any time with no negative consequence. There will be no monetary gain from participating in the study. **Your anonymity** will be maintained by the researcher and the School of Management, I.T. & Governance and your responses will not be used for other purpose out of this study. All data, both electronic and hard copy will be securely stored during the study and archived for 5 years. After this time, all data will be destroyed

Sincerely

Miss Ofusori Lizzy Oluwatoyin.



University of KwaZulu-Natal, Durban, South Africa

School of Management, IT and Governance

Researcher: Lizzy Oluwatoyin Ofusori, +27621623285

Supervisor: DR. Prabhakar Rontala Subramaniam, +2733 260 5643

Research Office: Mariette Synman, +27312608350

CONSENT TO PARTICIPATE

I have read the informed consent letter shown above and hereby confirm that I understand the content of this document and the nature of the research project, and I consent to participating in the research project.

I have been informed of the audio record of the interview.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher at lizzyofusori@yahoo.co.uk.

I hereby provide consent to participate in the Audio-record interview

YES / NO

Signature of Participant

Date

Instructions:

- Please sign the letter of informed consent, giving me permission to use your responses.
- Please be honest in your responses.

SECURITY FRAMEWORK FOR BANKING SECTOR IN LAGOS STATE OF NIGERIA

Short explanation on technical terms for reference

BYOT (Bring your own Technology) is a trend that allows employees to bring their personal mobile devices to the work place. They have the freedom to use mobile devices (such as laptops, tablets or smartphones) for work related purpose.

Technical System: In this study the technical system represents all categories of BYOT hardware and software technology used for work related purpose.

Social System: The social system refers to employees' attitude, value/norms and their level of security awareness to the security threats posed by their mobile devices.

Mobility System: Mobility system refers to how employees or clients perform banking while travelling via their portable devices such as laptops, tablets or smartphones.

Interview questions for IT personnel

Technical

1. What type of internet connection does the bank uses?
2. How does the bank connect to other branches of the bank?
3. Who maintains the network?
4. Do you register users' mobile devices in your database for knowledge?
5. Do you restrict the number of registration for mobile devices?
6. Do you keep database of users' activities on the network?
7. Is the database accessible to other branches of the bank?
8. How do you manage employees' authentication to operational services? e.g client account
9. Do you allow employees personal devices (laptops, smartphones, and tablets) to access operational service?
10. What are the existing security measures used to secure the bank's network?
11. Have you experienced or received any security threats regarding employees' mobile device? Please share
12. How are these security threats mitigated?
13. What are the difficulties you experienced in mitigating these security threats? Please share
14. Which aspect of the bank security will you like to focus more?

Social

15. How do you manage/control employees' access to social media (e.g. facebook, twitter, WhatsApp) for both official and personal purpose? Please elaborate on each purpose
16. Where does the employees' backup mobile device data that contains work documents?
17. What are the security threats faced due to non-compliance to security policies by employees

Mobility

18. Do you allow employees' to share mobile device used for official purpose with others (e.g. family/friends/colleagues)?
19. Do you allow employees' to use pre-owned mobile devices?
20. How do you address security threats arising from employees' sharing their mobile devices with family/friends/colleagues?
21. How do you address security issues related to using pre-owned mobile device by employees?
22. Are you aware of lost/stolen mobile devices by employees (reported, unreported, recovered or unrecovered)?
23. How do you address security issues that can be caused by lost/stolen device?
24. How do you address security threats arising from employees' disposing their mobile devices?
25. How do you address security threats arising from employees' connecting mobile devices to public network to respond to bank's messages?

Thank you for participating

APPENDIX D: INTERVIEW FOR EXECUTIVE MANAGERS (THREAT IDENTIFICATION)



UKZN HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE (HSSREC) APPLICATION FOR ETHICS APPROVAL

Researcher: Lizzy Oluwatoyin Ofusori, +27621623285

Supervisor: DR. Prabhakar Rontala Subramaniam, +2733 260 5643

Research Office: Mariette Synman, +27312608350

Greetings,

My name is Lizzy Oluwatoyin Ofusori a Doctoral student in Information System & Technology at University of KwaZulu-Natal, Durban, South Africa (lizzyofusori@yahoo.co.uk).

You are invited to participate in a study that involves investigating the security threats associated with BYOT trends in the financial institutions, specifically with regards to vulnerabilities and threats against portable mobile technology used by employees of the Nigeria banking sector. The aim and purpose of this research is to develop a security framework that could protect the bank from security threats associated with mobile devices such as smartphones, laptop, and tablets. The study is expected to include 4 respondents (1 each) from the four participating banks in Lagos State, Nigeria. The interview will be carried out with the Executive Managers across the selected banks in Lagos State. The duration of your participation is expected to be 20minutes.

The interview will be recorded and I hope that the study will be of great benefit to the selected banks as it will provide a basis through which the bank can enhance security while encouraging the employees to use their mobile devices in executing their duties. In addition, I hope the study will contribute towards policy development discourses to extrapolate new ways of curbing vulnerabilities and threats associated mobile devices.

In the event of any problems or concerns or questions you may contact the researcher at lizzyofusori@yahoo.co.uk or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office, Westville Campus
Govan Mbeki Building
Private Bag X 54001
Durban 4000 KwaZulu-Natal, SOUTH AFRICA
Tel: 27 31 2604557- Fax: 27 31 2604609
E-mail: HSSREC@ukzn.ac.za

Your participation in the study is voluntary and by participating, you are granting the researcher permission to use your responses. You may refuse to participate or withdraw from the study at any time with no negative consequence. There will be no monetary gain from participating in the study. **Your anonymity** will be maintained by the researcher and the School of Management, I.T. & Governance and your responses will not be used for other purpose out of this study. All data, both electronic and hard copy will be securely stored during the study and archived for 5 years. After this time, all data will be destroyed

Sincerely
Miss Ofusori Lizzy Oluwatoyin.



University of KwaZulu-Natal, Durban, South Africa

School of Management, IT and Governance

Researcher: Lizzy Oluwatoyin Ofusori, +27621623285

Supervisor: DR. Prabhakar Rontala Subramaniam, +2733 260 5643

Research Office: Mariette Synman, +27312608350

CONSENT TO PARTICIPATE

I have read the informed consent letter shown above and hereby confirm that I understand the content of this document and the nature of the research project, and I consent to participating in the research project.

I have been informed of the audio record of the interview.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher at lizzyofusori@yahoo.co.uk.

I hereby provide consent to participate in the Audio-record interview

YES / NO

Signature of Participant

Date

Instructions:

- Please sign the letter of informed consent, giving me permission to use your responses.
- Please be honest in your responses.

SECURITY FRAMEWORK FOR BANKING SECTOR IN LAGOS STATE OF NIGERIA

Short explanation on technical terms for reference

BYOT (Bring your own Technology) is a trend that allows employees to bring their personal mobile devices to the work place. They have the freedom to use mobile devices (such as laptops, tablets or smartphones) for work related purpose.

Technical System: In this study the technical system represents all categories of BYOT hardware and software technology used for work related purpose.

Social System: The social system refers to employees' attitude, value/norms and their level of security awareness to the security threats posed by their mobile devices.

Mobility System: Mobility system refers to how employees or clients perform banking while travelling via their portable devices such as laptops, tablets or smartphones.

Interview questions for Executive Managers

Technical

1. Do you have a definite policy that support the use of BYOT devices (e.g. smartphones, laptops, tablets) in handling official duties?
2. What are your policies about using mobile device with respect to the following
 - a. Acquisition (How do employees acquire their mobile devices)
 - b. Monitoring (App usage, regular update, office e-mail usage, location tracking)
 - c. Maintenance (e.g. does the bank accept to repair employees personal device?)
3. Do you have any specific operating system for mobile devices used by employees?
4. What are the procedures that regulate access of employees' mobile device to the bank's infrastructure (e.g. server)?
5. Are there limit to what employees' personal device can do on the network?
6. Are there ways you monitor employees' personal device on the network? Please share

Social

7. Do you provide security awareness programs (e.g. training) that emphasize bank's policy and procedures?
8. How do you ensure that employees' comply with the security policies?
9. How often do you review your security policies
10. What is the regulation that guides the interaction with the following types of employees' with the bank's infrastructure?

- a. Previous employee
- b. Disgruntled employee
- c. Temporary/contract employee
- d. Outsourced employees'

11. Do you have any budget constraint in developing a security framework?

Mobility

12. How do you handle employees' lost/stolen devices

13. How do you handle faulty mobile devices?

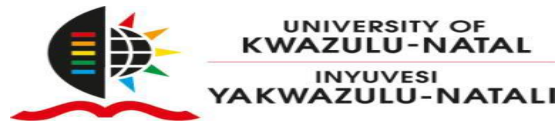
14. What are the procedures that guides employees' disposal of mobile devices

15. Are there rules that guides employees' sharing mobile devices? Please share

16. Are you willing to share threats related data to secure banking system with other banks?

Thank you for participating

APPENDIX E: EVALUATION QUESTIONNAIRE



UKZN HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE (HSSREC) APPLICATION FOR ETHICS APPROVAL

Researcher: Lizzy Oluwatoyin Ofusori, +27 621623285

Supervisor: Dr. Prabhakar Rontala Subramaniam, +27 33 260 5643

Research Office: Mariette Synman, +27 312608350

Greetings,

My name is Lizzy Oluwatoyin Ofusori, a Doctoral student in Information System & Technology at the University of KwaZulu-Natal, Durban, South Africa (lizzyofusori@yahoo.co.uk).

You are invited to participate in a study that involves investigating the security threats associated with BYOD trends in the financial institutions, specifically with regards to vulnerabilities and threats against portable mobile technology used by employees of the Nigerian banking sector.

The data you have already contributed to this study through an interview process has been used to develop a proposed security framework. In order to assess the suitability of using the framework in your banks, the researcher has come up with some evaluation questions that can accomplish this objective. It requires no more than 10 minutes of your time to complete this questionnaire.

I hope that the study will be of great benefit to the selected banks as it will provide a basis which the banks can enhance security while encouraging the employees to use their mobile devices in executing their official duties. In addition, I hope the study will contribute towards policy development discourses to extrapolate new ways of curbing vulnerabilities and threats associated with mobile devices.

In the event of any problems, concerns or questions you may have, please feel free to contact the researcher at lizzyofusori@yahoo.co.uk or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office, Westville Campus

Govan Mbeki Building

Private Bag X 54001

Durban 4000 KwaZulu-Natal, SOUTH AFRICA

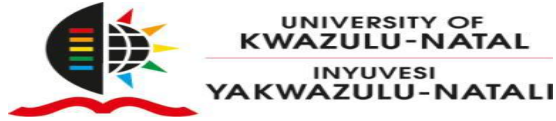
Tel: 27 31 2604557- Fax: 27 31 2604609

E-mail: HSSREC@ukzn.ac.za

Your participation in the study is voluntary and by participating, you are granting the researcher permission to use your responses. You may refuse to participate or withdraw from the study at any time with no negative consequences. There will be no monetary incentive to participate in the study. **Your anonymity** will be assured by the researcher and the School of Management, I.T. & Governance and your responses will not be used for purposes other than for that of this study. All data, both electronic and hard copy will be securely stored during the period of study and archived for 5 years. After this time, all data will be destroyed

Sincerely

Miss Ofusori Lizzy Oluwatoyin.



University of KwaZulu-Natal, Durban, South Africa
School of Management, IT and Governance

Researcher: Lizzy Oluwatoyin Ofusori, +27621623285

Supervisor: Dr.. Prabhakar Rontala Subramaniam, +2733 260 5643

Research Office: Mariette Synman, +27312608350

CONSENT TO PARTICIPATE

I have read the informed consent letter and hereby confirm that I understand the content of this document and the nature of the research project, and I consent to participate in this project.

I declare that my participation in this study is voluntary and that I may withdraw at any time.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher at lizzyofusori@yahoo.co.uk.

I hereby indicate my willingness to participate in answering the questionnaire: YES / NO

Signature of Participant

Date

Instruction to respondents

- Please sign the letter of informed consent, giving me permission to use your responses.
- Please be honest in your responses.
- Please tick the appropriate options

EVALUATION QUESTIONS: These questions require of you to mark the option that best suits your opinion with an ‘X’, in accordance to the scale provided. The following rating scale applies to questions 1 to 4 only.

Rating scale:	
Strongly Disagree:	1
Disagree:	2
Slightly disagree:	3
Slightly Agree:	4
Agree:	5
Strongly Agree:	6

Please indicate how you would rate the proposed framework in relation to the following criteria. The framework:

1	Appropriateness	1	2	3	4	5	6
1.1	Is aligned with the policies and strategies of the bank						
1.2	Enhances the effectiveness of the bank’s data security.						
1.3	Could contribute towards the efficiency of bank operations						
2	Adequacy						
2.1	Could address all the technical threats identified.						
2.2	Could address all the social threats identified.						
2.3	Could address all the mobility threats identified.						
3	Feasibility						
3.1	Could be cost-effective						
3.2	Could be implemented within a short period of time						
3.3	Could be implemented with the available resources of the bank.						
4	Flexibility						
4.1	Could be easily adopted with changing policies.						
4.2	Could be adopted for mitigating security threats within different branches of the bank.						
4.3	Could be adopted for mitigating security threats across different banks.						

5. Intention to use

Please indicate the willingness of your bank to use the framework.

		As it is	With changes
5.1	Willing to implement the framework		

		Immediately	Near future
5.2	Willing to adopt the framework		

		Difficult	Easy
5.3	Use of framework by bank employees' could be		

NB: 'Difficult' requires extensive training, while 'Easy' requires little or no training

6. Suggestions for Improvement

6.1 If your response to 5.1 is 'with changes', what changes you suggest?

.....

6.2 If your response to 5.2 is 'near future', provide reasons

.....

6.3 If your response to 5.3 is 'difficult', provide suggestions for improvement.

.....

6.4 Recommend consideration of the threats and solutions that are not considered in the framework.

.....

APPENDIX F: STATISTICIAN LETTER

Gill Hendry B.Sc. (Hons), M.Sc. (Wits), PhD (UKZN)
Mathematical and Statistical Services

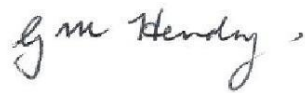
Cell: 083 300 9896
email : hendryfam@telkomsa.net

12 February 2018

Re: Assistance with statistical aspects of the study

Please be advised that I have assisted Lizzy Ofusori (Student number 214584651), who is presently studying for a PhD Information Systems and Technology in the School of Management, IT and Governance at UKZN, with the questionnaire validation and data analysis for her study.

Yours sincerely



Gill Hendry (Dr)

APPENDIX G: DECLARATION OF EDITING AND TRANSLATION SERVICES

Editing and Translation Services

8 Weymouth Place

Beethoven Avenue

Walmer Heights

Port Elizabeth

6070

Mobile: 083 415 4570

E-mail: renvandm@gmail.com

Renée van der Merwe

B A Hons (Applied Linguistics)

SATI Accredited (1998)

14 December 2018

Dear Dr Subramaniam

This serves to confirm that the thesis by Oluwatoyin Lizzy Ofusori has been submitted to me for language editing, excepting for the Appendices as per agreement.

While I have suggested various changes, I cannot guarantee that these have been implemented nor can I take responsibility for any other subsequent changes or additions that may have been made.

Yours faithfully

