UNIVERSITY OF KWAZULU-NATAL

THE EFFECTS OF SECURITY PROTOCOLS ON CYBERCRIME AT AHMADU BELLO UNIVERSITY, ZARIA, NIGERIA

By

Bukhari Badamasi
212560983

A dissertation submitted in fulfillment of the requirement for the degree of Master of Commerce

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

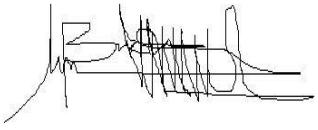
Supervisor: **Prof. Manoj S. Maharaj**
Co-supervisor: **Mr. Nurudeen Ajayi**

2018

DECLARATION

I, Bukhari Badamasi, declare that

i. The research reported in this dissertation, except where otherwise indicated, is my original research.
ii. This dissertation has not been submitted for any degree or examination at any other university.
iii. This dissertation does not contain other person's data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
iv. This dissertation does not contain other person's writing, unless specifically acknowledged as being sourced from other researchers.
   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. This dissertation does not contain text, graphics or tables which have been pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation and in the references sections.

Signed: 

Date: 14th August, 2018

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to Allah (S.W.A), who gave me the wisdom, power and strength to carry out this study.

I would like to thank all those who contributed to this study. I would not have managed to complete this study without their constant support, help and guidance.

First is Professor Manoj Maharaj, my supervisor, for his professional guidance. Then, Mr. Nurudeen Ajayi, my co-supervisor, for his dedication, diligence, guidance, encouragement, constant support and excellent mentoring. They both always wanted the best from me and believed I could do better. Their inspirational motivation and energy kept me going throughout the duration of the study.

The School of Management, Information Technology and Governance staff, Academic leaders, Professor Brian McArthur and Professor Irene Govender, Dr. Mutina, Dr. Van Niekerk, for their valuable comments on the proposal and questionnaire.

The Director of the Institute of Computer and Information Communication Technology at Ahmadu Bello University, Zaria, Nigeria, Professor Sahalu Junaidu, Yusuf Abdullahi, Network Infrastructure and Security for his time to participate in the interview schedule.

The staff at ICICT, Ahmadu Bello University, Zaria, who filled out the questionnaire for this study, I thank you all.

My late mother and father thank you for being loving, caring and supportive parents. Thank you for your love, patience and respect as well as belief in my abilities, may ***your soul rest in perfect peace*** **and may Allah (S.W.A) grant you Jannatul-Firdaus, Ameen thumma ameen.**

My brothers, who never gave up on me and supported me when I was going through hardship, your love and support was more than enough to see me overcome those challenges without seeking professional help. Salisu Baadamasi Mu'azu, Dayyabu Badamasi Mu'azu, Mustapha (late) Badamasi Mu'azu, Mrs. Fatima Badamasi Mu'azu, Mrs. Amina Badamasi Mu'azu and all my other family members. Thank you for everything, more especially your moral support.

My beloved wives, Jamila Mahmood Liman and Ruqayya Abdullahi Muhammad thank you for your support and understanding throughout the period of this work (*I love you all dearest and beloved wives*).

My daughters and son, Maryam Bukhari Badamasi, Badamasi (Abul-khair) Bukhari Badamasi, Khadijat Bukhari Badamasi and Aishat Bukhari Badamasi thank you for your patience during this study.

Lastly, everyone who contributed to the study physically or virtually, your valuable contribution is much appreciated.

DEDICATION

This dissertation is dedicated to my dearest father and mother (the late), who will always have a special place in my heart.

My bothers (Salisu and Dayyabu).

My wives (Jamila and Ruqayya) and three little children (Maryam, Badamasi ‘Abul-khair’, Khadijat ‘Siyama’ and Aishat ‘Humaira’), who will always be my role models and their values, dreams and wisdom will always live through me.

LIST OF ACRONYMS

ABU	Ahmadu Bello University
ACL	Access Control List
APT	Advanced Persistent Threat
ATM	Automatic Teller Machine
CA	Certificate Authority
CASS	Computing and Academic Support Services
CPU	Central Processing Unit
CDS	Cross Domain Solution
CISCO	Computer Information System Company
CIS	Computerised Information System
DDoS	Distributed Denial of Service
DMZ	De-Militarized Zones
DNS	Domain Name System
DoS	Denial of Service
EFT	Electronic Fund Transfer
HTTP	HyperText Transfer Protocol
ICT	Information and Communications Technology
ICICT	Institute of Computer and Information Communication Technology
IDS	Intrusion Detection Systems

ID	Identification
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security
IRC	Internet Relay Chat
IS	Information System
ISP	Internet Service Provider
ISO	Information Security Officer
IT	Information Technology
ITA	Information Technology Academy
IOS	International Organisation for Standardisation
MAC	Media Access Control
MIS	Management Information System
NDIC	Nigerian Deposit Insurance Corporation
NIS	Network Security and Infrastructure
NIST	National Institute for Standards and Technology
OS	Operating System
PC	Personal Computer
PTT	University of Pittsburg
PII	Personnel Identifiable Information

PIK	Public Key Infrastructure
POPI	Protection of Personal Information
PoS	Point of Sale
RAM	Random Access Memory
RAT	Remote Administration Tool
RAS	Remote Access Services
R&D	Research and Development
SDU	Software Development Unit
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPSS	Special Package for Social Sciences
SSN	Social Security Number
SSH	Secure Shell
SSL	Secure Socket Layer
SQL	Structured Query Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
WWW	World Wide Web

ABSTRACT

The use of Information Communication Technology (ICT) within the educational sector is increasing rapidly. University systems are becoming increasingly dependent on computerized information systems (CIS) in order to carry out their daily routine. Moreover, CIS no longer process staff records and financial data only, as they once did. Nowadays, universities use CIS to assist in automating the overall system. This automation includes the use of multiple databases, data detail periodicity (i.e. gender, race/ethnicity, enrollment, degrees granted, and program major), record identification (e.g. social security number 'SSN'), linking to other databases (i.e. linking unit record data with external databases such as university and employment data).

The increasing demand and exposure to Internet resources and infrastructure by individuals and universities have made IT infrastructure easy targets for cybercriminals who employ sophisticated attacks such as Advanced Persistent Threats, Distributed Denial of Service attacks and Botnets in order to steal confidential data, identities of individuals and money. Hence, in order to stay in business, universities realise that it is imperative to secure vital Information Systems from easily being exploited by emerging and existing forms of cybercrimes. This study was conducted to determine and evaluate the various forms of cybercrimes and their consequences on the university network at Ahmadu Bello University, Zaria. The study was also aimed at proposing means of mitigating cybercrimes and their effects on the university network. Hence, an exploratory research design supported by qualitative research approach was used in this study. Staff of the Institute of Computing, Information and Communication technology (ICICT) were interviewed. The findings of the study present different security measures, and security tools that can be used to effectively mitigate cybercrimes. It was found that social engineering, denial of service attacks, website defacement were among the types of cybercrimes occurring on the university network. It is therefore recommended that behavioural approach in a form of motivation of staff behaviour, salary increases, and cash incentive to reduce cybercrime perpetrated by these staff.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The Internet as described by Zittrain (2006), is a global computer network that provides a variety of communication facilities using standard communication protocols. The Internet has become a very effective tool for all forms of business transactions. Its usage now spans the globe as organisations around the world are increasingly depending on it for the facilitation of their business transactions. The use of Internet in today's businesses makes it possible to obtain information, exploit new ideas and even facilitate business alliances across the globe.

The Internet enables online transactions through password-protected payment methods. These payment methods allow the transfer of funds over an Electronic Funds Transfer (EFT) platform (Cassidy, Gross, & Malekpour, 2002). The underlying security architecture such as Public Key Infrastructure (PKI), Secure Socket Layer (SSL) and Transport Layer Security (TLS) provides some level of protection and authenticity to ensure that information in transit, over the Internet, is secured.

Organisations are embracing the Internet and new technologies in order to carry out their day-to-day activities and transactions. Today's educational institutions are, likewise, also embracing the Internet and new technologies for performing their day-to-day operations and transactions. These transactions include but are not limited to payment of application and school fees.

The usage and dependence on the Internet increase the challenges relating to securing individual and organisational information and information systems. It is also forcing organisations to invest in technologies, management procedures and initiatives that enhances the security of their network, information and information systems.

Furthermore, educational institutions are highly dependent on computerised information systems (CIS) in order to carry out their daily routines. Considering the continuous advancements in technology, CIS are no longer confined to their traditional tasks of processing staff records and financial data. Institutions now use CIS to automate their overall processes. The increasing use of CIS is causing educational institutions to be exposed to cyber threats (Ewell, Jankowski, & Provezis, 2010) that could exploit any vulnerability within the CIS. Also, consequently, institutions are becoming aware of the range of risks associated with the use of CIS and the Internet. Some of which include: malware, viruses, spams, scams, and phishing.

Technology is now being rapidly integrated into the various departments of universities. However, the rapid integration of technology also comes with its own challenges. The number of vulnerabilities associated with technology use in universities is on the increase (Brody, Zahran, Vedlitz, & Grover, 2008). This is compelling universities to implement various security controls and measures that can help mitigate and manage the associated risks of adopting and using information technologies. According to Barton (2011, pp. 6 - 9), a security control is a “sequence of operations that ensure protection of data”. Security controls are mostly used together with communications protocols to ensure data delivery between two or more parties.

1.2 Motivation for Research

Cybersecurity is a field that is gaining much more attention. This stems from the fact that cyber attacks are increasing in both intensity and complexity (Cavelty, 2012). To address information threats, organisations are increasingly adopting and updating their Information security controls and measures. Educational institutions, just like any other organisation, are continuously searching for better means to protect their information and clients from attacks (Carolina, 2014).

Educational institutions are prioritizing and increasing data security by implementing security protocols that can protect their users (Whitman and Mattord, 2011). However, with this increase in data security, cybercriminals are still managing to bypass the university's network. This study therefore aimed at understanding, from an educational institution's perspective, the effectiveness of security protocols in relation to cybercrime. The study also focused on understanding the challenges faced by educational institutions in the implementation of security controls that can help in mitigating the effects of cybercrimes.

1.3 Objectives of the Study

The main objective of this study is to explore the effectiveness of security protocols in relation to cybercrime. To achieve this main objective, this study set to achieve the following objectives:

i. To determine the types of cybercrimes that Ahmadu Bello University Network could be susceptible to.
ii. To identify the areas of Ahmadu Bello University's Network that is vulnerable to cybercrime.
iii. To determine the security protocols that can be used to effectively manage Ahmadu Bello University's Network from cybercrime.

1.4 Significance of the Study

In recent years, there has been a surge in the use of mobile devices, computer systems and the Internet in educational institutions. Likewise, the crimes committed by cybercriminals that use the Internet, mobile devices and computer systems have gained momentum. Cybercrime prevention at institutions of higher learning requires that information should be well secured and managed to prevent breaches in the university's networks and protect the university community from cybercriminals (Herzog, 2010; M. Whitman & Mattord, 2011). This study will be of importance because it aims to contribute to the existing

literature that educates both staff and students in educational institutions of the potential vulnerabilities and threats associated with universities' IT resources, and also online transactions. The study will also be of importance to people involved in the universities' information and network management portfolios because it proposes security measures on how to protect the university's information and network resources against the cybercrimes.

1.5 Statement of the Problem

Cybercrime at universities is a challenging area for information technology (IT) professionals (Carolina, 2014). Students' passwords, credit card details, grades as well as alumni information can be obtained by hackers (Carolina, 2014). According to a news report by NBCNews (2013), a student at the University of Nebraska, United States, hacked into the University's database and compromised the records of about 650,000 current and old students. Another security breach occurred at the University of Pittsburg (PTT) in 2013, where hackers compromised PTT's server and obtained private information of students and staff. The hackers then threatened to release the information publicly unless the university apologised for the lack of security on the server (NBCNews, 2013).

Information is of significant importance in the university environment and should be protected by all means. When security protocols are breached, confidential information could become compromised. According to Ponemon (2012) and Sinanaj and Muntermann (2013), the cost of protecting cybercrime from occurring in an academic environment is high. The current dependency on technology and integration of such technology into the academic environment has created a vulnerable atmosphere for Internet users within the University community. This dependency and integration has also led to threats and attacks on the records and personal information of individuals and universities (Kalinich & McGrath, 2003).

Studies have been conducted to find a lasting solution to cybercrimes in Nigeria (Adeta, 2014; Hassan, Funmi, & Makinde, 2012). These studies helped in understanding the causes and effects of cybercrimes. The studies recommended the establishment of cybercrime laws and individuals' use of licensed anti-viruses. However, to date cybercrime remains a considerable issue in Nigeria. According to Adeta (2014), male youths are the major perpetrators of cybercrime and poverty, corruption and the absence of cybercrime laws are the major causes of cybercrime in tertiary institutions in Nigeria. In order to reduce incidents of cybercrime in Nigerian Universities, there is a need to explore the effectiveness of the security protocols put in place on Universities' networks. This study therefore explores the effectiveness of the security protocols put in place by Ahmadu Bello University, Zaria, on the University's network.

1.6 Research Questions

The questions drawn from the problem statement to achieve the objectives of this research are:

i. What types of Cybercrime is Ahmadu Bello University's Network susceptible to?

ii. What areas of the University's Network are vulnerable to cybercrime?

iii. How effective are the security protocols used by Ahmadu Bello University in protecting their Network from cybercrime?

1.7 Research Methodology

The study was conducted at Ahmadu Bello University, Zaria, Nigeria. In order to get the sample of participants from all relevant units involved in the study within Ahmadu Bello University, a qualitative research methodology was used. The research was exploratory, and the methodology was implemented through interviews and document analysis as a means of data collection. Interviews were conducted based on a schedule and were recorded digitally, after which analysis

procedures were used to determine similarities and differences of the interviewees' responses. The content of Case File Documents from the Security Unit of the University provided another source of data.

In particular, a qualitative research methodology was chosen for this study because it allowed the researcher to uncover important questions and processes, and also understand relationships among data collected. Interviews were conducted with fifteen (15) staff members with more than three (3) years working experience from the Institute of Computing and Information Communication Technology (ICICT) Directorate. Recorded interviews were transcribed and the transcribed interviews were analysed thematically.

1.8 Limitations of the Study

Due to lack of access to cybercriminals, the study focused only on the university staff's perspective as far as the effectiveness of cyber-security measures is concerned. The author acknowledges that interviews with other cyber-security experts could have been conducted in order to get more insights on what universities should do in order to shield themselves from cyber-attacks. However, the researcher overcame this limitation by using the case files in the Security Unit.

1.9 Chapter Outline

This dissertation is divided into five chapters. They are as follows:

Chapter one provides an overview, the background, objectives, significance and problem statement guiding the study. Research questions, limitations of the study and the chapter outline are also outlined.

Chapter two presents the literature review on cybercrime and security protocols as well as the effects and factors that influence cybercrimes. The chapter also discusses information security control measures in a university network set up.

Chapter three explains the methodology used in this research. The chapter begins by presenting the sequence in which the research methodology of this study is conducted. It further explains the theoretical framework used in this study.

In chapter four, the findings from the interviews as well as discussion are presented.

Chapter five concludes the dissertation by presenting the summary of the research findings. The chapter also suggests recommendations and areas in which further studies on cyber-security protocols should focus.

1.10 Conclusion

In this chapter, cybercrime was briefly described, a motivation for the study, aims and objectives, and the significance of the study were also stated. The chapter also stated the problem of the research, the methodology adopted and the research questions. It was highlighted that the usage and dependence on the Internet is continuously and increasingly posing challenges such as propagation of viruses, hacker's attacks, denial of service attack and other information security risks. These challenges have prompted a necessary action to be taken in order to guard against potential attacks. Thus, securing the university's network has become imperative, because without securing it users are prone to cyber-attacks with devastating consequences.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents the review of literature related to this study. In order to identify the gap which this research tries to fill, the chapter discusses the concept, categories, techniques and effects of cybercrimes. The chapter also discusses how cybercrime is grossly increasing to the detriment of security controls being implemented at higher institutions of learning. The review of the literature, as presented in the subsequent sections, is in relation to the objectives of the study.

2.2 The Concept of Cybercrime

The Internet and related technologies brought about the development of a variety of tools and applications which are used to transmit information across the globe using standard communication protocols (e.g. HTTP, TCP, SMTP, UDP) (Paul, 2014, p. 9). The Internet and related technologies also provide easy communication among faculties, departments, units and even across universities. However, according to Van Eeten and Bauer (2009), a lot of financial risks are attached to the Internet, and these risks do not exclude academic institutions. It has been stated by Lemon (2006) that if the Internet or part of the universities information system goes down, it could lead to enormous loss. Therefore, educational institutions, like any other organisation, need to take proactive measures in protecting their information and information system (Urbas & Choo, 2008).

The Internet has made today's living easier in many ways. However, people are using it to commit crime and exploit information systems vulnerabilities in order to carry out attacks for malicious or personal gains (Zittrain, 2006). One of the prominent crimes that is being committed through the Internet is popularly

referred to as cybercrime (V. Sharma, 2015). Cybercrime has been a major concern in the last two decades (Lesk, 2011). Considerable amount of resources is spent on both preventive and reactive measures across the globe. Nowadays, malicious software also known as malware, have become a serious security threat to Internet users. It has been ascertained by Pierluigi (2013) that cybercrime could pose a lot of security threats to universities' information and information system. These threats include phishing, virus attack, hacking, breaking security codes, spamming, etc. These threats by implication can compromise the availability, integrity and confidentiality of stored information and information in transit.

Cybercrimes are increasing at a greater rate on a daily basis than conventional crimes. Poonia, Bhardwaj, and Dangayach (2013) stated that cybercrime and conventional crimes are two entirely different concepts, even though both are performed by people with criminal motives. Cybercrimes involve the use of communication media and the use of computer-mediated means, while conventional crimes may not necessarily require technical means. According to a survey conducted by the United Nations Office of Drugs and Crime (2013), 17% of Internet users in 20 countries fell victim to cybercrime, but in the case of conventional crime, the study reported that in the same 20 countries only 5% fell victim.

Cybercrime is a form of criminal activity that involves the use of a virtual medium such as the Internet. It also involves illegal access to computer data via the Internet (Goldsmith & Wu, 2006). It is one of the prevalent, and perhaps the most challenging and intricate problem in cyberspace (Poonia *et al.,* 2013). According to Ani (2011) and Hassan et al. (2012), it can simply be described as criminal offences that can be carried out online with the aid of technological infrastructure. Also, according to Poonia *et al.* (2013, p. 5) it is "any criminal activity that uses a computer either as an instrumentality, a target or a means for perpetuating crimes". Futhermore, Halder and Jaishankar (2011) described cybercrime as

offences that are committed against individuals, property, or government, with the motive to cause physical or mental harm or even cause reputational damage, either directly or indirectly, using modern technologies that comes with the Internet and telecommunication devices. In addition, the literature also shows that cybercrime can also be referred to as a harmful act which involves acquisition and manipulation of organisational data. Such crimes can threaten a nation's security, universities' infrastructure or individual's computer systems, communication devices and even the cyberspace.

According to Murray (2017), cyberspace refers to an electronic medium used to form a global computer network to facilitate online communication. The Cyberspace has become one of the greatest areas where people perform illegal activities due to the vast amount of information that is processed and exchanged via the Internet. Such illegal activities occur in almost all the different types of organisational sectors. For example, Millet (2015) reported an instance in Poland where hackers targeted airline travelers and successfully grounded around 1,400 passengers. Similarly, the United Kingdom (UK) security intelligence's database was reported to have been hacked into, and this resulted in compromising the confidentiality of e-mails and personnel information of security personnel (Shimomura & Markoff, 1995). United Nations Office of Drugs and Crime (2013) also stated that private sector enterprises in Europe reported serious cybersecurity threats while performing online transactions. In the same study, it was further indicated that 16% of cybercrimes were due to intrusion, phishing or e-mail spamming.

Burstein (2008) stated that the increasing reliance on the Internet has resulted into today's environment being more prone to activities such as identity theft, larceny, sabotage, espionage etc. He further reiterated that most crimes that can be committed in person can now be committed through the Internet. Hence, Universities like organisations that are negligent or have weaknesses in their security protocols make themselves vulnerable to Internet crimes.

Groves *et al.* (2013) stated that the frequency of cybercrimes is increasing rapidly and affect almost all organisational sectors. According to the Data Breach Investigation Report of 2013 by Verizon globally, about 37% of cybercrime affected financial institutions, 24% of security breaches occurred in retail companies and restaurants, 20% of network intrusions involved supply chains and 38% of security breaches impacted large multinational organisations, such as telecommunication companies, Airlines, Oil companies, and other conglomerates, while 20% of network intrusion hit information and professional service firms, such as law firms, hospitals and academic institutions (Cert, 2013; Verizon, 2013).

According to Burstein (2008), the United States of America (USA) has been the most hard-hit country by cybercriminals. Other countries that are victims of cybercrime include: Indonesia, Yugoslavia, Ukraine, Egypt, Lithuania, Bulgaria, Romania, Russia, Malaysia, Israel, Pakistan and Nigeria (Kshetri, 2009). Kshetri (2009) also indicated that for every 10,000 Internet users in Nigeria, 23.4% fall victims of cybercrime.

The level of Internet penetration in Nigeria is rapidly increasing. The percentage of cybercrime via the Internet was less than 5% between 2003 and 2010. However, by the end of 2012, cybercrimes increased to over 30% (Sesan, Soremi, & Louwafemi, 2014). Sesan *et al.* (2014) in their study also observed that 70% of the surveyed participants affirmed that they had been victims of cybercrimes in Nigeria at one time or another. The Nigerian Deposit Insurance Corporation (NDIC) disclosed in its 2012 annual report that 3,380 cybercrimes involving the sum of 25.1 million US dollars occurred in 2012. In 2011, cybercrimes in the country accounted for 22.6 million US dollars (Iyoha, 2012).

Educational institutions are not immune to cybercrimes. According to NBC News (2013), the University of Pittsburg, in the USA encountered a cyber attack where by private information of staff and students were obtained. The hackers then threatened to release the information publicly unless the university apologized for

its lack of security. Alazab, Venkatraman, Watters, Alazab, and Alazab (2012) also stated that a cybercriminal breached the security protocols of university of Maryland (USA) and exposed records containing personnel identifiable information (PII) of students and staff. Furthermore, Halder, Jaishankar, and Jaishankar (2012), Yassir and Nayak (2012) indicated that records of over 146,000 students from the Indiana University (USA) were exposed due to cybercrime. The North Dakota University (USA), similarly, reported that a server containing names and social security numbers of more than 290,000 current and former students and about 780 faculties and University staff members was hacked (Butts & Shenoi, 2013). This shows that universities are not excluded from cybercrime.

2.3 Categories of Cybercrime

The Internet has added another dimension to how organisations conduct their businesses and nurture their activities. However, it has also brought an equally real and serious threat that every year results in loss of vast amount of money to businesses (Adeta, 2014; Singleton, 2013). Studies such as that of Saini, Rao, and Panda (2012), Valkenburg and Peter (2009) have categorised these threats to organisations and higher institutions. Saini *et al.* (2012) in their study provided three categories of cybercrimes, which are: data crime, network crime and access crime. Data crime may take place in form of data interception, data modification and data theft (Saini *et al.,* 2012).

According to Stallings (2007), data interception involves an unauthorized party on the network that intercepts data in transit and changes part of that data before re-transmitting it. On the other hand, data theft was described by McCormick (2008) as a growing phenomenon primarily caused by system administrators and office workers with access to technology infrastructure or services such as database servers, desktop computers and a growing list of hand-held devices such as USB flash drives, iPods, digital cameras, capable of storing digital information.

According to Valkenburg and Peter (2009), network crime also known as network interference is also a category of cybercrime. Network interference affects the functioning of a computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing network data. Network interference is an act whereby computer networks specialists deliberately interfere with normal functioning of the network in an organisation, with the aim of causing problems (DSLReport, 2011). Cybercriminals use various devices in facilitating their unlawful activities. Desai (2010) noted that they also use different technologies to illegally intercept, interfere or alter information over the Internet. According to Ablon, Libicki, and Golay (2014b), skimmer, john and ripper, wireshark, nessus remote security scanner, Kismet, cain and abel and NetStumbler are used by cybercriminals to commit cybercrime, obtain intelligence and sensitive information that are used for personal gain. Another category of cybercrime mentioned by Saini *et al.* (2012) is access crime. Access crime refers to the accessing of computer systems without permission (Britz, 2009). Stihler and Bachtold Jr (2014) described access crime as the unauthorised and unauthenticated access to computer systems.

Categories of cybercrime were also provided by Wolfe, Higgins, and Marcum (2008), who in their study identified cyber piracy, cyber trespass and cyber vandalism as categories of cybercrime. According Wolfe *et al.* (2008), cyber piracy involves the use of cyber-technology in an unauthorized ways in order to reproduce copies of proprietary software and proprietary information. WaII and Yar (2010) further added that cyber piracy has to do with distribution of proprietary information (in digital form) across a computer network. Chung, Chen, Chang, and Chou (2006) described cyber piracy as the intercepting or stealing confidential company data by malicious hackers.

According to Wolfe *et al.* (2008), cyber-trespass involves the use of technology to gain unauthorized access to an individual's or an organisation's computer system. Similarly, Wong (2006) stated that cyber trespass is the act of accessing

a password-protected web site by cybercriminals. Cyber-trespass is also described as a means of accessing someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection (Kshetri, 2009).

The last category identified by Wolfe *et al.* (2008) is cyber vandalism which is a process of using information technology facilities to unleash one or more programs that disrupt the transmission of electronic information across one or more computer networks, including the Internet. Jaishankar (2011a) further assert that cyber vandalism involve the use of cyber-technology to destroy data resident in a computer or damage a computer system's resources, or both. In another study by Fung (2014), cyber vandalism is described as the act of damaging someone's data that in a way disrupts the victim's image or business due to editing the data into something invasive, embarrassing or absurd. Kharat (2017), also described cyber vandalism as a means of deliberately damaging computer data, and affect the services that a businesses can deliver. Thus cyber vandalism means destroying or damaging the data or information stored in computer by stopping or disrupting the network services. It may also include any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or peripheral device attached to the computer.

Dalla and Geeta (2013) categorised cybercrimes in his study titled "Cybercrime – A Threat to Persons, Property, Government and Societies". They identified cybercrime against individual, cybercrime against property and cybercrime against government as categories of cybercrime. Similarly, Goutam (2015) in another study identified cybercrime against individuals as a category of cybercrime. Cybercrime committed against individuals include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail, and cyber-stalking. The potential harm of such a crime to humanity can hardly be explained. Cyber-harassment is another distinct

cybercrime category. Various kinds of harassment which can be sexual, racial or religious occur through the use of cyberspace. Persons perpetuating such harassment are guilty of cybercrimes.

The second category of cybercrimes identified by Dalla and Geeta (2013) is cybercrimes against property. Cybercrime against property is a situation where by a person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. Similarly, Rantala (2008) stated that cybercrime against property includes unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

2.4 Common Cybercrime Techniques

The common techniques used to perpetrate cybercrime were also identified in the literature. Cybercriminals of the 21st century explores various means in committing criminal activities. They use planned procedures and devices to aim at their victims (Alcaraz & Zeadally, 2013). As the use of Internet is becoming increasingly prevalent due to its ease of access, its acceptance by organisations and educational institutions and the monetary benefits associated with its use are also on the rise. Internet users are at great risk of unknowingly passing on their information to cybercriminals and fraudsters (Wada & Odulaja, 2012b). These techniques are used to perpetrate the different forms of cybercrimes in organisations and universities.

Different tools (hardware and software) are being used by cybercriminals in gaining access into organisational network. Brandon (2007) stated that cybercriminals use various tools in breaching the network security protocols in organisations. Ablon, Libick, & Golay, (2014) mentioned some of the tools used by cybercriminals to include John and Ripper, Wireshark, Nessus Remote security scanner, Nmap, Kismet, Cain and Abel, mad-in-the-middle attack and

NetStumbler. also mentioned other tools such as, Crack-A Unix based program, L0phtcrack (a window based program), telnet, CGI logins and Kali. These same tools could be used in gaining access to universities network (Andoh-Baidoo & Osei-Bryson, 2007).

In another related study, Carnegie (2015) provided some techniques used by cybercriminals. These techniques include denial-of-service attack, botnet, skimming, shoulder surfing, social engineering, spamming, key logging, spoofing, espionage, web site defacement. Once a network has been hacked or cracked, victims become easily accessible by perpetrators, and the network gets treated and accessed like any open network. Some of the techniques used by cybercriminals identified in literature are described below.

2.4 (a) Denial of Service Attack

According to Smith (2001) and Smith *et al.* (2007), denial of service attack (DoS) is a technique in which cybercriminals use to access computer systems or network illegally. DoS is described as a process whereby victim's computer is flooded with more requests than it can handle which causes it to be inaccessible by legitimate requests (Smith et al., 2007). According to Carl, Kesidis, Brooks & Rai (2006), DoS attack is a type of attack on a network that is designed to bring the network to its knees by flooding it with a lot of data traffic. Lincoln and John (2015) in their work described it as an attack designed to render a computer or network incapable of providing normal services This act can potentially lead to the compromise of the victim's information. DoS attack does not require the attacker to have any physical proximity to the victim nor does it require the explicit download of traditional malicious software (Carl, Kesidis, Brooks, & Rai, 2006).

Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit vulnerabilities in the TCP/IP protocols (Carl *et al.,* 2006). According to Maxim (2015), in a DoS attack, a perpetrator uses a single Internet connection to either

exploit a software or flood a target with fake requests usually in an attempt to exhaust server resources (e.g., RAM and CPU). Unauthorized access to computer systems or network, theft of information stored in electronic media, email bombing, virus attack, logic bomb, Internet time thefts, web jacking could all occur through DoS in a university set up, just like in any other organisational network (Needham, 1994).

According to Lincoln and John (2015), the most common DoS attacks will target the computer's network bandwidth or connectivity, hence causing a bandwidth attack or connectivity attack, which causes the bandwidth and network connectivity to slow down. Bandwidth attacks flood a network with a high volume of traffic causing all available network resources to be consumed, hence denying access to legitimate user requests. Connectivity attacks flood a computer and network with such a high volume of connection requests, to such an extent that all available operating system resources are consumed, and the target computer can no longer process legitimate user requests (Lincoln & John, 2015). A successful DoS attack is a highly noticeable event that impacts the entire online user base.

DoS assaults often last for days, weeks and even months, making them extremely destructive to any organisation with an online presence. DoS can cause loss of revenues, erode consumer trust, force businesses to spend fortunes in compensations and cause universities to suffer long-term reputation damage (Maxim, 2015). DoS attacks can be mitigated by ensuring organisations enforce tight security policies and parameter defences such as firewalls, vendor recommended patches (Saravanan & Asokan, 2011).

2.4 (b)Botnet Attack

Another technique used by cybercriminals is botnet which is becoming one of the most serious threats to Internet security (Stone-Gross *et al.,* 2009). The word botnet is a combination of the words robot and network. According to Abu Rajab,

Zarfoss, Monrose, and Terzis (2006, p. 9), “A botnet is a network of compromised machine under the influence of malware (bot) code”. While, according to Radware (2015), a botnet is a collection of compromised computers often referred to as ‘zombies’ infected with malware that allows an attacker to control them.

Botnet owners are able to control the machines in their botnet by means of a covert channel such as IRC (Internet Relay Chat), issuing commands to perform malicious activities such as distributed denial-of-service (DDoS) attacks, the sending of spam mail, and information theft. The botnet is commandeered by a ‘botmaster’ and utilised as ‘resource’ or ‘platform’ for attacks. Botnet can cause security threats such as distributed denial-of-service (DDoS) attacks, spamming, identity theft, and information exfiltration (Gu, Perdisci, Zhang, & Lee, 2008). Silva, Silva, Pinto, and Salles (2013) believed that the use of intrusion detection systems, signature and anomaly based detection systems would help effectively detect and mitigate botnet attacks.

2.4 (c) Skimming

Another technique used by cybercriminals is skimming. In skimming, criminals use skimmer to steal credit card information when the card is swiped through the skimmer (Lusthaus, 2013). Skimmer is referred to as a scanning device and reader that could be used to access, read, scan, obtain, memorize or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card without the permission of the owner (Jonathan, 2015). Wells (2017) further stated that skimming is the unauthorized capture and transfer of payment data to another source.

According to Ahmed (2010), cybercriminals use skimmer to steal credit/debit card numbers and social security number from unsuspecting victims. With skimming, payment information can be stolen directly from the consumer’s payment card or from the payment infrastructure at a merchant location. This technique typically

requires the use of a rogue physical device planted onsite. De Luca, Weiss, and Drewes (2007) believed that skimming can be mitigated by providing some IT security guidance. Such guidance may include properly educating personnel about the threats and risks associated with skimming.

2.4 (d) Shoulder Surfing

Another example of cybercrime technique that involves less usage of technology is shoulder surfing. According to Wiedenbeck, Waters, Sobrado, and Birget (2006) and Gao, Ren, Chang, Liu, and Aickelin (2010), shoulder surfing refers to a direct observation, such as looking over a person's shoulder in order to obtain confidential information. Wiedenbeck *et al.* (2006) further stated that, shoulder surfing is done for no reason other than to get useful information from unsuspecting victims. In their study, Kumar, Garfinkel, Boneh, and Winograd (2007, p. 1) stated that shoulder surfing can also be described as the "practice of spying on the user of a cash-dispensing machine (i.e. ATM) or other electronic device in order to obtain sensitive information" such as personal identification number, password. In essence, shoulder surfing is most common in busy and crowded areas where a cybercriminal is not likely to be caught (Lashkari, Farmand, Zakaria, Bin, & Saleh, 2009). This is because it is relatively easy to stand next to someone and watch as they fill out a form online, or enter a PIN number at an ATM machine, or use a calling card at a public pay phone (Kumar *et al.,* 2007). In another related study, Tari, Ozok, and Holden (2006) stated that, shoulder surfing can be done at a distance using other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be hidden in ceilings, walls or fixtures to observe data entry.

To prevent shoulder surfing, it is advised to shield paperwork or the keypad from the view of people by using one's body or cupping one's hand (Long, 2011). Furthermore, to secure or prevent shoulder surfing, the European Association for Visual Data Security recommends that, when a user is in a situation with heightened risk, the user should protect him/herself by angling the screen away

from the gazes of other people, or use a special privacy screen shield to reduce the visibility of the screen (De Luca *et al.,* 2007). De Luca *et al.* (2007) further recommend that some of the corporate IT security guidance should be used. Such guidance may include properly educating personnel about the threats and risks associated with shoulder surfing.

2.4 (e) Social Engineering

Social engineering is another technique used by cybercriminals. Social engineering is the art of manipulating people so they give out confidential information (Harrison, 2010). It as a non-technical method of intrusion, relies heavily on human interaction and often involves tricking people into breaking normal security procedures (Harrison, 2010; Thompson, 2013). It is one of the greatest threats that organisations today encounter. The types of information the attackers target can vary. In the case of social engineering attacks against individuals, criminals usually try to trick them into giving passwords or bank information, or giving access to computer. The intent of social engineers is to sometimes secretly install malicious software that will give the criminals access to the kind of information they want. In other instances, the intent could be to gain control over the victims entire computer. A pre-texter for example, could call an individual, pretending to be from an organisation the individual trusts, and ask for important personal data such as a social security number (Harrison, 2010). A common way of committing social engineering crimes is through Phishing.

According to Wada and Odulaja (2012a) phishing is one of the most common ways in which cybercrime is performed, especially social engineering crimes. They describe phishing as one of the means used by cybercriminals to acquire sensitive and confidential information. They further ascertained that phishing could be attributed to advanced identity theft. This type of theft aims at not only stealing the identity and personal information from unsuspecting individuals, but also denotes fraudulent acts against legitimate businesses in the financial and academic institutions. Rogers (2000) defined phishing as a social engineering

crime that is commonly used in attacking information systems (IS) in organisations, in order to gather private and confidential information. According to a report by Manning and Aaron (2013), phishing scams remain one of the most prominent form of spam sent worldwide today that pose significant dangers to unsuspecting victims.

Halder and Jaishankar (2011) ascertained that most phishing attacks use links to illegitimate websites that have similar visual content as legitimate businesses. The aim is to lure unsuspecting to enter their sensitive information that can then be intercepted and used to commit further crimes. Dhamija, Tygar, and Hearst (2006) conducted a research in the United States of America on users of the Internet and found that cybercriminals lured 90% of Internet users into visiting fraudulent websites. According to Ahmed (2010), phishers often pretend to be financial institutions or companies and send spam or pop-up messages to get one to reveal his/her personal information. Cohen *et al* (2011) and Chen, Bose, Leung, and Guo (2011) further explained that this is due to the fact that most Internet users do not look at the status bar, address bar or any other security indicators, such as “https” or a golden key on the address bar before logging into websites. Criminal hackers obtain information of individuals or organisations that have performed transactions on such fraudulent websites and then make fake credit or debit cards through the obtained information (Myers & Avison, 2002). Hadnagy (2010) believed that the most effective way to protect oneself or the employees of an organisation from social engineering attacks is to stay informed. Staying informed usually involves knowing what to be careful of, what to watch out for and what to shun (Hadnagy, 2010).

2.4 (f) Worms and Viruses

Worms and viruses are also used by cybercriminals as a technique to carry out cybercrimes. According to Aycock (2006), viruses are programs that are created and distributed to computers, they attach themselves to a file and then circulate to other files and to other computers on a network. They normally affect the data

on a computer, either by altering or deleting it. “Worms, unlike viruses, do not need to attach themselves to a host, they only make functional copies of themselves and do this repeatedly until they eat up all the available space on a computer’s memory” (Kerr, Rollins, & Theohary, 2010, p. 4). According to Newman, Forrest, and Balthrop (2002), many computer viruses spread via electronic mail, making use of computer users’ email address books as a source for email addresses of new victims. These address books form a directed social network of connections between individuals over which the virus spreads. Balthrop, Forrest, Newman, and Williamson (2004) further reiterated that computer viruses usually spread in one of the three ways: from removable media, from downloads from the Internet, and from e-mail attachments (Aziz, 2011). Wu and Feng (2006) opined that implementing common security baselines is a way in which worm and viruses could be mitigated. These security baselines could be Anti-viruses, vulnerability assessments, penetration tests.

2.4 (g)Spoofing

Spoofing is another technique used by cybercriminals to hide the origin of their e-mails and leads to problems such as misdirected e-mail spam. Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages with a source IP address that has been compromised, but to indicate that the messages are coming from a trusted host (Whitman and Mottord, 2012). Kratchman, Smith, and Smith (2008) further explained that spoofing occurs when the cybercriminal uses e-mail to gain trust from a victim in order to steal personal information that is later used for unauthorised purposes, such as fraudulent purchases, obtaining fraudulent loans, or identity theft. To engage in IP spoofing, cybercriminals use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers to insert these forged addresses (Koh, Chang, & Lee, 2004). Internet users are becoming accustomed to accessing wireless routers in places like airports, conferences, libraries, universities and other public places which makes individuals and organisations

become more prone to spoofing attack (Karlof, Shankar, Tygar, & Wagner, 2007). According to Akritidis, Chin, Lam, Sidiroglou, and Anagnostakis (2007), a lot of cybercriminals use public internet access hot spots such as airports, conferences, libraries, universities and other public places to set-up malicious wireless routers to redirect users to spoofed websites.

Kahate (2013) stated that, spoofing involves getting a computer on a network usually one with special access privileges in order to obtain access to the other computers on the network. In practice, spoofers use several techniques, for instance an attack might work through DNS poisoning, spoofed DNS responses, modifying a user's hosts file or tricking a user to modify his/her DNS settings as an entry into the victim's cyberspace.

It was stated by Morris (2004) that, in spoofing, the sender's address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to opening e-mail they are not supposed to open. Spoofing can also alter data being transmitted across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable the attacker to get access to data stored on computer systems. In their study, Bose and Shin (2006) categorised spoofing into two different categories, these categories are: E-mail spoofing and SMS Spoofing. E-mail spoofing is described according to them as the mails which misrepresents the original e-mails. It shows its origin to be different from where it actually originates. While on the other hand, SMS spoofing is blocking of spam (i.e. unwanted or uninvited messages). In SMS spoofing, a cybercriminal hijacks a victim's phone number and uses it to send messages to people whose numbers are stored in the victim's phone contacts list.

In another related study, Sharma and Xie (2008), stated that spoofers can also exploit users' lack of understanding of the verification process for secure socket layer (SSL) certificates. SSL is the standard security technology for establishing an encrypted link between a web server and a browser (Thornewell & Hughes, 2014). This link ensures that all data passed between the web server and

browsers remain private and integral. Most Internet users do not know how to check SSL certificates in the browser, or understand the information presented in a certificate. In a spoofing scam, a rogue website may display a Certificate Authority (CA) which is not a trusted and seal certificate that links to the original CA website. It is only the informed and diligent Internet users that would know how to check that the Uniform Resource Locator (URL) of the originating site and the legitimate site described by the CA are matching. Sharma and Xie (2008) found that in the USA, spoofers deceived up to 5% of their recipients into providing sensitive information to spoofed websites (Loftesness, 2004). In this scam, about two million users gave information to spoofed websites which resulted into direct losses of $1.2 billion for U.S. banks and card issuers in 2003 (Litan, 2004).

2.4 (h) Espionage

Espionage, another technique that can be employed in conducting a cybercrime, is the act or practice of spying, used by cybercriminals to obtain secrete information (Stoll, 2005). Espionage otherwise known as trespass (Chauhan, 2010), is a well-known and broad category of electronic and human activities used in breaching the trust given to workers, by way of divulging confidential information to a party that is not officially allowed to be given the information (Stoll, 2005). Different techniques can be used to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called competitive intelligence (Hinckley, Bi, Pahud, & Buxton, 2012). Crane (2005) stated that, when information gatherers employ techniques that crosses the threshold of what is legal or ethical, they are conducting industrial espionage. Espionage may involve educational institutions, government agencies, private organisations, business enterprise or even individuals (Rezgui & Marks, 2008).

Espionage or trespass may also lead to unauthorised real or virtual actions that enable information gatherers to login to computer systems they have not been authorised to operate (Herrmann & Paech, 2005). Techniques for control of information systems from intruders are very important because they sometimes mark the boundaries of an organisation's virtual territory (Mcleod & Charles, 2011). These boundaries give notice to trespassers that they are intruding on the organisation's network (Mcleod & Charles, 2011). Sound principles of authentication and authorisation can help organisations protect their valuable information and information systems (Olden, 2010).

2.4 (i) Web Site Defacement

Website defacement is another technique used by cybercriminals in carrying out their unlawful acts. Website defacement is an attack in which the content of a website is changed in order to lure victims into an illegitimate website (Hinckley *et al.,* 2012). Usually, the new content on the website attracts the attention of the victims with the intention to motivate and lure them into supplying the necessary information that could be used against them. One of the most common methods of website defacements is known as SQL injection. Halfond, Viegas, and Orso (2006) described SQL injection as a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (mostly to transfer database contents into the attacker's repository). In an SQL injection attack, the cybercriminal is able to pass commands to the database by altering malicious data in the web form (Hinckley *et al.,* 2012). A good example of a well-known website defacement attack happened during the cyber-attacks on Georgian websites in August 2008, when unknown attackers gained access to the website of the Parliament of Georgia and posted college pictures of Adolf Hilter and Georgian President Mikhail Saakashvili (Kosina, 2012).

Umar-Ajilola (2010) stated that it is impossible to have an exhaustive list of the types of cybercrimes, and the skills/techniques that are used by cyber-criminals.

However, using any of the techniques/forms described in the paragraphs above, could pose a great danger to organisations, and can also result in loss of data, destruction of vital information and information systems (Chen & Zhao, 2012). The literature shows that today's cybercrime cannot be fought with yesterday's technology.

Security measures such as Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), IP Security (IPSec), Cryptographic system have become very important (Hoffman & Schlyter, 2012) in addressing issues relating to cybercrimes and cybercriminals' activities. Therefore, it is imperative to understand the techniques used by cybercriminals to breach the security protocols of the organisational network, as such, this will help to know the ways in which cybercrime can be curtailed.

2.4.1 Cybercrime Perpetrators' Profile

The full description of a 'cybercrime perpetrator' may contain many elements. These elements, which are amongst the core characteristics of cybercriminals include age, gender, level of education and experience, socio-economic background, nationality, and motivation (Malby *et al.,* 2013). While individual characteristics are comparatively straightforward to define, it is well known that analysis of organised crime frequently presents both definitional and measurement challenges.

Looking at the age range of cybercrime perpetrators, Konradt, Schilling, and Werners (2016) stated that Adolescents represent the highest percentage of people involved in cybercrime mainly due to their inquisitive nature (to know and explore secrets and confidential information). Another reason may be to prove themselves to be outstanding amongst their peers (Prins, 2011). The reason may also be psychological. For example, Felner, Jackson, Kasak, and Mulhall (1997) and Schell and Martin (2004) stated that they witnessed some young people who, for a variety of sociological and psychological reasons, have become

attached to their computers, and as a result, are exploring their potential in criminal manners such as getting unauthorised access to computers, programs, server, services, or other system, using someone else's account without permission or consent (Allsopp, 2010).

Several studies conducted in developing countries also provide a clear picture of age range of cybercriminals. One of such study conducted by Adeniran (2011) confirmed that 50% of the perpetrators are young men aged between 22 - 25 years, with more than half claiming to have already spent five to seven years in cybercrime activities. While corroborating the above findings, Aransiola and Asindemade (2011) also indicated that, most cybercriminals of the age between 22 – 25 constituted the highest percentage of people involved in online fraudulent activities in most West African countries.

Furthermore, Aransiola and Asindemade (2011) also reported that in terms of characterising cybercrime perpetrators by gender, male (90%) recorded the highest number of cybercrime activities than female (5%). In another related study conducted by Ablon, Libicki, and Golay (2014a), it was mentioned that children and adolescents, aged between 16 and 18 years mostly male by gender, are people involved in cybercriminal activity.

In addition, in the developing countries, most young men engage in computer-related financial fraud in their late teenage years (Helsper, 2008). This shows that the demographic nature of offenders mirrors conventional crime in that young males are the majority, although the age profile is increasingly showing older (male) individuals committing conventional crime, particularly concerning child pornography offences (Lu, Jen, Chang, & Chou, 2006).

Cybercriminals' unique profiles are significantly different from the conventional criminals in terms of educational background and experience. In Russia, for instance, most hackers are young, highly educated, and work independently (Kshetri, 2010). Evidence indicates that criminals' skill, intelligence, and

experience co-vary positively with the odds of getting away with crimes (Levy & Lemeshow, 2013). Some cybercriminals are highly skillful and thus face very low odds of getting caught. While some perpetrators of cybercrime may have completed advanced education, especially in the computer science field, many known offenders do not have specialised education. There is evidence that some less skillful cybercriminals get help from experienced cybercriminals and transnational organised crime groups thereby minimising the probability of getting caught (Chang, 2012).

Increasingly, a large number of unemployed or underemployed graduate students with computing skills have also been reported to be potential new resources for organised crime (Kannan, Rees, & Spafford, 2009). According to Malby *et al.* (2013), over 80 % of cybercrime are estimated to originate from some form of organised activity. This could be because, cybercrime in most cases often requires a high degree of organisation to carry out their criminal activities. Today, cybercrime perpetrators no longer require complex skills or techniques, due to the advent of readily available malware toolkits (Malby *et al.,* 2013). Cybercrime black markets are being established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information (Warikoo, 2014).

2.5 Effects of Cybercrime

Cybercrimes have emerged rapidly in the last few years and have major effects. Some of the effects that cybercrime may cause, as stated by Winston (1990) include identity theft, security cost and software piracy. Thampi, Anand, and Balakrishnan (2014), in their study on cybercrime types also identified software piracy, security coast, and identity theft as the effects of cybercrime. Niles, Sowa, and Laden (1994) further stated that most organisations can easily fall victim of cybercriminals and might also have consequences of cybercrime when any of the above listed effects occur on their networks. In another study conducted by Smith

et al. (2007), different effects of cybercrime were identified, and they are theft of intellectual property, identity theft and malicious software. Some of the prominent effects of cybercrimes as identified in the literature are discussed below.

2.5 (a) Identity Theft

According to Gordon, Rebovich, and Gordon (2007), Identity theft also known as identity fraud, is one of the major effects of cybercrime. It involves the cybercriminals obtaining key pieces of personally identifiable information of their victims, such as Social Security Number (SSN) or credit card number in order to impersonate them. Bilge, Strufe, Balzarotti, and Kirda (2009) further added that the effects of identity theft on its victim can have long-lasting effects. Once the information is obtained, it allows the cybercriminals to access bank details and other relevant information of a victim. The cybercriminals can even destroy or tarnish someone's image. This effect of cybercrime can take months or even years to fix. The damage can cost millions of dollars.

2.5 (b) Security Cost

Cybercriminals usually focus their attacks on businesses (large, medium and small enterprise) and the rich individuals (Byres & Lowe, 2004). According to Byres and Lowe (2004), cybercriminals usually take over company servers so as to steal information or use the machine for their own purpose, and in most cases steal monies. This requires organisations to invest heavily on security (to hire staff so as to update software to keep intruders out. This leads the organization incurring cost that will otherwise be used for other purposes. According to Taft (2010), a survey of large companies found an average expenditure of $8.9 million per year on cyber security, with 100 percent (100%) of firms surveyed reporting at least one malware incident in 12 months and 71 percent (71%) reporting hijacking of company computers by outsiders.

2.5 (c) Monetary Losses

Monetary loss is also identified as effect of cybercrime in the organisations and universities. This effect of cybercrime could immensely affect the entire activities and services. According to Symantec (2012), more than 1.5 million people fall victim of some sort of cybercrime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cybercrime worldwide every year. As victims get wise to traditional avenues of attack, cybercriminals have developed new techniques involving mobile devices and social engineering techniques to keep their illicit gains flowing. Some of the techniques used by cybercriminals are phishing, shoulder surfing, denial of service attack (Goodchild, 2012).

2.5 (d) Piracy

The cybercrime of piracy has had major effects on the entertainment, music and software industries (De Vany & Walls, 2007). As stated earlier by Wolfe *et al.* (2008) that, cyber piracy involves the use of cyber-technology in an unauthorized ways in order to reproduce copies of proprietary software and proprietary information. WaII and Yar (2010) also described cyber piracy has to do with distribution of proprietary information (in digital form) across a computer network. Claims of damages to this digital information are hard to estimates and even harder to verify.

2.5.1 Effects of Cybercrime on Universities

University networks have become an attractive target to cybercriminals (Sterbenz *et al.,* 2010). By the inherent nature of their operations, Universities' networks have a large number of transient users, making it more difficult to detect and respond to incidents than it would be in a more tightly controlled corporate environment (Osuagwu, Ogiemien, & Okide, 2010).

Universities are at the forefront in terms of academic and government research. Hence, it is important that information stored on computer devices or that passes through their networks be guarded against malicious and other cybercriminal attacks. Arguably, in the context of academic institutions, intellectual property, alumni databases and even a database of car parking permits containing details of vehicle owners would present great values to cybercriminals (Walker, Adomi, & Igun, 2008). Such information if accessed by criminals can be used to impersonate victims.

Educational institutions continue to hold a great deal of wealth of information that are typically and insufficiently protected (Burns, 2015). According to Ringwelski (2008) and Lenhart, Rainie, and Lewis (2001), the consequences of cybercrime in universities translate into wasted financial sources, time, and effort spent by IT personnel in trying to fix problems rather than focusing on the core competencies of the university. Another consequence of cybercrime on universities is reputational damage (Lenhart *et al.,* 2001). In cases where student records are compromised by a security breach, the university's reputation can seriously be damaged. Students whose personal information are intercepted or accessed by cybercriminals may not trust the university's information management structure and system anymore, hence tarnishing the University's public image.

According to Oyesanya (2004), a global anti-corruption body called Transparency International, has already categorized Nigeria as one of the country with high number of cases related to cybercrime in the world. Furthermore, private companies around the world are beginning to take steps toward blocking email traffic originating from Nigeria (Grover & Saeed, 2004). Financial transactions arising from Nigeria are now accepted with extreme due diligence around the world and some international banks completely deny access to their web sites when traffic originates from Nigeria (Awe, 2009).

2.6 Factors Contributing to Cybercrime Increase

Technological advancements have brought some improvements in various aspects of human lives, challenging human imagination and expectations. In this sense, the Internet has been no different and, just as with other technologies of the past, has generated a lot of dilemma (DiMaggio, Hargittai, Neuman, & Robinson, 2001). However, beyond the appreciation of its usefulness, the relationship between Internet technology and human social structure has proven not to be metaphysical but materialistic instead (Jegede, 2010). Hence, the Internet, rather than remaining a tool for enhancing the global economy tends to give birth, nurture and reinforce the intensity of risk and insecurity in socio-economic interactions, globally. The Internet has also greatly facilitated illicit transnational economic activities (Jegede, 2010). Many analysts have suggested that the Internet has offered great potential in terms of stimulating illicit cross-border activities that are unmatched by any other previous technologies. According to Grover and Saeed (2004), cybercrime also affects Internet-based businesses and service providers. These businesses stand to lose money in the event of any downtime created by cybercriminals.

The increasing use of the Internet creates new opportunities for cybercriminals. The cyberspace being virtual, that is, where transaction could be made without physical contact, has created new phenomena that are notably distinct from the (mere) existence of computer systems, but also provide opportunities for crime and criminals. Persons may, for example, commit crimes on the Internet that they would not otherwise commit in physical space due to their status and position. As supported by Jaishankar (2011b) who stressed that, identity flexibility, dissociative anonymity and lack of deterrence may serve as contributing factors and may provide opportunities for criminal behaviour in cyberspace. According to Phair and Hodges (2007), by the 1990's, cyberspace had become established as one of the fasted growing environment for criminal activities. In the last two decades, the number of people using the Internet for commercial purposes and

personal activities has increased substantially, and thus providing an environment that is being exploited by cybercriminals (Appel, 2014).

According to Goje, Gornale, and Yannawar (2007), Nadiah (2014), Amit and Schoemaker (2012), Levy and Lemeshow (2013), and Ionescu (2012), the factors contributing to the increase in cybercrime includes: economic factor (get rich quick syndrome), urbanisation, difficulty in tracing cybercriminals and loose laws and penalties in some countries (e.g. Nigeria), negligence of some IT staff etc. All these factors in one way or the other have contributed to the increase in cybercrime.

Levy and Lemeshow (2013) stated that economic factor which is worsened by the 'get-rich-quick' syndrome is one of the main factors that is influencing cybercrime. In another related study, Nadiah (2014) observed that, like many crimes committed outside the Internet, money is a major motivator for most cybercrimes. The perception of low risk and very high financial reward is also prompting many cybercriminals to engage in phishing, identity theft and fraudulent money request attacks (Castell, 2013). According to a Business week report of 2015, it was estimated that cybercrimes targeting online banking accounts alone hit nearly 700 million dollars per year globally. Another economic factor that contributes to cybercrime according to Amit and Schoemaker (2012), is the high level of unemployment. According to Ionescu (2012), cybercrime can also be associated with high rate of unemployment, harsh economic conditions, and poor educational system. Unemployment is identified as another crucial factor luring youths to 'cybercrime' *(*Malby *et al.,* 2013*).* In a study in Ghana, Warner (2011) highlighted that 'Sakawa' boys (cybercriminals) engaged in Internet fraud frequently, and justified their actions as the only way they can survive in the absence of employment.

Amit and Schoemaker (2012) further stated that, urbanisation is also another factor that leads to the increase of cybercrime-related activities. The massive movement of people from rural settlement to cities is increasing cybercrime.

Meke (2012) showed that urbanisation is one of the major factors contributing to the increase in cybercrime both in developing and developed countries. He further emphasized that urbanisation is one of the major contributing factor to the continuous increase in cybercrime. Cybercriminals in urban areas find it lucrative to invest their time and energy into cybercrime because it is a business that requires less capital and yield more profits when it hit the target (Meke, 2012).

Gardere (2014) and Grimes (2015) stated that the rise in cybercrime activities is due to the fact that cybercriminals are not been easily caught or easily trackable, especially while in the act. At the same time, Shinder and Cross (2008) further reported that inaccessibility to cybercriminals while in the act of committing the crime and tracing them after they might have committed the crime is another factor leading to the increase in cybercrime. They further stated that even if traced and caught by law enforcement agents, little or no punishments/penalties are given. Especially in some developing countries like Nigeria and Ghana where in most cases cybercriminals are charged little fines if any at all.

Kahoka (2015) observed that the negligence of some IT staff in organisations also contributes to the increase in cybercriminal-related activities. The negligence may be in form of revealing passwords that is meant to be confidential, to friends, using sensitive data in a public place and even storing data without protecting it. Cybercriminals can take advantage of such negligence and use it to obtain, manipulate and forge information. The negligence is very closely connected with human conduct (Kahoka, 2015). It provides a cybercriminal access and control to computer systems.

2.7 International Cyber Law

Cyber law is a term used to describe the legal issues related to the use of communication technologies, particularly the Internet (Y. Hu, Wood, Smith, & Westbrook, 2004). Cyber law denotes legal sanctions to cyber criminals in accordance with the provision of the laws. According to Kshetri (2006), cyber law

covers a wide range of rules and regulations pertaining to computers, software, hardware, data storage devices, the Internet, websites, e-mails and even mobile devices such as cell phones. According to Gemmill and Peterson (2006), cyber law is any law relating to protecting the Internet and other online communication technologies. Contreras-Castillo, Pérez-Fragoso, and Favela (2006) emphasized the needs for cyber law. The needs according to them include: ensuring integrity and security of information, security of government data, intellectual property rights, privacy and confidentiality of information and protection of online transactions.

The advancement of modern technologies, which plays a huge role in the way organisations and universities function, has raised the need for new cyber laws and the creation of multiple regulatory bodies across the globe. According to Ellison, Steinfield, and Lampe (2007), the law that regulates the Internet must be considered in the context of the geographic scope of the Internet and political borders that are crossed in the process of sending and receiving data around the globe. The unique global structure of the Internet raises not only jurisdictional issues, that is, the authority to make and enforce laws affecting the Internet, but also questions concerning the nature of the laws themselves (Rosenoer, 2012).

According to Broadhurst (2006), the areas that need to be considered when developing cyber laws include offences against confidentiality, integrity and accessibility of computer systems and data. They should also cover conventional offences perpetrated or facilitated by means of computer systems. In another related study, Krieger (2006) suggested that cyber laws need to cover areas such as human rights standards on criminalisation, tools for investigation of crimes involving electronic devices, orders for expedited preservation of data, orders for obtaining stored and real-time data, search and seizure of electronic evidence and guidance for addressing issues of concurrent jurisdiction. Cybercrime, computer-related crime, and strengthening of international, regional and national partnerships, including the private sector and academic institutions,

with a view of delivering enhanced technical assistance for the prevention and combating of cybercrime in developing countries also need to be addressed (Ojo, 2015).

Many countries highlighted that an expedited mechanism for international cooperation procedures in criminal matters involving cybercrime should be developed (Schaap, 2009). Although, most developed and some developing countries today have already established laws against computer misuse and cybercrime. Examples of countries that have already developed cyber laws includes: Malaysia, United Kingdom, United Arab Emirate, United States of America and Nigeria (Graham, 2010; Schaap, 2009).

2.7.1 Cyber Laws in Nigeria

Nigeria has become one of the leading countries in West Africa in the development and implementation of cyber laws (Ojo, 2015). The laws cover offences that include, among others; offences against critical information infrastructure, unlawful access to computer, system interference and interception of electronic messages (email, electronic money transfer) (Ojo, 2015). The law also highlights other offences such as tampering with critical infrastructure, willful misdirection of electronic messages, unlawful interception of computer data, computer related forgery, computer related fraud, and theft of electronic devices. In addition, Oke (2015) stated that the unauthorised modification of computer system, modification of network data, modification of electronic signature, cyber terrorism, fraudulent issuance of e-instructions, identity theft and impersonation are also covered by the laws.

The implementation of the Nigerian cyber laws enhances a more reliable business environment, which in turn, enables a stable and conducive market environment (Shariff, 2005). In its global leadership capacity, Nigeria has demonstrated a clear understanding of the importance of securing information technology and related information infrastructure as well as implementing

penalties for people and organisations that breach the Nigerian cyber laws (Ojo, 2015).

The Nigerian cyber act of 2015 provides a unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, protection and punishment of cybercrimes (Shariff, 2005). These acts also ensure the protection of critical national information infrastructure, promotion of cyber security, protection of computer systems and networks. The acts serve as the cornerstone in checkmating computer-related offences at federal, state and even organisational level. In these acts, the existing laws were modified to increase the penalties for some selected crimes. The severity of the penalty depends on the value of the information obtained and whether the offence is judged to have been committed (Oke, 2015).

Some of the cyber acts as provided by Oke (2015) include the following:

i. The Nigerian Cybercrime Act 2015 gives the President the power to designate certain Network Infrastructures (computer systems, networks and information infrastructure) that are vital to the national security and the economic and social well-being of its citizens, as Critical National Information Infrastructure.

ii. The Act also prescribes the death penalty for an offence committed against any of the critical national information infrastructure that leads to the death of a citizen.

iii. The Cybercrime Act 2015 also stipulates a fine of ₦10 Million or a jail term of 5 years for any cybercriminal found guilty of unlawfully accessing a computer system or network (depending on the purpose of the crime).

iv. The Act stipulates punishment ranging from a fine of not less than ₦2 Million or a jail term of not less than one year for the following forms of cybercrimes (Outlaws, Cyber-stalking and Cyber-bullying).

v. The Nigerian Cybercrime Act 2015 prohibits cyber-squatting and cyber-squatters are liable to conviction and imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.

vi. The Cybercrime Act 2015 mandates that service providers should keep all traffic data and subscriber information having due regard to the individual's constitutional Right to privacy, and they should take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

2.8 Security Control

Researchers have conducted different studies on security controls in relation to cybercrimes in universities. According to Ross (2005), security controls are countermeasures or safeguarding mechanisms that are used to avoid, detect, counteract, or minimize security risks to physical property, information and information systems. Stoneburner, Goguen, and Feringa (2002) stated that security controls could also be referred to as security protocols used on the Internet. Security protocols are sets of technical procedures that are applied to computer networks in order to ensure information availability, integrity, and confidentiality (Abdul *et al.,* 2014). Alfredo, Devide, and Riccard (2011) described security protocols as the communication protocols that uses cryptographic technology in order to protect organisational assets. In a university setting, there are a lot of assets that need to be protected against adversaries. These assets include information (student records, staff records, correspondences) and information system (application software, network equipment, computer hardware). Some researchers presume that, all the information stored in a university's database are assets that normally require proper protection.

Cochran (2007) and San, Kirstie, and Konstantin (2012) emphasized that information and information systems within the university setting need to be protected in order to ensure smooth operation of the university. The continuous development of new technologies and the convenience that is associated with

them warrant a switch from physical environment to virtual environment (i.e. cyberspace) in order to tap the benefits of the emerging technologies. Unfortunately, while this is happening, cybercriminals are also busy spying and seeking means of luring people into their traps in order to obtain vital information that can help them perpetrate their acts (cybercrime) (Bunker & Fraser-King, 2009). Expert across the globe are, on the other hand, putting concerted effort into providing measures that can help control or prevent the activities of cyber criminals (Obama, 2010). As found in the literature, security control measures can be divided into three; technical security controls, administrative security controls and physical security controls.

2.8.1 Technical Security Controls

To protect the university networks from cybercrimes, underlying technical security controls and controls must be considered. Technical security control uses technology as a basis for controlling the access and use of sensitive data throughout a physical structure and over a network. According to Sobell (2013), technical security controls are far-reaching in scope and encompasses technologies such as encryption, smart cards, network authentication, access control lists (ACLs) and file integrity auditing software.

Jensen, Schwenk, Gruschka, and Iacono (2009) further stated some of the technical security protocols that can be applied on the Internet to include Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), Virtual Private Network (VPN), IP Security (IPSec), Cryptographic system. These protocols are operated at different layer in the network (Bunker & Fraser-King, 2009). According to Aiello *et al.* (2002), when technical security protocols are properly implemented, effective, reliable, and private, communication can be achieved.

Furthermore, Aristotle (2012) stated that one of the best ways to tackle cybercrime technically is by using Cross-Domain Solutions. When organisations use cross domain cyber security solutions, they can ensure that exchange of

information adheres to security protocols. A Cross Domain Solution (CDS) is a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains (NationalInformationAssurance, 2006). The solution allows organisations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information (WordPress, 2006). Cross-Domain Solution also helps to keep the network and the systems safe. It also offers a way to keep all information confidential by using safe and secure domains that cannot be easily tracked or accessed (Chiu & Shu, 2007). According to Aristotle (2012), this security solution can be used by commercial and government institutions to ensure network safety while still making sure that users get easy access to the required information.

2.8.2 Administrative Security Controls

Organisations are trying to protect their data and network from thousands of daily intrusion attempts (Amit & Schoemaker, 2012). Technical protections alone are however not sufficient (Tavani & Moor, 2001). Educational institutions, just like organisations need to develop and implement cyber security plans and control measures that would clearly outline the best policies and practices for tracking and addressing cyber security threats to the institution's employees and students. Ciampa (2013) stated that for educational institutions to be successful in securing their resources, administrative control measures must be considered and implemented on the information and information systems of the institution. Administrative control measures as provided by Lemon (2006) include :

i. Assigning roles and responsibility to personnel who will be responsible for the university Internet security. Information Security Officer (ISO) is required to oversee organisations' compliance with policies and procedures regarding the security of information assets (Whitten, 2008). Universities, like any other organisation, are encouraged to assign personnel who will be in charge of

information and Internet security. The responsibilities of such personnel should include:

- Learning about threats, security trends and options.
- Planning, acquiring and implementing security safeguards.
- Helping other personnel understand Information and Internet security best practices and policies.
- Enforcing Information security best practices and policies with management support.

Even with the ISO in charge of Internet security, the ISO's success within an organisation or the university relies on management support (Karyda, Kiountouzis, & Kokolakis, 2005).

ii. Clear instructions, in the form of policies, should be made available to employees on what is expected of them while using computers and handling networking equipment. According to Carolina (2015), sensitive information is often protected by the University's law and/or policy. One of such policies is the Risk Manag*ement P*olicy. According to Stony (2015), one of the issues that need to be considered by a university when reviewing the value of its information and information system is risk management policy which serves different purposes, to identify, reduce and prevent undesirable incidents or outcomes and to review past incidents and implement changes to prevent or reduce future occurrence (Bruix & Sherman, 2011). Organisations follow different steps in ensuring the successful management of risks (cybercrimes). According to AustralianCatholicUniversity (2015), Risk Management can be successfully managed by using different approaches, but which mostly consist of the following:

- *Identification*: this step involves the identification of the risk events that may prevent or delay the achievement of the University's strategic goals and objectives.

- *Analysing*: in this step causes of risk are outlined. The impacts of existing treatments are outlined and analysed in order to assess the consequences and likelihood of the risk and determine the risk rating.

- *Treatment*: In this step treatments are implemented. Both existing and future treatments are implemented in order to prevent and/or mitigate the risk.

- *Monitoring*: in this step risks and treatments are monitored. The risks and their respective treatments are continually monitored and evaluated in order to maintain the effectiveness and appropriateness of the University's risk management.

- *Reporting*: in this step regular reports are provided. Regular reports and updates are provided in order to assure the University and key stakeholders that the risks are being appropriately managed and treated.

iii. Educating and creating awareness programs that make sure employees understand why Internet security is important for them and to the university community. Security awareness is a way of keeping employees and clients informed about good Information security practices (Lemon, 2006). Universities need to create security awareness programs for both employee and students. Lemon (2006) suggested security awareness programs around the training of staff, updates and reminders on policies, standards and best practices. Security awareness also includes regular and scheduled reviews to update existing software and hardware security measures (Torres, Sarriegi, Santos, & Serrano, 2006). Training and educating personnel is vital in order to have a strong Internet security system (Jensen *et al.,* 2009). Advocacy to the University Internet community is equally important. The advocacy could be in various ways, such as periodic lecture, seminars, workshops, distribution of handbills, pamphlets, electronic billboard notice, social media (e.g. Facebook, tweeter). Chen and Zhao (2012) stated that security awareness strategy for protecting sensitive information could be in the form of campaigns on how the users of university

network can protect the university network and their personal information against cybercriminals. These campaigns may include awareness on how to recognise phishing scams, use of strong password, regular update of software installed on the computer systems, use of licensed antivirus software, and strong firewalls protection on the computers. According to McCain (2015), security awareness in the form of training is one of the most important means of reducing security risks to information and information technology.

Sobell (2013) reported that, tackling cybercrime efficiently is not a one-man show. Essentially, strong and active partnerships and cooperation need to be established between the private sector, information security organisations, financial institutions and public institutions to investigate cybercrime, to supervise financial market transactions and to enforce laws. This is because, without efficient private-public cooperation, cybercrime will not be tackled effectively (McQuade, 2006). Universities should also try to forge partnerships with relevant agencies in order to prevent and manage cybercrimes.

2.8.3 Physical Security Controls

Physical security is a vital part of any security plan and is fundamental to all security efforts. This stems from the fact that without effective physical security plan, securing other assets such as databases, would be more difficult, if not impossible (Subashini & Kavitha, 2011). In addition, Garcia (2007) described physical security as the protection of building sites and equipment (all information and software contained therein) from any form of adversity that may arise. This protection requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders (Garcia, 2007).

Physical security is not limited to installing locks, bars, alarms, and having uniformed security guards. While these countermeasures are by no means the only precautions that need to be considered in the quest to secure information and information system, they are a perfectly logical places to begin (Yeh &

Chang, 2007). Physical security is another area that needs to be considered when reviewing the value of information and information systems of the University.

Subashini and Kavitha (2011) stated that, physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. Ortmeier (2009) also highlighted that, physical security may comprise protection of institutional assets from any incidence of fire, natural disasters, burglary, vandalism and terrorism.

2.9 Conclusion

In this chapter, the researcher reviewed related literatures on the concepts of cybercrime, types of cybercrime, Internet security protocols and security control measures. The literature reveals that various organisations and Universities fall victim of cybercrime, as such, proper management of information and Internet security protocols is vital to organisations and universities. Based on the literature reviewed, it is evident that the implementation of security controls and their rightful application in universities could guarantee the safety of university's information and information systems. Security controls could also deter cybercriminal attacks. The literature also shows that universities need to have full awareness and understanding of what they are trying to secure, the appropriate security controls to be applied and when to apply them.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Neuman (2013) stated that the methodology section of every study usually focuses on the process of research and the tools or techniques used when conducting a research. Many scholars highlighted the importance of research methodology in academic research. For example, Marczyk, DeMatteo, and Festinger (2005) stated that, in every research, the methodology section is important because it guides the researcher on how to ask and answer important questions relating to their research objectives. In this chapter, the discussion on the research methodology adopted in this study is presented. The theoretical framework, research design, location of the study, the population, sample and sampling strategy, procedure for data collection and analysis, the issue of credibility of the data are also all addressed in the chapter.

3.2 Research Methodology

Sekaran and Bougie (2010) described research methodology as a way of systematically solving research problems. In this study, the researcher employed qualitative method. Qualitative methodology allows the researcher to collect and analyse data using interview, focus group and/or observation. It also captures experiences and behaviours of people in natural settings. This methodology is deemed appropriate for this study because it captures the experiences of participants in Ahmadu Bello University as regards the effectiveness of security protocols in combating cybercrime in Ahmadu Bello University, Zaria. Creswell (2013) stated that, qualitative method allows for the examination of data with better understanding of the research problem as compared to using quantitative method. Using qualitative method, the researcher would be able to get more information from the study's participants, on the phenomenon under study (Liamputtong, 2009). Sekaran and Bougie (2010); Babbie and Mouton (2001);

Creswell (2013); and Viswanath, Brown, and Hillol (2013) also stated that, qualitative method is the best way to collect information about a phenomena from different perspectives.

3.3 Research Design

Research design is a systematic and organized way to solve a scientific-related problem (Wyk, 2013). It also articulates the kind of data needed for a research, the methods and procedures to be used in order to acquire and analyse relevant data so as to provide answers to the research questions. The research design ensures that the evidence obtained from various participants are well-structured in order to enable the researcher address the research problem with less ambiguity (Wyk, 2013).

This study adopted exploratory research design. The exploratory research design provides a work plan that serves as a source of new ideas, definitive explanations and rich insights into the phenomenon under study (Brown & Suter, 2012). Exploratory research enables the researcher to become more familiar with the phenomenon under study, especially when he/she has little or no knowledge of the research problem (Brown & Suter, 2012). It also elaborates on the “what and why” questions of a research. The exploratory research design is employed in this study to provide the needed insight and to understand the effect of security controls on cybercrime at Ahmadu Bello University.

3.4 Study Site

According to Sekaran and Bougie (2010), study site is a physical environment or place where the study is conducted. In this research, the study site is Ahmadu Bello University, Zaria. The University is one of the largest academic institutions in sub-Sahara Africa, situated in the city of Zaria. Currently, the university covers a land of 7,000 hectares and has 2 campuses, 14 faculties, 82 departments and 12 centers. The University has a data center hosting about 150 different servers

and several databases that contains different confidential information of both students and staff.

3.5 Population of the Study

Hungler and Polit (1999) refers to population as an aggregate or totality of all the objects, subjects or members that conforms to a set of specifications. For consistency, coordination and reliability, the researcher considered (in this study) the staff of the six different units under the Institute of Computing and Information Communication Technology at Ahmadu Bello University as the target population. These units comprise of Information Technology Academy (ITA), Management Information System (MIS), Computing and Academic Support Services (CASS), Research and Development (R&D), Software Development Unit (SDU) and Network Infrastructure and Security (NIS).

Table 3.1: Breakdown of the target population

S/No.	Units of the ICICT Directorate	Population
1	Information Technology Academy (ITA)	14
2	Management Information System (MIS)	19
3	Computing and Academic Support Services (CASS)	35
4	Research and Development (R&D)	10
5	Software Development Unit (SDU)	22

6	Network Infrastructure and Security (NIS)	23
Total Population		**123**

At the time of the study, the total population was 123 staff members of the ICICT Directorate. These populations deal with the University Network Security and Information Management.

3.6 Sample and Sampling Technique

A sample can be defined as a subset of the target population, whose characteristics are studied to gain a general view of the target population (Dessel, 2013). A sample size can be understood to represent the total number of participants, individual elements or units that have been carefully selected to take part in a research study (Yin, 2009). In this study, a non-probability sampling technique was used to select the sample from the population. According to Battaglia (2011), non-probability sampling technique is often used in situations where the selection of participants that make up the sampling frame is based on subjective methods. The non-probability sampling technique is composed of 4 sampling techniques which are: convenience sampling, quota sampling, snow-ball sampling, and purposive sampling (Battaglia, 2011).

Convenience Sampling: Convenience sampling (also known as availability sampling) is a type of non-probability sampling strategy that relies on data collection from a population based on the convenience of the researcher or the study's participants (Farrokhi & Mahmoudi-Hamidabad, 2012). Etikan, Musa, and Alkassim (2016) iterated that convenience sampling is a process of selecting subjects or units for examination and analysis that is based on accessibility, ease, speed, and low cost. Lam and Hsu (2006) further stated that, researchers use convenience sampling not just because it is easy to use, but because it also has other research advantages. For example, in pilot studies, convenience

sampling is usually used because it allows the researcher to obtain basic data regarding his/her study without the complications of using a randomized sample.

Quota Sampling: Quota sampling is a non-probability sampling technique wherein the assembled sample has the same proportions of individuals as the entire population with respect to known characteristics, traits or focused phenomenon (Battaglia, 2008). It is a sampling technique for selecting representative respondents from a group by virtue of allocating a proportion of the entire sample to different subgroups of the population (Battaglia, 2011; Polgar & Thomas, 2011).

Snow-ball Sampling: Snow-ball sampling is a non-probability sampling technique in which the participants of a study recruits other participants to participate in the same study (Noy, 2008). According to Browne (2005), snow-ball sampling is used where potential participants are hard to find. In snow-ball sampling, researchers used their own judgment to choose participants.

Purposive Sampling: Purposive sampling technique is a non-random sampling technique in which the selection of participants by the researcher is usually deliberate and or based on some considerations that suit the research objectives (Dessel, 2013). Tongco (2007) stated that purposive sampling is also known for producing reliable and robust data from participants. In purposive sampling, the researcher already knows what he/she wants and looks out for people/elements that would provide the needed knowledge and information (Battaglia, 2011). Hence, in this sampling method, the selection of participants is usually dependent on some distinct qualities and characteristics evident in the respondents (Tongco, 2007).

In this study, purposive sampling technique was adopted in the selection of participants that have the required knowledge to fulfill the criteria as required by the research problem.

3.6.1 Eligibility Criteria for Selecting Participants in the Study

Eligibility Criteria pertain to the characteristics that people in the population must possess in order to be considered as a participant in the study (Hungler & Polit, 1999). The eligibility criteria in this study were that, the participants had to be IT staff of the Institute of Computing and Information Communication Technology with a minimum of three (3) years working experience and they should have the required knowledge of cybercrime and security controls used on the university network.

Two (2) participants were selected from each of the units of the ICICT except in the Network Infrastructure and Security (NIS) unit where five (5) participants were selected. The selection of five (5) participants from NIS unit is due to the fact that the unit is responsible for evaluating and ensuring security efficiency and assist in the provision of security controls to strengthen security system on the information systems. The unit also coordinates with other units in order to evaluate and ensure accuracy on all server operating systems. The NIS unit is also responsible for implementing, managing, and maintaining network security processes and ensuring effective protective measures to upgrade systems for upkeep of information.

In this study, a total of 15 participants met the selection criteria for inclusion in the sample. The selected participants from the different units were experts in areas of network management, vulnerability assessments, penetration testing, IT management and cyber threat analysis.

3.7 Instrument/Source of Data Collection

The instruments used for data collection were semi-structured interview and Documentary sources. These sources (Interviews and case files) are forms of qualitative research methods that are often employed to obtain participants' perceptions, ideas and attitudes towards a particular phenomenon under study (Stuart & Headlam, 2008). Interviews, which could be conducted on a one-on-

one basis, are generally used to support and extend an investigator's knowledge on the thoughts and attitudes of the phenomena under study (Woods, 2011). Interview techniques can be structured, semi-structured or unstructured (Stuart & Headlam, 2008). Semi-structured interview was adopted in this study.

Semi-structured interview is one of the most appropriate means of data collection in a study (Brown & Suter, 2012). This is because it provides a broader perspective, more detailed explanation and richer insight on the phenomenon under study. It is a more frequently used interview technique and is guided by a framework that addresses vital themes rather than key research questions (Stuart & Headlam, 2008). Semi-structured interview involves the collection of rich and insightful data/information from participants through a casual or informal manner (Harrell & Bradley, 2009). Semi-structured interview also ensures that there is a certain degree of flexibility on the part of the researcher when responding to answers from the various participants, so that key themes and issues can be developed when they arise (Stuart & Headlam, 2008). Harrell and Bradley (2009) further stated that semi-structure interviews are often adopted when in-depth understanding of a phenomenon is required.

In this study, Interview questions were first sent to the fifteen (15) participants in order to allow them familiarize themselves with the interview questions. Then, a follow-up was made by the researcher after one week. The interviews were guided by an interview schedule. Interview was scheduled at the convenience of each of the participant, and the interview time were approximately between 45 minutes to one hour each. Interviews were recorded and notes were taken for further review of the interviewees' responses. Interviews were transcribed verbatim from audio to text. Furthermore, Case files (documents) were obtained from the security unit of the Ahmadu Bello University as another source of data.

3.8 Procedure for Data Analysis

The process of data analysis involves the drawing of inferences from the data gathered by the researcher. In this study, thematic Analysis was used to analyse data, because it enabled the researcher to identify, analyse and interpret patterns from the data collected from the participants. According to Nyoni and Segoe (2013) it is the most common form of analysing qualitative data, because it emphasises pinpointing, examining, and recording patterns (i.e. 'themes') within data. Nyoni and Segoe (2013) further stated that themes are patterns in a data set that are used to described a phenomenon associated to a specific research question. However, themes are patterns across data sets that are important to the description of a phenomenon and are associated to a specific research question. Moreover, thematic analysis is performed through the process of coding in six phases to create and establish meaningful patterns. According to Bondage, (2001) and Braun & Clarke, (2006), these phases are: i. Familiarizing with data, ii. Generating initial codes, iii. Searching for themes among codes, iv. Reviewing themes, v. Defining and naming themes, and vi. Producing the final report. For the data analysis (Empirical Support), (see Appendix C and D).

In this study, the researcher transcribed the recorded interviews (verbatim) and cleaned the data. Any information that could identify the participants was purposely not reported as part of the research findings in order to maintain the anonymity of the participants and confidentiality of personal information.

3.9 Theory Defined

According to the American Heritage Dictionary of the English Language, a theory is defined as a set of statements or principles derived to explain a group of facts or phenomena, especially the ones that has been repeatedly tested or widely accepted and can be used to make the predictions about a phenomena (Morris, 2004). Similarly, Wacker (1998) also stated that, a theory is a statement of relationships between units to be observed during experiment.

3.9.1 Theoretical Framework

Borgatti (1999) pinpointed a theoretical framework as a collection of interrelated concepts, in which a researcher determine what to be measured, and the corresponding relationships. In order to understand and explain how cybercriminals perform their activities, the researcher adopted Routine Activity Theory (RAT) as a theoretical framework to guide the study. The next section provides an in-depth discussion of the RAT framework as adopted for this study.

3.9.1.1 Routine Activity Theory (RAT)

The routine activity theory is one of the theories of rational choice and criminology that have been used extensively in research to explain criminal inclinations. Cybercrime is a type of these criminal inclinations. Even as cybercrimes are perpetrated online, they are criminal and as such RAT could be used to explain cybercriminal behavior. The theory has three constructs: suitable target, offender, and absence of suitable guardian (figure 3.1). This theory was proposed by Cohen and Felson in 1979 (Felson & Cohen, 1979) in their article titled “Social Change and Crime Rate Trends: A Routine Activity Approach”. The theory attests that “Crime occurs when there is an intersection in time and space of a motivated offender, an attractive target, and a lack of capable guardianship” (Felson & Cohen, 1979, p. 27). Further, as illustrated by this theory, crime can only occur when the following components come together in any given time and space:

3.9.1.1 (a) The presence of a motivated offender

Motivated offender is someone with criminal motive or reason to carry out a crime. This motive varies, based on the objectives of the offender. Alexander (2014) explained that an offender can have the motive to exact revenge on a particular organisational network or to steal or extort money from the target. Cybercrime is dependent on available opportunities to offend. If there is an

unprotected target and there are sufficient rewards, a motivated offender is likely to commit a crime (Plan, Plan-main, & Stones, 2017).

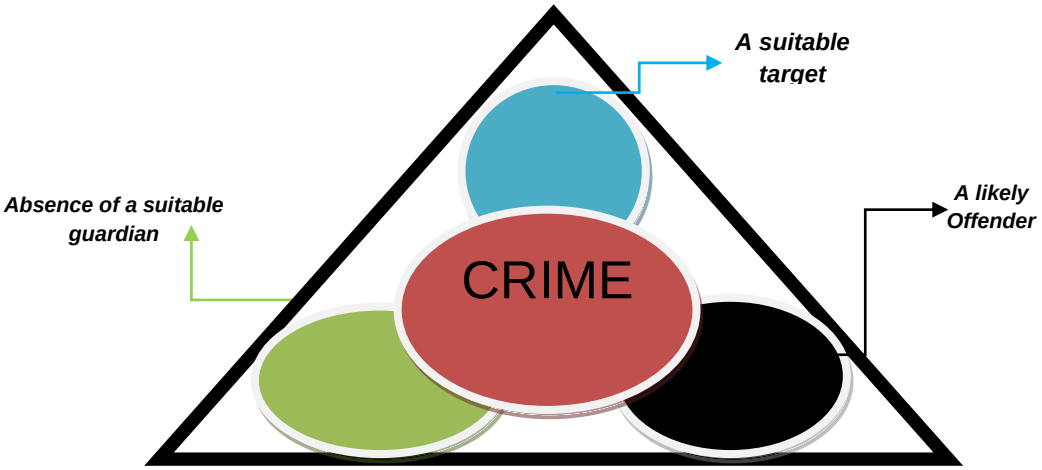


Figure 3-1: Crime Triangle

3.9.1.1 (b) An accessible target

This is determined and influenced by the vulnerability of the target. The more suitable and accessible the target, the more likely that a crime will occur. Alexander (2014) further stated that a person or organisation can become a target based on attractiveness or vulnerability. Cybercrime is likely to occur on targets that are easily accessible or networks that are not adequately protected.

3.9.1.1 (c) The absence of capable guardian that could intervene

A motivated offender is discouraged from committing an offense when he/he sees or knows that the target victim has a guardian. Guardianship can be physical presence of a person who is able to act in a proactive manner or in more passive mechanisms devices such as video surveillance or security systems. The physical security measures help limit an offender's access to suitable targets. Other security measures that could serve as guardian and also help in

protecting an individual or institution from being subjected to cybercriminals attacks include firewalls, antivirus, antispam, intrusion detection system.

From Fig. 3-1, it can be deduced that, if at least one of the actors is controlled (the offender, the target or the absence of capable guardians), the rate of crime could be reduced. However, managing all the three actors constitutes the most effective crime prevention mechanism.

In a study conducted by Pratt, Holtfreter, and Reisig (2010), it was shown that technology, coupled with the absence of a capable guardian can increase the convergence of motivated offenders and suitable targets, leading to an increase in cybercrime. Pratt *et al.* (2010) further stated that routine activity theory helps to understand the behaviour of cybercriminals, their personal characteristics and how online routine activities increase peoples' exposure to motivated offender.

In order for a theory to be considered useable, the theory must be empirically valid (Mustaine & Tewksbury, 1999). Mustaine and Tewksbury (1999) further stated that, this validity is determined by testing the theory in different circumstances using experiments to either prove that the theory is correct, or figure out if there are any shortfalls in it. Groff (2008) tested routine activity theory, and reported her findings in an article titled 'Simulation for Theory Testing and Experimentation: An Example Using Routine Activity Theory and Street Robbery.' She started off with the hypothesis that, as the time spent away from home increases, so does the chance that a criminal will commit a crime also increases. Rather than using real people in this experiment, Groff used a computer simulated model incorporating different geographical information as well as crime rates from these geographical areas. The researcher found that, crime follows at least 5 specific patterns.

Routine Activity Theory was also tested by Navarro and Jasinski (2012) but in relation to a different type of crime. Navarro and Jasinski (2012) used Routine Activity Theory to find out who has the highest risk to participate in cyberbullying.

According to them, cyberbullying came to the public in 2006 after a 16 year old committed suicide when he had been a victim of bullying through an online social networking site. The study of Navarro and Jasinski (2012) showed that the three constructs of the Routine Activity Theory are present while online. It has been found by Swan (2015) that routines activities can make crime easy and low risk, or difficult and risky, because opportunities varies over time, space, and among people, and even in organisations so too does the likelihood of crime. Parents tend to assume parental controls installed on a computer can act as a capable guardian. However, this is not the case. Parental controls cannot filter what young people convey on the websites they are allowed to access, such as their email or social networking sites like Facebook, tweeter. The tenets of this theory are based on a number of assumptions about the decision-making process and behavioural motivations. People decide to commit crime after a careful consideration of the costs and benefits of committing the crime. This consideration includes considering both personal factors, which may include a need for money, revenge, or entertainment, and situational factors such as the target/victim's vulnerability and the lack of guardians (Plan *et al.,* 2017).

3.9.2 Application of the theory

In this study, Routine Activity Theory was adopted because it can serve as a lens to explore the effectiveness of the existing security protocols used in Ahmadu Bello University to prevent cybercrime. The application of the theory to this study is explained below:

1st construct: attractive target: this could be a person, an object or an organisation. In this study, Ahmadu Bello University is an organisation that can be considered a target which can be attacked by cybercriminals. Hence, it is presumed that Ahmadu Bello University's Network could be infiltrated by cybercriminals at any point in time, especially if the network is considered an attractive target by cybercriminals. A target may come in contact with a cybercriminal searching for an opportunity or the target itself may exhibit certain

behaviour that may place it in contact with cybercriminals especially when there are no deterring mechanisms present to prevent it from being subjected to cybercrime.

The commission of cybercrime can be triggered by an increase in the number of routine activities on the Internet and the use of computer networks, thus making users of networked computers prone to cybercrime. The emergence of online transactions performed on the university's network gives rise to many potential victims (Selwyn, 2008). In this regard, the first construct of the theory is used to address the first research question which is set to identify the activities within Ahmadu Bello University that makes it an attractive target to cybercriminals. The construct is also used to identify the type cybercrimes that Ahmadu Bello University (target) could be susceptible to.

2nd construct: motivated offender: Predatory crime is a technique used by cybercriminals in order to secure their basic needs (Felson & Cohen, 1979). The action of cybercriminals may be intentional or unintentional, but often illegal. Cybercriminals use their technical skills and the opportunity of improper implementation and management of security protocols to commit cybercrime

Based on the second construct, it is assumed that offenders (cybercriminals) on the Internet may commit a crime by luring their victims into their snare. Unlike many theories that focus on why people commit crimes, RAT posits that in order for a cybercrime to take place there needs to be an offender with criminal inclinations and the ability to carry out the cybercrime. It does not really matter why individuals are motivated to commit crimes, what matters is that an individual with the inclination to commit a crime is in the right place to move against his or her target at the right time when there is no one around to stop him.

3rd construct: a capable guardian: this can be any security mechanisms that could intervene and prevent cybercrime from occurring. Weaknesses or improper management of these security mechanisms such as passwords,

tokens, antivirus, firewalls, and security protocols can influence cybercriminals to commit criminal activities. The security mechanisms can serve as guardians. This 3rd construct (i.e. capable guardian) was used to answer the third research question of the study. Based on the construct, the current weakness or strength of security protocols will have direct bearing on the prevention of cybercrime. Also, the success of a cyber attack on any network largely depends on the current, weakness or strength of the guardian on a network. However, even with the presence of the capable guardian in the form of the systems administrator and the security protocols, Ahmadu Bello University still experiences cybercrimes. In this regard, the third construct of the theory is used to address the third research question which is set to determine how effective are the security protocols used by Ahmadu Bello University in protecting their network from cybercrime. In a university, web servers and database servers can equally be affected if security protocols are not properly implemented and well managed. Therefore, it is in the interest of the university to improve its security protocols to regain the confidence of its end users. This section stands on the premises that the more effective the guardian is, the more difficult it becomes for cybercriminals to infiltrate a Network. Conversely, guardians' weaknesses are vulnerabilities that can be exploited.

3.11 Ethical Considerations

Before data collection, permission to conduct the study was sought and obtained from Ahmadu Bello University, Zaria (See attached, Appendix B). Subsequently, the University of KwaZulu-Natal research ethics' committee issued an ethical clearance letter specifying that the research follows the institution's research ethics (See attached, Appendix C). In addition, the researcher clearly indicated to the participants the objectives of the study and the nature and purpose of the research. It was also explained to the participants that their participation is voluntarily. Prospective participants were also assured that confidentiality and

anonymity will be upheld by ensuring that any personal identifying information is not divulged in the research outputs.

3.12 Conclusion

This chapter described the research methodology used in this study. The chapter highlighted that a qualitative research design was adopted in this study coupled with a purposive sampling method. The theoretical framework adopted in the study was discussed and the guiding ethics for the study was also presented. The following chapter presents the findings and their corresponding analysis.

CHAPTER FOUR

DISCUSSION AND PRESENTATION OF RESULTS

4.1 Introduction

In the preceding chapter, the research methodology, research design, and the instruments used for data collection were discussed. The theory underpinning the study was also discussed. In this chapter, the analysis of data gathered from the responses of IT personnel of the six different units of the Institute of Computing and Information Communication Technology (ICICT) of Ahmadu Bello University is presented. The chapter also demonstrates the extent to which the research questions presented in this study have been answered.

4.2 Analysis

This section presents the results of the analysis of the interview responses relating to the first, second and the third objectives of the study. Thematic analysis was used to systematically analyse the responses. The thematic analysis of data in this study followed the guidelines provided by Braun *et al.* (2014). Hence, the findings of the study were presented according to the objectives of the study. The first objective highlights the types of cybercrimes that Ahmadu Bello University Network could be susceptible or exposed to. The second objective identifies the areas of Ahmadu Bello University's Network that is vulnerable to cybercrime. While the third objective is to determine the security protocols that can be used to effectively manage Ahmadu Bello University's Network from cybercrime.

The analysis section also presents the identified themes in relation to the study's objective, and the corresponding discussions by the participants, around the themes. These findings are further discussed in the context of the literature and

the guiding theoretical framework adopted in this study. The themes identified in this study, in relation to the objectives of this study are discussed below.

4.2.1 Objective 1: To Determine the Types of Cybercrimes that Ahmadu Bello University Network could be Susceptible to.

The first objective of the study was to determine the types of cybercrimes that Ahmadu Bello University Network could be susceptible or vulnerable to. Vulnerability in information system is a flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect organisation's operations or assets. The exploitation of vulnerability often affects the confidentiality, integrity or availability of information and information system (NIST, 2010). From the responses of the participants in this study, the common types of cybercrime that Ahmadu Bello University Network is susceptible to are categorised into social engineering attacks, denial of service attacks, Malware, pharming attacks, SQL injection and cross-site scripting attacks, website defacement, and port scan attacks.

4.2.1.1 Social Engineering Attacks

Social engineering is a type of cybercrime attack that Ahmadu Bello University Network is constantly and continuously exposed to. Social engineering attacks are often aimed at manipulating users into divulging relevant information that would help cybercriminals attack a particular network (Irani *et al.,* 2011). Anderson (2008) in his study explained that social engineering is a psychological manipulation of people into performing actions or divulging confidential information. The manipulation is by gathering information (e.g. staff or students' details) and using such information for fraud or system penetration.

A participant from the network infrastructure and security unit stated that cybercriminals have at some point used social engineering techniques to

enhance Advanced Persistent Threat (APT) attacks in order to cause damage to the university network and steal valuable data or reach a particular target. According to another participant, from the same unit, most cybercriminals employ social engineering technique at the initial stage of an attack, and they use the information obtained through this means to create an opening for executing more sophisticated forms of cybercrimes. Participants in this study felt that social engineering attacks are the most common techniques that cybercriminals are using to attack the university students, staff and network. They also agreed that the common types of social engineering attack affecting Ahmadu Bello University Network are phishing attack, shoulder surfing, and password sniffing.

Phishing attacks: A participant identified phishing attacks as a type of cybercrime affecting the University. According to Kaspersky (2013), phishing is a malicious attack that involves the creation of false website by a cybercriminal before proceeding to using various social engineering techniques to attract targets to the website. Popper (2013) further explained that, it is when a malicious party sends a fraudulent email disguised to look like a legitimate email, often purporting to be from a trusted source. The message in such email is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware on the user's device (Rouse, 2010). A phishing attack can be seen as a success once a target clicks on the fake link that redirects the target to the false website (Symantec Corporation, 2014). An investigation by Junxiao and Sara (2012) pin pointed the fact that most educational institutions' information systems and some social media websites are the most targeted by phishing campaigns.

A study by Chen *et al.* (2011) reported that 89% of cybercrime offences in universities are committed through phishing attacks. Similarly, respondents in this study also identified phishing as a prevalent cybercrime affecting Ahmadu Bello University. It was explained by one of the respondents that educational institutions are targeted by cybercriminals because of the valuable information

maintained by the institutions. This is similar to a study by Pratt *et al.* (2010) where they reported that phishing attack is on the rise and it is increasingly affecting many organisations and educational institutions alike. Some of the information targeted at educational institutions includes intellectual property and databases that contain the information of employees and students that can be used for identity theft and fraud.

Shoulder Surfing: Shoulder surfing was identified by participants as a type of cybercrime experienced on the university network. According to Wiedenbeck *et al.* (2006) and Gao *et al*. (2010), shoulder surfing refers to a direct observation, such as looking over a person's shoulder in order to obtain confidential information. Wiedenbeck *et al.* (2006) further stated that, shoulder surfing is done for no reason other than to get useful information from unsuspecting victims. In their study, Kumar *et al*. (2007) stated that shoulder surfing can also be described as the practice of spying on the user of a cash-dispensing machine (i.e. ATM) or other electronic device in order to obtain sensitive information such as personal identification number, password. A participant from Research and Development unit stated that “Criminals use to visit most of the digital centres within the university and watch users while entering their log-in credentials in order to get the victim details”. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. Shoulder surfing is an effective way of getting information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form online, or enter a PIN number at an ATM machine, or use a calling card at a public pay phone (Kumar *et al.,* 2007).

Participants stated that there had been reports from students that when they were doing their online registration, people stood by their side in what they (i.e. the students) believe was an attempt to observe/spy carefully over their shoulder so as to get valuable information. Tari *et al.* (2006) in their study stated that, shoulder surfing can be done at a distance using other vision-enhancing devices

such as binocular, miniature closed circuit camera. If the cybercriminal carrying out shoulder surfing was successful, sensitive information such as user name and password of students will be obtained, and which can be used by cybercriminals for furtherance of their attack.

Password Sniffing: Responses from the interviews shows that password sniffing is a form of social engineering. One of the respondents explained that password sniffing is a technique used to gain knowledge of passwords. It involves monitoring traffic on a network to pull out sensitive information such as users' password. A respondent remarked that this crime is usually perpetrated by users with the technical know-how skills of managing network traffic. Lee *et al.* (2009), similarly, explained that password sniffing is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. A study by Abbas *et al.* (2006) reported that cybercriminals also use password sniffing software to scan incoming and outgoing network traffic and records any instance of a data packet that contains a password.

4.2.1.2 Denial-of-Service (DoS) Attacks

Apart from social engineering attacks, another cybercrime that participants attested to is the denial of service attacks. A respondent stated that "Denial-of-service attack is another cybercrime type that the university's network has been exposed to". Participants stated that cybercriminal adopt DoS attacks mainly so as to make the university network resources unavailable to staff and students. According to Burden and Palmer (2003), denial-of-service attacks are usually designed to disrupt the access and use of Internet resources from legitimate users. Investigations by Pilling (2013) showed that universities globally have lost valuable information to denial of service attacks. This losses occurred either through the disruption of Internet access or through the illegal utilisation of Internet resources.

Saravanan and Asokan (2011) stated that denial of service attacks occur when a cybercriminal attacks the server of an organisation by loading them with millions of spoof messages. The large amount of spoof messages eventually consumes all the available bandwidth of the organisation. The servers that are loaded with the spoof messages often crashes or freezes at some point, making it difficult for legitimate users to access them (Burden and Palmer, 2003).

Participant indicated that there are cases when the university servers respond very slowly to the request of users. This, they opined is as a result of the demands on the servers. This huge amount of data is mostly sent through amplified attacks, and the limited processing capacity to handle the huge amount of data. For example, instead of sending 4Mix (a Mix is an Internet traffic model that describes user behaviour using a number of systems) of web traffic, an attacker can send 20Mix; the line would be congested and there would be slower response by the server. Attackers often aim at bandwidth, memory or CPU, depending on what they are trying to obtain.

4.2.1.3 Malware

Participants identified Malware as another cybercrime that ABU Network is susceptible to. Malware (known as malicious software) is any program or file that is harmful to a computer and/or computer network. Malware includes computer viruses, ransomware, worms, Trojan horses and spyware (Bergman *et al*., 2013). These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

Botnet Attack: A form of malware that participants indicated is botnet. According to Bleaken (2010), botnet is a program that facilitates an attack from coordinated systems. The botnet is a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. these bots

form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks. A participant remarked that in 2016, computers were infected with malicious software sent as e-mail spam to several computers on the university network. This brought down the e-mail server for several months. This eventually led to the close-down of the e-mail server for many months, with lecturers not able to read their mails. Sérgio *et al.* (2012) also believed that the main purpose of botnets is for cybercriminal to employ enslaved computers for malicious activities in order to steal confidential information, disrupt service and carry out identity theft. The effect of botnet attack is disastrous and often lead to damages to organisational information systems, and loss of trust by Internet users (Gercke, 2012).

4.2.1.3 (b) Means of Malware Distribution

Malware distribution can occur in many different ways. According to OECD (2007), malware distribution refer to the means in which malware is propagated. Examples of means through which malware is propagated include; USB devices, Internet Relay Chat, Bluetooth, e-mail. In line with this, the interviewees in this study pointed out that the most common means of malware distribution on the university network is through plugging in USB devices with malicious content, and Internal Users crime.

Plugging in USB Devices with Malicious Contents: Most of the participants expressed that USB device is sometimes employed by cybercriminals as a means of installing malware on the university network. These devices could be Flash Drives, Phones, Digital Cameras, and Biometric devices for thumbprints. Plugging in these USB devices with malicious content (like viruses and worms) in order to get access to the university network sometimes requires paying a disloyal employee some amount of money or the use of computers on the university network. These computers include computers used in the Computer Based Test (CBT) Centres and the computers in the MTN Net Library.

Distribution by Download: Participants explained that malware can also be distributed by download of free software (from uncertified websites and websites that are censored/blocked by the administrators of the network), by users of the university network. Manuel *et al.* (2009) stated that attacks in the form of distribution-by-downloads is any download of software programs that occurs without a user's authorisation or knowledge. In a typical distribution-by-download attack, merely visiting a web site that embodies the malicious content can result in the infection of users' machine or device with malware which, as an after effect, often enslaves the user's machine to become a member of a botnet (Manuel *et al.,* 2009, Marco *et al.,* 2010). The malicious code or program that is installed for the execution of the attack then has typically full control over the user's computer system (Marco *et al*., 2010). Another participant from the software development unit (SDU) stated that attacks in the form of distribution-by-download is any download of files, images, and documents that occurs without a user's authorization. For example, pornographic videos, images and documents are blocked from users by the network administrators.

Internal Users: Participants explained that internal users within the university network aid the distribution of various kinds of malwares in organisations via the use of malicious software. Respondents stated that most internal fraudsters are often very knowledgeable about the systems they want to exploit. As supported by Hemavathy *et al*.(2005), internal perpetrators are dangerous to an organisation because most of them possess exclusive and administrative rights to organisational resources. This enables them to avoid being detected by the various security mechanisms available on the network. One of the cyber security analysts stated that: "Attacks aided by cyber channels against enterprises could either be internal or sneaker based. In the case of internal attackers, the attackers have the necessary authorisation to Information Systems, know how the system works and therefore find it easy to use the system to their advantage. However, some respondents stated that internal fraudsters are in some cases

not careful or experienced enough to completely remain anonymous during the period of their activities, and usually end up being caught.

4.2.1.4 Pharming Attacks

Responses from the participants identified pharming as a type of cybercrime affecting the University. A participant opined that pharming is common crime during Admission period at Ahmadu Bello University. Targets are directed to web pages controlled by the cybercriminals and are asked to pay money to be given admission into the University. According to Gercke (2012), pharming is a cyber attack intended to redirect a website's traffic to a fake website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into real IP addresses (GFI, 2009). According to Robert (2015), pharming requires unprotected access to target a computer, such as altering a customer's computer IP address. Once a victim is lured to the website, an unpatched computer would download a Trojan horse in a file called "iexplorer.exe" from the cybercriminal server. The victim's computer displays an error message and recommends that the user shut off their firewall and antivirus software. Without the firewall the victim's computer becomes vulnerable. When the user visits any of the targeted banking sites, they will be redirected to a mock-up of the bank's Web site. This site then collects the victim's login credentials and transfers them to the criminals. The victim is then passed back to the legitimate site where they were already logged in, making the attack invisible.

4.2.1.5 Website Defacement Attacks

Participants stated that website defacement is another form of attacks that affect the university network. Website defacement is an attack that changes the visual appearance of the site or a webpage. These are typically the work of cybercriminals, who break into a web server and replace the hosted website with

one of their own (Alhamed and Alsuhaibany, 2013). A participant explained that the new content on the website attracts the attention of the victims with the intention to motivate and lure victim into supplying the necessary information that could be used against them. According to Hinckley *et al.* (2012), this attack could be in a form of denial of service attacks, port scan attack, or through SQL injection and cross site scripting attacks.

4.2.1.6 Port Scan Attacks

Walter *et al.*(2011) stated that port scan is viewed as an attack technique that dispatches legitimate user requests to a range of server address ports on a network host, with the aim of discovering an open or active port (e.g. File Transfer Service (FTP)). Once an open port or service is discovered by an attacker, the computer with the open port can be easily compromised, infected with a virus or lose valuable data (Walter *et al.,* 2011). The responses of the participants indicated that malicious programs capable of port scanning were seen to be frequently used by attackers to exploit vulnerabilities in the university network. One of the participants stated that: “the university network has seen lots of port scans on the server infrastructure side. The university network has also seen lots of "SYN" programs running on their web service that are constantly looking for vulnerabilities to exploit.” According to Bogdanoski *et al.* (2013), A SYN program is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target’s system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Participants felt that the risk of port scan attacks is often common with the web servers of the university network involved in creating port connections. One of the participants stated that: “After building a secure architecture and acquiring the necessary monitoring software, it would be very easy to know when a web server is port scanning a virtual box”. Since a virtual box only makes SQL connections on a particular port, an attempt by a cybercriminal to use web server to make connections on different ports or search for different host should

immediately raise a red flag as a result of the network security protocols monitoring software.

4.2.1.7 SQL Injection and Cross Site Scripting Attacks

SQL injection is a type of exploit whereby the cybercriminal injects Structure Query Language (SQL) code through a web application in order to gain access to recourses, or make changes to data (Awodele *et al.,* 2012). Here, the attacker injects SQL commands to exploit non validated input vulnerabilities in a web application database backend and consequently execute arbitrary SQL commands through the web application. Because programmers use sequential commands with user input, it makes it easier for cybercriminals to inject commands (Kar and Panigrahi, 2013). From the responses of the participants, it was reported that, SQL injection and Cross Site scripting attacks are also techniques used by cybercriminals in order to obtain valuable information from the university network. One of the participants asserted that, the university network experienced SQL injection in 2015 were some students changed the content of the website in which about 52 students were lured into paying their school fees into different account. Symantec (2012) believed that cross-site scripting and Structured Query Language (SQL) injection techniques are the most widely used attack methods by cybercriminals. Adam *et al.* (2009) believed that SQL Injection and cross-site scripting attacks (XSS) are common types of attacks that can be employed by an attacker to craft input to a target application in order to gain access or alter user data, and execute malicious code. Etienne (2008) stated that organisations should always validate user supplied data, enforce data types for all inputs, employ the least privilege rule, filter input data via white-list and black-list filtering, snort-based solutions, and host based IDSs. This is in order to censor the types of content that are allowed for downloading by the different categories of users of the network.

With respect to Cross site scripting attacks, Philipp *et al.* (2007) stated that cross-site scripting can be prevented in an organisation by properly validating

input from users, employing static analysis on the server side of an organisation, and deploying anomaly based intrusion detection systems in organisations. In a typical drive-by-download attack, merely visiting a web site that embodies the malicious content can result in the infection of a user's machine or device with malware which, as an after effect, often enslaves the user's machine to become a member of a botnet (Manuel *et al.,* 2009, Marco *et al.,* 2010). The malicious code or program that is installed for the execution of the attack then has typically full control over the user's computer system (Marco *et al*., 2010). Ahmadu Bello University Network remains vulnerable to cyber piracy attacks except if there are adequate security measures in place to prevent the depletion of resources on Information Systems by cybercriminals. The presence of suitable target as a construct of the routine activity theory stipulates that networks without adequate and capable security protocols in place would often be vulnerable to cybercrimes (Felson and Cohen, 1979). The responses of the various respondents, in line with the theme on the types of cybercrimes prevalent on the university network, provide answers to the research question that seeks to determine the types of cybercrimes that Ahmadu Bello University Network could be susceptible to.

4.2.2 Objective 2: To Identify the Areas of Ahmadu Bello University's Network that are Vulnerable to Cybercrime

This objective seeks to identify the areas in which the university network is vulnerable to cybercrimes. Identifying parts of the Network that are vulnerable will highlight areas that need more attention by the management of the university in order to increase security measure.

University networks have become an attractive target to cybercriminals (Sterbenz *et al.,* 2010). By the nature of universities' operations, their networks have a large number of transient users, making it more difficult to detect and respond to incidents (Osuagwu *et al.,* 2010). It is clear that any information gathered on staff and students may not be relevant at the time of attack, but may form very real

and useable human intelligence on notable individuals in the future that would lead to cybercrime (Lenhart *et al.,* 2001).

In cybercrime, areas of vulnerabilities are always targeted by cybercriminals. Cybercriminal are always on alert to such vulnerabilities and are always online waiting for such opportunities.

The routine activity theory explains that one of the necessary conditions for crime to occur is the availability of suitable target (Felson and Cohen, 1979). The vulnerabilities of Ahmadu Bello University's Network provide cybercriminals with such targets. The major target areas at Ahmadu Bello University are presented in below.

4.2.2.1 ABU Registration Portal

The areas of the network that are vulnerable to cybercrimes are categorised into the following.

i. Admission Page

ii. Accommodation Page

4.2.2.1 (i) Admission Page

This category emerged from the narratives of the participants of this study and from the Security Case Documents from the Security Unit related to areas of Ahmadu Bello University Network that are vulnerable to cybercrime. According to the responses of the participants, at the beginning of each academic session, meetings are held to warn the staff of the ICICT Directorate from involving themselves in any criminal activities in regards to admissions cases. Examples are always given about the members of staff who have indulged in such activities.

Participants remarked that the major time when there is always a problem on the network is during the beginning of new sessions of admissions. During these times, cybercriminals often put up websites that resemble that of the university just to lure victims to pay some amounts of money towards their registration and accommodation. One of the reviewed security case document corroborates this narrative. The document reported the case of a staff member of the ICICT directorate that was caught granting access to the accommodation page of the network to some students so that they can click for bed spaces from the accommodation page illegally during the 2015/2016 session. The issue of allocating rooms or accommodations to students in universities is rampant. From the Case file analysed, a staff member of the university was also caught hacking the university's portal so as to print fake admission letters for some students. Similarly, Security case document alleged a staff of the MIS Unit was brought to the security unit for breach of security protocols and connivance with some students of the university to illegally allocate rooms and print admission Letters.

4.2.2.1 (ii) Accommodation Page

This subcategory emerged from the narratives of participants in relation to areas where the university's network is vulnerable and also from the analysis of the case files from the security unit. From the responses of the participants, it was opined that there is a limited number of accommodation spaces hence the accommodation page has always being compromised because cybercriminals look for ways to gain access to this page so as to take advantage of the space limitation and make profit of the situation. Similarly, it was also discovered that during registration exercise, the traffic to the page is so high as students are on the page trying to get accommodation. This usually increases the vulnerability of the page. Security case document reported the case of accommodation racketeering during the 2016/2017 session of the university. The case was reported on the 26th November, 2016 where the syndicates illegally allocated rooms to students by hacking the university's accommodation portal.

This finding is similar to a study conducted by Lifars (2016) where it was reported that cybercriminals targets university registration portal where students use their bio-data for registration.

4.2.3 Objective 3: To determine the Security Protocols that can be used to Effectively Manage Ahmadu Bello University's Network from Cybercrime

This objective focuses on suggesting measures that can help with the management of the university's network from cybercrime activities. Each of the identified sub-themes from the interviews regarding the prevention of cybercrimes are presented. These themes are then tied to the literature and the theoretical framework of this study. There were two major sub-themes identified from the narratives of the participants of the study. The sub-themes are Security Measures, and Security Tools.

4.2.3 Cybercrime Control

Cybercrime and its effects can be managed if the correct preventive measures are taken. The following are some of the preventive measures that can prevent cybercrimes.

4.2.3 (i) Cybercrime Control Measures

Cybercrime refers to illegal activities that take place on the Internet (Hassan *et al.,* 2012). These include fraud, spamming, identity theft, distribution of computer viruses, cyber stalking, denial of service attack, social engineering attacks, port scan attack. Most people and organisations fall victim to these crimes, but the use of proper cybercrime control measures can help in mitigating these illegal activities (Ani, 2011, Hassan *et al.,* 2012). According to Shinder and Cross (2008), cybercrime control measures are the application or use of technical or administrative security controls on organisational network in order to prevent cybercrime from occurring. Participants in this study explained that for

cybercrime to be controlled, applications of effective control measures are necessary. The participants further indicated that cybercrime control measures such as antivirus software, password authentication, anti-phishing software, and firewall are some of the security measures that are effective in the management of cybercrime on the Ahmadu Bello University Network. A study conducted by Anderson *et al.* (2013) also indicated that to avoid cybercrime on organisational networks, control measures such as use of strong password, antivirus software, firewall, virtual private networks have to be properly in place.

4.2.4 Security Measures

In this study, the participants indicated that Ahmadu Bello University Network is susceptible to cybercrime. Some of the cybercrime experienced by the University include social engineering, denial of service attack, malware, pharming attacks, SQL injection and cross-site scripting, website defacement, and port scan attacks. The findings of this study also shows that the use of security measures such as firewall, antivirus software and password authentication have been effective in managing cybercrime activities across the university network. In agreement to these security measures being effective in managing cybercrime within the university, Lazenby (2012); Brewer (2014) and Brynjolfsson and McAfee (2014) also identified these security measures as being effective in preventing cybercrime from happening. Some other security measures identified by the participants of these study are malware defenses, security audits, penetration tests, controlled use of administrative privileges, incident response capabilities. In the study of Brynjolfsson and McAfee (2014) it was also stated that routers and switches can be used to effectively block current and emerging high-priority cyber-attacks and threats on a network.

4.2.4 (a) Common Security Baselines

Common security baselines, as identified in this study, as a means of mitigating vulnerabilities also conform to the study of Stein (2008), stated that technical measures provide the needed procedures for addressing vulnerabilities in

various software applications/products. Security baseline is a set of basic security objectives which must be met by any given service or system (Yong-Hong, 2011). Proper patch management procedures were seen to be amongst the common security baselines identified in this study. Participants were of the opinion that attackers often attack the server infrastructure on the university network once the proper patching procedures for the software applications and OS is fail to be implemented. In line with this response, Stouffer *et al.* (2011) suggested the use of proper patching procedures for mitigating cyber-attacks on various software applications and operating system platforms. It was stated by one of the participants that an emphasis on proper patch management procedures would go a long way in securing the University's network from cybercrimes. This patch management tasks include maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures such as specific configurations required. It was also suggested that system administrators and network engineers take simple steps such as performing backups and testing patches on non-critical systems prior to installation, so as to avoid cybercrime related losses.

Participants were of the view that vulnerability assessments and penetration testing should be employed by security firms in order to examine the span of a client's network or security posture, so as to identify loopholes that can be exploited by an attacker. Most penetration testing tools can either be used to prevent attacks or sometimes used by cybercriminals for cybercrimes (Christian, 2012). The top penetration testing tools that can be employed by the University are Metasploit, n-map, burp, burp-proxy and some decompiler tools. The University can also construct small penetration testing tools using programming languages such as python, pearl or bash that would enable the testing of a specific issue on a client's network. While vulnerability assessment looks at the organisation's security posture and then tries to identify vulnerabilities that might

expose the organisation to future attacks. Participants were also of the opinion that regular Vulnerability assessments on web applications of organisations can be instrumental in preventing high-level attacks such as espionage, sabotage and malware infections that are often aimed at compromising the services and hosts of organisations.

In relation to penetration testing, respondents explained that more sophisticated attacks in the form of sabotage and espionage that aim to compromise an organisation's web services and hosts can be prevented by conducting regular penetration testing. This penetration testing often encompasses the simulation of attacks against an organisation's network in order to determine vulnerable points in an organisation's network. According to Missiaen *et al.* (2015), a successful simulated attack during penetration testing against an organisation's network serves as an indication to the organisation that its security mechanisms are not well-aligned. The misalignment between the organisation's security mechanisms can easily be exploited. The findings identified under penetration testing and vulnerability assessments are also in line with the capable guardian construct of the RAT. Based on the construct, a university that does not conduct assessments and tests on their networks would constantly remain vulnerable to cybercrimes (Felson and Cohen, 1979).

From the participants' responses, it was deduced that the security measures that can be conducted on the University network include access control, monitoring and logging, robustness testing and deployment, configuration of network devices, and software application.

Access control: This form of assessment was identified to be helpful in controlling and restricting access on the University's network. Cybercrimes occur on networks only when the cybercriminal has access. Access control will limit this access by decentralizing full access to multiple administrators. This would help prevent any staff that is tempted to grant illegal access. It also helps to restrict access remote access to the university's network.

Monitoring and logging: The Monitoring is a process that oversees all the tasks and metrics necessary to ensure that the approved and authorized activity is within scope, and secure so that the activity proceeds with minimal risk. Monitoring is a continuous process performed throughout in every organisation. In this regards, the University would setup a monitoring system to check device status so as to have complete visibility and control. The monitoring also allows the University to monitors all the entities which are communicating with each embedded device and ensure they are allows to interact. The logging on the other hand, also allow the deployment of intrusion detection system (IDS) for any traffic on the network by ensuring that it does not impact the expected functionalities of the information systems. This could be done through granting access to users of the university's information systems.

Robustness testing and deployment: These measures check the effectiveness of the built-in device security systems (e.g. firewall, password checking, etc), it also scan the devices that form nodes on the network which can be used as potential vectors of attack and make sure that there are no hidden vulnerabilities on the network.

It was also evident that a good security measure for the University network is to have reputable and up-to-date anti-virus software installed. Participants also indicated that the removal of default passwords and prevention of employees from using their mobile devices and the use of wireless mobile connections to connect to the university network would go a long way in limiting the exposure of critical university information or Information Systems from various kinds of attack.

4.2.4 (b) Incident Response

According to Cassey (2011), incident response plays a vital role in mitigating cybercrimes on the organisational network. Respondents indicated that the ability for a university just like organisations to quickly respond to attacks and take strong steps could help to reduce the level of attack on its network. The speedy

response involves how quickly the university can detect and responds to an attack. However, it is also often dependent on the quality of the incident response process adopted by the university. For example, if the university network is attacked, how quickly can the university confirm that there is an attack on the network, and how quickly could the university shut down the network and reboot it again. Ahmad *et al.* (2012) opined that when an organisation or university detects an attack or a piece of malware, the incident response team would enable effective analyse of their findings. The Incident response team also helps a university to easily eradicate a malware infection.

Risk analysis: The Participants identified risk analysis as a means of securing the University network from cybercrime. Majority of the participants stated that the university should constantly simulate attacks on the network in order to access the level of risk on the University network. Risk analysis helps to design a secure model that can adequately help to a line with the operations of university activities. Participants stated that, simulating attacks on the employees in the university would create some level of perspective on how much risk the university or the employee are exposed to in case of an attack. Simulated attacks would also help to determine the kind of user education required by the employees. Furthermore, it will be useful in determining whether there is a need to improve on response capabilities to attacks, and identify other steps (from a more technical perspective) for mitigating attacks

4.2.4 (c) Training and Constant Awareness

Participants indicated that education and awareness initiative are very vital to employee in the University. Training and awareness make employees more knowledgeable about the various attack methods/techniques of cybercriminals. User education has made it possible for employees to avoid clicking unknown links, opening attachments from sources they do not know or carelessly connecting to an open wireless network with their mobile phones. It was also

deduced from the participants that training employees helps them to be more security conscious and to be pro-active.

Participants stated that the training programs carried out by ICICT Directorate should not just be all about security at an IT level or technical level. The training programs should also involve teaching employees to be security conscious. Employees should be able to ask themselves questions such as: Why are these websites blocked from users on the network? Will this link not lead me to malicious content?

In relation to the training of employees to think and be proactive, respondents expressed that the University should teach their employees to ask questions and think about the implications of their actions online when faced with uncertainties. In agreement with this finding, Symantec Corporation (2014) stated that regular security skills assessment and appropriate training of employees would help mitigate various attacks. Hence, Universities should constantly enlighten and train users on essential security protocols, so as to reduce human errors to the barest minimum. Similarly, Kapp (2012), immediately an individual is hired by an organisation, a considerable amount of time should be dedicated to training and educating the new intake on the organisation's security policies and procedures.

4.2.5 Security Tools

According to Fenwick et al. (2009), security tools can be classified based on how it would be employed in an organisation. These tools can be grouped into host or end-point based tools, and network-based security tools (Fenwick *et al.*, 2009, Karen and Theodore, 2009).

4.2.5 (a) Host or Endpoint Based Tools

The respondents of this study established that the three types of host or endpoint based tools used in the University network are firewall, anti-virus software and password authentication.

Firewall: According to Medeiros *et al.* (2009), a firewall enforces access control policy between two or more networks. A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules (Wasserman and Baker, 2011). A firewall can be seen as a network security system designed to prevent unauthorised access to or from a private network. According to Margaret (2016), firewall is frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet, especially intranets.

A study by Wool (2010) pinpointed that firewalls are configured to protect against unauthenticated interactive login from outside the university's network, as such, it helps to prevent cybercriminals from accessing the entire network. The respondents indicated that firewall is an effective cybercrime control measure used on the University network. Thus, participants suggested that firewall is a common cybercrime security measures used on the University network. This suggestion is similar to a study by Liu and Gouda (2008) where they reported that firewalls help universities across the globe in preventing cybercrime from occurring. Similarly, a study by (Margaret, 2016) defined a firewall as the ability to block specific content, such as known malware or certain websites, and recognise when certain applications and protocols such as HTTP, FTP, and DNS are being misused.

This firewall could be installed in a form of network level firewall, circuit level firewall, application level firewall, or stateful multilayer firewall.

Network Level Firewall: In network level firewall, it was stated that the firewall is operated on the network layer of the OSI and TCP/IP models and hence, they filter incoming and outgoing traffic based on packet headers, IP addresses, service requested, and the port utilized for forwarding the data packet. Network firewalls can also filter unauthorized traffic based on other factors like specific domain names. Routers usually come built-in with such firewalls.

Circuit Level Firewall: Circuit level firewall is one of the most expensive firewall. This firewall operates at the transport layer of TCP/IP model and the session layer of the OSI model. It determines the authenticity of the session that is requested by monitoring and inspecting the handshake between data packets. The handshake process is simple and can easily be manipulated by hackers. When one device sends data segments in packet form, the other device responds with its own data packet. As a result, the first device acknowledges the sent packets and validates their receipt as well. Hackers can modify this process to overload the destination, causing a denial of service or distributed denial of service (DDoS) attack. Internal networks can be hidden on such firewalls from the outside world and session rules can also be changed or restricted.

Application Level Firewall: Application level firewall is also known as proxy servers or proxies and it is similar to circuit level firewalls. The difference between application firewall and circuit level firewall is that they work on particular applications only. Their main function is to protect the internal network of an organisation from trojans, malware, viruses, keyloggers, and other types of malicious programs. They can also be used to block a website based on the content. The downside of application level firewalls is that they are slow because they examine each data packet in a thorough manner; hence, it takes more time for the data to be filtered. They have no transparency for the end user and usually require manual configurations on systems.

Stateful Multilayer Firewall: This type of firewall is the most expensive compared to the other three, but they offer all the combined benefits of the other three firewalls. On the network layer, SML firewalls filter unauthorized data packets, check for session authenticity, and inspect the content of the data packets. The advantages of using SML firewalls are that they establish a direct connection between the client and host, thus offering transparency, and they are much faster as no proxies are involved.

Anti-Virus software: In relation to anti-viruses software, some participants were of the opinion that anti-viruses that are regularly updated should be employed to protect the University network client side and to protect systems used by the employees in the university. However, Symantec Corporation (2014) opines that anti-viruses on the endpoints of an organisation are not enough to prevent sophisticated attacks or zero-days. University would also need to employ endpoint protection mechanisms, browser protection and implement effective device control settings in order to provide more additional layers of protection for their information and information systems. Antivirus software, as identified in this study is an effective cybercrime control measure. Antivirus software is a program designed to prevent, detect and remove malicious software on the network (Chamorro, 2012). According to Catalin and Oiu (2007), universities are using anti-virus software to block many viruses before they infect servers or computers. Catalin and Oiu (2007) further added that antivirus software are used in order to identify any malicious software before they cause damage to information systems. A study conducted by Gupta (2015) pinpointed that anti-virus is a utility that searches a hard disk for viruses and removes the virus if found.

Similarly, Luftmann and Kempaiah (2008) also reported that universities across the globe are using anti-virus software for the protection of their resources such as students' information, staff data and university's information systems. As pin-pointed in a study by Hagen *et al.* (2008), the best defence against the theft of staff and students' information is through the use of management practices and the use of anti-virus software on all servers, workstations, and even laptops accessing the university's network resources. Participants opined that Antivirus software are effective tools for control of cybercrimes on the university network, it controls the distribution of malicious content on the network. Thus, anti-virus software is a common cybercrime preventive measure used on the Ahmadu Bello University Network. It is therefore suggested that Universities should impose the use of anti-virus software as a measure of cybercrime prevention.

Password authentication: Apart from Anti-virus Software, Participants also indicated Password authentication as an effective cybercrime control measures on the University network. According to Florencio and Herley (2007), password is a string of characters that authenticate a system user to a system. password authentication prompts a user to enter his or her ID and password in order to gain access to a network (Liao *et al.,* 2006). Invariably, without being authenticated by the university, a staff or students cannot be able to gain access into the University network.

This finding is similar to a study by Xu *et al.* (2009) where they reported that password authentication helps a lot of universities across the globe to prevent their intellectual property. Similarly, a study by Ampomah *et al.* (2013) also reported that universities use password authentication to prevent crime related offence on their network. Ampomah *et al.* (2013) further added that unauthorised access to a network from a private network is minimised when password authentication is available within the university's network. A password is usually used as a second authentication after the user has entered his/her ID. According to Komanduri *et al.* (2011), a password is the first line of defence against any form of attacks. A weak passwords is however easy to break using tools like L0phtCrack (LC3) or John the Ripper (Fox *et al.,* 2002).

This finding conforms to the third construct of RAT; Absence of capable guardian will aid the occurrence of cybercrime on the University network. Therefore, firewall, antivirus software, and password authentication can effectively reduce various attacks on the University network. It can also serve as measures of mitigating cybercrime and security breaches of the University network.

Participants in this study identified IDPSs as cybercrime control measures on the University network. According to Scarfone and Mell (2007), to detect unauthorised activity within the network or on individual machines, organisations should implement intrusion detection and prevention systems (IDPSs). The

IDPSs assign priorities to various files depending on their value, and can then alert administrator for any suspicious activity (Scarfone and Mell, 2007).

De-Militarised Zone (DMZ) network was also identified by the participants that it is been used on the university network. According to Bradley (2016), De-Militarised Zone is a special local network configuration designed to improve security by segregating computers on each side of the network. White (2010) further described DMZ as an intermediate area between a trusted network and untrusted network. Only few of the participants identified DMZ as cybercrime control measures used on the university network. Some of them however, also stated that DMZ is not been managed effectively on the university network. Thus, it was emphasized that DMZ should be implemented and managed effectively in order to enjoy the benefits it offers.

Participants identified Virtual Private Network (VPN) as another cybercrime control measure used on the University network. According to Clayton and Rakes (2007), a VPN is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network. A VPN is a “private data network that makes use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures” (White, 2010, p. 282). Participants explained that VPN helps the University to encapsulate and encrypt any incoming and outgoing data and keep the data contents private while in transit over the public network (Odiyo and Dwarkanath, 2011). It also helps in the authentication of remote computer and, perhaps, the remote user such as university visitors. Participants, however, further revealed VPN as security control measures is not commonly used as a cybercrime control measure on the Ahmadu Bello University Network.

It is also recommended that the University should adopt tools from IT vendors (e.g. CISCO, IBM, Hewlett Packard Enterprises) with profound security reputation when implementing their back-bone infrastructure technology. Tools like burp are predominately used for web and web applications’ testing.

Metasploit and Nessus are the two main tools for network testing. It is also suggested that open source tools such as Microsoft Threat Modeler and Snort that can help the University test for vulnerabilities on their network and for monitoring should be deployed.

4.2.6 Measures for managing some common types of cybercrimes

From the response of the interview, participants identified some common specific measures of cybercrime and attack prevention. The types of cybercrimes and their respective measures are discussed below.

Phishing attacks: Majority of the respondents identified security measures for preventing phishing attacks on the university network which include anti-phishing software, user education, and use of firewall.

Anti-phishing software: Respondents felt that the provision of anti-phishing software is necessary on the university network. Most of the participants stated that phishing is very relevant and rampant on the university network as such, anti-phishing software will go a long way in avoiding phishing attacks on the University network. Jain *et al.* (2007) stated that in order to improve the security capabilities of access control systems on universities network, it is vital and necessary to install anti-phishing software. Similarly, Alnajim and Munro (2009) in his study reported that the use of anti-phishing software is necessary for organisational network to be protected from adversaries.

Denial of Service attacks: In denial of service attacks, respondents stated that no one is completely prevented from being attacked by cybercriminals, but, the level of attack can be reduced. Participants in this study stated that the security measures for preventing denial of service attacks include deployment of antivirus software and firewall, server configuration, and regular communication with the Internet Service Provider.

Server configuration: Participants believed that server machine on the university network integrates with a number of components on the university IT infrastructure in order to provide a unique self-service data analytics culture for the users. It is therefore important that a server administrator understands how server can be configured properly in order for the IT infrastructure within the university to align with each other, as such would help in reducing the level of attacks on the university network. Similarly, in a study by Kim and Elazary (2013), it was stated that for successful prevention of unnecessary attacks on university network, proper configuration of server machine has to be done in order for the IT infrastructure to be in conformity with one another.

Regular communication with the Internet Service Provider (ISP): Respondents suggested that constant communication by the university with their Internet Service Providers (ISPs) could go a long way in mitigating sophisticated forms of denial of service attacks (i.e. Distributed Denial of Service attacks (DDoS)). Participants are of the believed that ISPs are usually in a strong position to prevent most DDoS attacks. Hence, university would need the influence of ISPs that control underlying Internet infrastructure in order to effectively prevent DDoS attacks. As stated by Beitollahi and Deconinck (2012) organisations should enhance cooperation with multiple ISPs and domains in order to properly manage sophisticated forms of cybercrimes and to also enhance the response time in trying to mitigating a cybercriminal activity against the organisation.

Botnet attack: In botnet attacks, participants stated that any university can be attacked by cybercriminals, but, the level of attack may vary and can also be reduces. Participants in this study stated that the security measures for preventing botnet attacks include multiple anti-virus and behavioural tools.

Multiple Anti-viruses: Participants opined that the use of different anti-viruses on various points on the university network is necessary in mitigating botnet attacks. The integration of different anti-viruses on the university's network allows

resilience against attacks. They further stated that running different anti-viruses on several points on the University's network increases the detection rate of malicious programs. Since the web gateway and endpoints are using the same anti-virus engine, it is therefore necessary for the university to have different anti-viruses for their web gateways and endpoint. The university also ensures that it uses the strongest anti-viruses for critical areas of the IT infrastructure. However, different anti-viruses might often try to kill each other and fight over malwares. This is, usually, as a result of anti-virus programs seeing other anti-virus programs that monitor and send information about a system as a virus or threat. In line with this finding, Jon *et al.*(2007) stated that instead of running just a single/specific anti-virus on various points of an organisations network, organisations can run multiple or a wide range of anti-viruses in parallel on an organisations IT infrastructure.

Behavioural Monitoring Tools: The respondents indicated that the use of special kinds of behavioural monitoring tools such as Intrusion Detective System (IDS) on the University network would help easily detect communications made by botnets with servers. According to Pastrana *et al.* (2012), the use of intrusion detection systems, signature and anomaly based detection systems would help effectively detect and mitigate botnet attacks.

SQL Injection and Cross-Site Scripting Attacks: The security measures for preventing SQL attacks and Cross-site scripting attacks are as follows;

SQL Injection Attacks: The Participants stated that one of the ways in which university can secure web applications from SQL injection based attack techniques is to sanitize user input coming from the web application and then protect their database. University protect their databases by locking down their database tables (even at a row level), and restricting what a database user has access to (i.e. making sure database users do not have file permission etc.). In line with this response, Etienne (2008) stated organisations should always validate user supplied data, enforce data types for all inputs, always employ the

least privilege rule, filter input data via white-list and black-list filtering, snort-based solutions, and host based IDSs.

Cross-site Scripting attacks: Cross-site scripting is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users (Adam *et al.,* 2009). In order to avoid the execution of administrative commands by an unauthorised individual/user, the participants were of the opinion that the University should employ robust and effective authentication and role command procedures. The Participants also felt that application developers should develop applications in a way that allows the easy configuration of security parameters against the execution of malicious Java Script codes in applications. Contrary to this finding, Philipp *et al.* (2007) stated that cross-site scripting can be prevented in an organisation by properly validating input from users, employing static analysis on the server side of an organisation, and deploying anomaly based intrusion detection systems in organisations.

4.3 Conclusion

This study investigates the various forms of cybercrimes and their consequences on the Ahmadu Bello University, Zaria Network. This chapter showed the results of the data analysis. The data collected using semi-structured interview and case files from the Security unit of the university, thematic analysis was used to systematically analyse the responses of the respondents. The findings from the study revealed that Ahmadu Bello University Network is susceptible to different types of cybercrime even though security protocols were put in place. This study found that cybercrime occurs when there is an area of vulnerability in a network and the absence of capable security protocols.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

In the preceding chapter, the findings of the study were presented and discussed. This chapter presents the concluding remarks for the study. The conclusions drawn in this chapter is based on data obtained from the participants with IT personnel in the six different units of the Institute of Computing and Information Communication Technology (ICICT), Ahmadu Bello University, Zaria. Documents from security unit of the University also form part of the source of data. Herein, research questions were related in order to further clarify the results and conclusions drawn from the

5.2 Summary of the Study

The increasing usage of technology at Ahmadu Bello University, Zaria, is causing an increase in various types of cybercrimes experienced in the university. Hence, the University needs to deploy more security baselines, technical security controls and administrative security measures, that would help mitigate cybercrime and security breaches on the University Network. The study was aimed at investigating the effects of security protocols on cybercrime at Ahmadu Bello University, Zaria.

The chapter one of the study presents the introduction and background to the study. It also outlines the research problem, the research objectives and the research questions that the study aims to achieve and answer. The chapter further gave a justification and significance for conducting this study, including a brief description of the research method used in the study.

Chapter two gave a review of the related literature on cybercrime within educational institutions and other IT organisations. In this chapter, definitions

were given with the description of key concepts that made up the research study. The chapter elaborates on the various categories of cybercrime, common techniques used by cybercriminals and cybercrime perpetrators' profile were presented in line with the objective of the study. The chapter also elaborated on the effects of cybercrime, factors contributing to cybercrime increase, international cyber law, and cyber laws in Nigeria. The chapter concludes by discussing technical, administrative, and physical security controls on IT organisations.

Chapter three highlights the research design and research methodology adopted in this study. The chapter presents the research design technique used, the research approach employed, the research population, sample selection, sample size, data collection procedure, and the data analysis technique used in the study. The theory used in this study was also discussed in the context of its applicability in the study.

Chapter four presents the analysis and interpretation of the research findings obtained from the responses of the IT personnel of the six different units of the Institute of Computing and Information Communication Technology (ICICT). The chapter also presents documents from security unit of Ahmadu Bello University, Zaria, that are related and relevant to the objectives and findings of this study.

Findings were presented in accordance with the objectives of the study. The findings, in relation to the objectives of the study, showed the types of cybercrime that Ahmadu Bello University Network is often susceptible to. It also showed the areas of Ahmadu Bello University Network that is vulnerable to cybercrime. Furthermore, it can help to identify the security protocols that can be used to effectively manage Ahmadu Bello University's Network from cybercrime.

Chapter five summarizes the various chapters of the dissertation. Recommendations and directions for future research are also provided in the chapter.

5.3 Summary of the Major Findings

Based on the data collected and analysed for this study, the following are major findings:

1. Findings from the study revealed that the University is continuously susceptible to different types of cybercrime. Among the cybercrimes are: social engineering, denial of service attacks, malware attacks, pharming attacks, SQL injection and cross-site scripting attacks, website defacement, and port scan attacks.

2. Different areas of the University Networks are vulnerable to attacks from cybercriminals. The most prominent being the admission page and accommodation page.

3. Even though, the university uses different security controls such as firewalls, antivirus software, password authentication, security audit, penetration testing, antivirus software, anti-phishing on the University network, there is still cybercrime that is occurring at the University.

   There is need for the University to carry out common security baseline exercises such as external and internal security audits, penetration and vulnerability assessments on a regular basis in order to properly ensure their information systems are protected from less sophisticated forms of cyber-attacks. The University should also have adequate incident response strategies on ground to enable them quickly respond to attacks and take drastic steps in reducing the magnitude of cybercrime on the University network.

5.4 Recommendations

Based on the findings of this study, it is recommended that a behavioural approach to cybercrime be implemented across the university. This can be achieved by motivation of staff of the ICICT directorate. Salary increases, cash incentives for hardworking staff and training of staff on a regular basis. These

could be a step in the right direction for effective management of the University Network.

There is a also the need for the University to be more security conscious of students who participate in projects such as website development. This is because of a recent event in which some students were caught trying to allocate rooms to their colleagues and also lure victims in paying school fees into different account that is similar to that of the University. Also the University should put in place adequate data protection measures that can help with the handling of employee data.

Finally, the University should be very proactive to the issues of cybercrimes. The University should organise regular seminars and workshops aimed at enhancing collaborative efforts between Government and the University on issues related to cyber security, also engage staff for international training as a form of motivation. Furthermore, the University should collaborate on a regular basis or be involved in software development projects that would provide better means of combating cybercrimes within the University. It is also recommended that the university should enhance and improve the level of cooperation and trust that exists with other agencies such as National Security Agency (NSA), Central Intelligence Agency (CIA), Inter-Service Intelligence (II), and European Union Agency for Network and Security (EUANS) in order to combat cybercrimes.

5.5 Direction of Future Research Work on Cybercrime and Security Protocols

It was evident from the literature and research findings that some areas within universities, relating to cybercrime and security protocols of Information Systems still need to be investigated. These areas include:

- The perception and understanding of cybercrime by non-teaching staff of the University

- Assessment of the extent of use of security protocols on the University network
- Understanding the influence of cybercrime risk on the e-service adoption of Nigerian Internet Users

5.6 Conclusion

In the 21st century, cybercrime attacks in universities have become rampant globally. Historically, university's ICT infrastructure has been based on an open access with very little restrictions on access to information. These infrastructures stimulates learning and its environment. It, however, increases cyber threat. Once breached, universities can be left with high financial losses and loss of valuable information such as students and staff members' personal information. Cybercriminals frequently device dynamic and sophisticated ways in perpetrating their illicit activities. In equal measure, universities should also be making effort to deploy and explore more divergent means of curtailing the menace of the cybercriminals. Hence, proper use of cybercrime control measures, as suggested in this study, could help in safeguarding and protecting students and staff members' information, and the university's information systems, at large, from cybercrimes and cybercriminals.

REFERENCES

Abbas, A., El-Saddik, A., & Miri, A. (2006). A comprehensive approach to desingning Internet security taxonomy.

Abdul, R., Khalid, L., Farooq, H. A., Hur, H., Zahir, A., & Bloodsworth, P. C. (2014). Semantic Security against web application attacks. *Information Science, 254 - 1*, 41.

Ablon, Libicki, & Golay. (2014a). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*: Rand Corporation.

Ablon, Libicki, & Golay. (2014b). Markets of Cybercrime Tools and Stolen Data: Hacker's Bazaar.

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006). *A multifaceted approach to understanding the botnet phenomenon.* Paper presented at the Proceedings of the 6th ACM SIGCOMM conference on Internet measurement.

Adam, K., Philip, J. G., Karthick, J., & Michael, D. E. (2009). *Automatic creation of SQL Injection and cross-site scripting attacks.* Paper presented at the ICSE '09 Proceedings of the 31st International Conference on Software Engineering Vancouver, BC

Adeniran, A. (2011). Café culture and heresy of yahooboyism in Nigeria. *Cyber Criminology*, 1.

Adeta, K. A. (2014). *PATTERN AND CONSEQUENCES OF CYBER-CRIME IN TERTIARY INSTITUTIONS IN ZARIA.* AHMADU BELLO UNIVERSITY, ZARIA.

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643-652.

Ahmed, A. A. (2010). Hack No More, Internet Security: Attacks and Defence.

Aiello, W., Bellovin, S. M., Blaze, M., Ioannidis, J., Reingold, O., Canetti, R., & Keromytis, A. D. (2002). *Efficient, DoS-resistant, secure key exchange for internet protocols.* Paper presented at the Proceedings of the 9th ACM conference on Computer and communications security.

Akritidis, P., Chin, W.-Y., Lam, V. T., Sidiroglou, S., & Anagnostakis, K. G. (2007). *Proximity Breeds Danger: Emerging Threats in Metro-area Wireless Networks.* Paper presented at the USENIX Security.

Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: the case of obfuscated malware *Global Security, Safety and Sustainability & e-Democracy* (pp. 204-211): Springer.

Alcaraz, C., & Zeadally, S. (2013). Critical control system protection in the 21st century. *Computer*(10), 74-83.

Alfredo, P., Devide, P., & Riccard, S. (2011). Formally based semi-automatic implementation of an open security protocol. *The Journal of Systems and Software*, 15.

Alhamed, M., & Alsuhaibany, O. M. (2013). Website defacement incident handling system, method, and computer program storage device: Google Patents.

Allsopp, W. (2010). *Unauthorised Access: Physical Penetration Testing For IT Security Teams*: John Wiley & Sons.

Alnajim, A., & Munro, M. (2009). *An anti-phishing approach that uses training intervention for phishing websites detection.* Paper presented at the Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on.

Amit, R., & Schoemaker, P. J. (2012). STRATEGIC ASSETS AND ORGANIZATIONAL RENT. *Strategische Managementtheorie, 14*, 325.

Ampomah, M., De Silva, Y., Li, H., Pahlisa, P., Yang, Q., & Zhang, Q. (2013). Information security strategy and teleworking (in) security.

Anderson, J. R. (2008). *Security engineering: a guide to building dependable distributed systems*.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime *The economics of information security and privacy* (pp. 265-300): Springer.

Andoh-Baidoo, F. K., & Osei-Bryson, K.-M. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached firms. *Expert Systems with Applications, 32*(3), 703-725.

Ani, L. (2011). Cyber Crime And National Security: The Role of the Penal And Procedural Law. *Law and Security in Nigeria*, 200-202.

Appel, E. J. (2014). *Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence*: Crc Press.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759-763.

Aristotle, J. (2012). Cross-domain Solution.

AustralianCatholicUniversity. (2015). Risk Management Policy.

Awe, J. (2009). Fighting cyber crime in Nigeria: Idea Group Inc.

Awodele, O., Onuiri, E. E., & Okolie, S. O. (2012). *Vulnerabilities in Network Infrastructures and Prevention/Containment Measures.* Paper presented at the Proceedings of Informing Science & IT Education Conference (InSITE).

Aycock, J. (2006). *Computer viruses and malware* (Vol. 22): Springer Science & Business Media.

Aziz, A. (2011). Computer worm defense system and method: Google Patents.

Babbie, E., & Mouton, J. (2001). The Social Practice of Social Research: Cape Town: Oxford University Press.

Balthrop, J., Forrest, S., Newman, M. E., & Williamson, M. M. (2004). Technological networks and the spread of computer viruses. *arXiv preprint cs/0407048*.

Barton. (2011). *Physical security management protocol*

Battaglia. (2008). Encyclopedia of survey research methods. *Publication date*.

Battaglia. (2011). Non-probability sampling *Encyclopedia of survey research methods* (pp. 523-526): SAGE publications.

Beitollahi, H., & Deconinck, G. (2012). Analysing well-known countermeasures against distributed denial of service attacks. *Computer Communications, 35*(11), 1312-1332. doi: http://dx.doi.org/10.1016/j.comcom.2012.04.008

Bergman, N., Stanfield, M., Rouse, J., Scambray, J., Geethakumar, S., Deshmukh, S., . . . Price, M. (2013). *Hacking exposed: Mobile security secrets & solutions*: McGraw-Hill.

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). *All your contacts are belong to us: automated identity theft attacks on social networks.* Paper presented at the Proceedings of the 18th international conference on World wide web.

Bleaken, D. (2010). Botwars: the fight against criminal cyber networks. *Computer Fraud & Security, 2010*(5), 17-19. doi: http://dx.doi.org/10.1016/S1361-3723(10)70055-5

Boeke, M., & Ewell, P. T. (2007). Critical connections: Linking states' unit record systems to track student progress.

Bogdanoski, M., Shuminoski, T., & Risteski, A. (2013). Analysis of the SYN flood DoS attack. *International Journal of Computer Network and Information Security, 5*(8), 1.

Borgatti, S. P. (1999). Element of Research: Theoretical Framework.

Bose, A., & Shin, K. G. (2006). *On mobile viruses exploiting messaging and bluetooth services.* Paper presented at the Securecomm and Workshops, 2006.

Bradley, M. (2016). DMZ - De-Militarized Zone (Computer Networking). http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm

Brandon, B. (2007). Top 15 Security/Hacking Tools and Utilities. Retrieved 2nd December, 2013, from http://www.teckh.com/?p=143

Braun, V., Clarke, V., & Terry, G. (2014). Thematic analysis. *Qual Res Clin Health Psychol*, 95-114.

Brewer, R. (2014). Advanced persistent threats: minimising the damage. *Network Security, 2014*(4), 5-9.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime: An Introduction, 2/E*: Pearson Education India.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29*(3), 408-433.

Brown, T. J., & Suter, T. A. (2012). Exploratory, Descriptive, and Causal Research Designs *Marketing Research* (pp. 240). Oklahoma State University, USA: Cengage Learning.

Browne, K. (2005). Snowball sampling: using social networks to research non-heterosexual women. *International Journal of social research methodology, 8*(1), 47-60.

Bruix, J., & Sherman, M. (2011). Management of hepatocellular carcinoma: an update. *Hepatology, 53*(3), 1020-1022.

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*: WW Norton & Company.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an emperical study of rationality-based beliefs and information security awareness.

Bunker, G., & Fraser-King, G. (2009). *Data leaks for dummies*: John Wiley & Sons.

Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime — A new breed of criminal? *Computer Law & Security Review, 19*(3), 222-227. doi: http://dx.doi.org/10.1016/S0267-3649(03)00306-6

Burns, J. (2015). Harvard hacked: the impact of educational cybercrime.

Burstein, A. J. (2008). Amending the ECPA to Enable a Culture of Cybersecurity Research. *Harv. JL & Tech., 22*, 167.

Butts, J., & Shenoi, S. (2013). *Critical Infrastructure Protection VII: 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers* (Vol. 417): Springer.

Byres, E., & Lowe, J. (2004). *The myths and facts behind cyber security risks for industrial control systems.* Paper presented at the Proceedings of the VDE Kongress.

Cárdenas, A. A., Amin, S., & Sastry, S. (2008). *Research Challenges for the Security of Control Systems.* Paper presented at the HotSec.

Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *Internet Computing, IEEE, 10*(1), 82-89.

Carnegie. (2015). How cybercrime criminals operate.

Carolina. (2014). Worst "EDU" Privacy Breaches of 2011-2012.

Carolina, C. (2015). Security Awareness Presentation - UNC School of Dentistry.

Cassey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet*.

Cassidy, K. J., Gross, K. C., & Malekpour, A. (2002). *Advanced pattern recognition for detection of complex software aging phenomena in online transaction processing servers.* Paper presented at the Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on.

Castell, M. (2013). *Mitigating online account takeovers: The case for education.* Paper presented at the Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, survey paper, April, available at www. frbatlanta. org/documents/rprf/rprf_pubs/130408_survey_paper. pdf.

Catalin, B., & Oiu, A. V. (2007). Optimization of Antivirus Software. *Informatica, 11*(2007), 99-102.

Cavelty, M. (2012). The militarisation of cyber security as a source of global tension. *Browser Download This Paper*.

Cert. (2013). Insider Threat.

Chamorro, E. A. (2012). *Antivirus software advising system*: CALIFORNIA STATE UNIVERSITY, DOMINGUEZ HILLS.

Chang, Y.-C. (2012). *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait*: Edward Elgar Publishing.

Chauhan, M. (2010). COMPUTER FRAUDS AND CYBER CRIME: A MIXTURE OF TRADITIONAL AND MODERN.

Chen, Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems, 50*(4), 662-672.

Chen, & Zhao, H. (2012). *Data security and privacy protection issues in cloud computing.* Paper presented at the Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on.

Chiu, I., & Shu, L. (2007). Biomimetic design through natural language analysis to facilitate cross-domain information retrieval. *AI EDAM: Artificial Intelligence for Engineering Design, Analysis, and Manufacturing, 21*(01), 45-59.

Choi, M.-k., Robles, R. J., Hong, C.-h., & Kim, T.-h. (2008). Wireless network security: Vulnerabilities, threats and countermeasures. *International Journal of Multimedia and Ubiquitous Engineering, 3*(3), 77-86.

Christian, M. (2012). Penetration Testing Tool for web services security. *IEEE*, 163-170.

Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: a review and the Taiwan experience. *Decision Support Systems, 41*(3), 669-682.

Ciampa, M. (2013). *Security awareness: applying practical security in your world*: Cengage Learning.

Clayton, T., & Rakes, R. B. (2007). Virtual private network software system: Google Patents.

Cochran, W. G. (2007). *Sampling techniques*: John Wiley & Sons.

Contreras-Castillo, J., Pérez-Fragoso, C., & Favela, J. (2006). Assessing the use of instant messaging in online learning environments. *Interactive Learning Environments, 14*(3), 205-218.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons, 48*(3), 233-240.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage.

Dalla, E., & Geeta, M. (2013). Cyber Crime A Threat to Persons, Property, Government and Societies. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 997-1002.

Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240-259.

De Luca, A., Weiss, R., & Drewes, H. (2007). *Evaluation of eye-gaze interaction methods for security enhanced PIN-entry.* Paper presented at the Proceedings of the 19th australasian conference on computer-human interaction: Entertaining user interfaces.

De Vany, A. S., & Walls, W. D. (2007). Estimating the effects of movie piracy on box-office revenue. *Review of Industrial Organization, 30*(4), 291-301.

Desai, M. M. (2010). *Hacking For Beginners: a beginners guide to learn ethical hacking*: Manthan M Desai.

Dessel, G. V. (2013). How to determine population and survey sample size? . Retrieved 26, October, 2015, from https://www.checkmarket.com/2013/02/how-to-estimate-your-population-and-survey-sample-size/

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works.* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social implications of the Internet. *Annual review of sociology*, 307-336.

DSLReport. (2011). Network Sabotage.

Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal-January*, 93-98.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends:” Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

Etienne, Z. P. (2008). *Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM*. Paper presented at the Application security conference, Ghent, Belgium.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4.

Ewell, P., Jankowski, N., & Provezis, S. (2010). Connecting state policies on assessment with institutional assessment activity. *Urbana, IL: University of Illinois and Indiana University, National Institute for Learning Outcomes Assessment. Retrieved from http://learningoutcomesassessment. org/documents/NILOAStateStudy_000. pdf*.

Farrokhi, F., & Mahmoudi-Hamidabad, A. (2012). Rethinking convenience sampling: Defining quality criteria. *Theory and practice in language studies, 2*(4), 784.

Felner, R. D., Jackson, A. W., Kasak, D., & Mulhall, P. (1997). The impact of school reform for the middle years. *Phi Delta Kappan, 78*(7), 528.

Felson, M., & Cohen, L. E. (1979). Human ecology and crime: A routine activity approach. *Human Ecology, 8*(4), 389-406.

Fenwick, D., Daim, T. U., & Gerdsri, N. (2009). Value Driven Technology Road Mapping (VTRM) process integrating decision making and marketing tools: Case of Internet security technologies.

Florencio, D., & Herley, C. (2007). *A large-scale study of web password habits.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Fox, E., Bush, J., Ashley, S., & Webb, I. (2002). Common Hacking Tools for Linux and Windows.

Fung, B. (2014). Obama Called the Sony Hack an Act of 'Cyber Vandalism.'He's Right. *Washington Post*.

Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U. (2010). *A new graphical password scheme resistant to shoulder-surfing.* Paper presented at the Cyberworlds (CW), 2010 International Conference on.

Garcia, M. L. (2007). *Design and evaluation of physical protection systems*: Butterworth-Heinemann.

Gardere, W. S. (2014). Cybercrime is getting worse - 5 reasons.

Gemmill, E., & Peterson, M. (2006). Technology use among college students: Implication for student affairs professionals. *NASPA Journal, 43*(2), 280-300.

Gercke, M. (2012). *Understanding cybercrime: Phenomena , challenges and legal response*. Geneva, Switzerland: TU Telecommunication Development Bureau.

GFI. (2009). Attachment spam – the latest trend (pp. 6). USA.

Goje, A. C., Gornale, S. S., & Yannawar, P. L. (2007). *Emerging Trends in Information Technology*: IK International Publishing House.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world* (Vol. 89): Oxford University Press New York.

Goodchild, J. (2012). Social engineering: The basics. *CSO Online*.

Gordon, G. R., Rebovich, D. J., & Gordon, J. B. (2007). *Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement*: Center for Identity Management and Information Protection, Utica College.

Goutam, R. K. (2015). Importance of Cyber Security. *International Journal of Computer Applications, 111*(7).

Graham, D. E. (2010). Cyber threats and the law of war. *J. Nat'l Sec. L. & Pol'y, 4*, 87.

Grimes, R. A. (2015). Reasons for Internt crime.

Groff, E. R. (2008). Adding the temporal and spatial aspects of routine activities: A further test of routine activity theory. *Security Journal, 21*(1), 95-116.

Grover, V., & Saeed, K. A. (2004). Strategic orientation and performance of internet-based businesses. *Information Systems Journal, 14*(1), 23-42.

Groves, R. M., Fowler Jr, F. J., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau, R. (2013). *Survey methodology*: John Wiley & Sons.

Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008). *BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection.* Paper presented at the USENIX Security Symposium.

Gupta, B. B. (2015). Web Application Security–What You Need to Know.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*: John Wiley & Sons.

Hagen, J. M., Sivertsen, T. K., & Rong, C. (2008). Protection against unauthorized access and computer crime in Norwegian enterprises. *Journal of Computer Security, 16*(3), 341-366.

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: laws, rights and regulations*: Information Science Reference.

Halder, D., Jaishankar, K., & Jaishankar, K. (2012). *Cyber crime and the victimization of women: laws, rights and regulations*: Information Science Reference.

Halfond, W., Viegas, J., & Orso, A. (2006). *A classification of SQL-injection attacks and countermeasures.* Paper presented at the Proceedings of the IEEE International Symposium on Secure Software Engineering.

Harrell, M. C., & Bradley, M. A. (2009). Data Collection Methods: Semi-Structured Interviews and Focus Groups (pp. 140). RAND National Defense Research Institute, Santa Monica, California, USA.

Harrison, G. (2010). *Neoliberal Africa: The impact of global social engineering*: Zed Books.

Hassan, A. B., Funmi, D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology, 2*(7).

Helsper, E. (2008). Digital natives and ostrich tactics?: the possible implications of labelling young people as digital experts.

Hemavathy, A., Pravin, M., Avichal, S., & Fleizach, C. (2005). Cybercriminal Activity. 45. http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf

Herrmann, A., & Paech, B. (2005). *Quality misuse.* Paper presented at the Proc. 11th Int. Workshop on Requirements Engineering: Foundation of Software Quality–REFSQ.

Herzog, P. (2010). OSSTMM 3–The open source security testing methodology manual. Barcelona, España: ISECOM.

Hinckley, K., Bi, X., Pahud, M., & Buxton, B. (2012). *Informal information gathering techniques for active reading.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Hoffman, P., & Schlyter, J. (2012). The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., . . . Scarfone, K. (2013). Guide to attribute based access control (ABAC) definition and considerations (draft). *NIST special publication, 800*(162).

Hu, Y., Wood, J. F., Smith, V., & Westbrook, N. (2004). Friendships through IM: Examining the relationship between instant messaging and intimacy. *Journal of Computer-Mediated Communication, 10*(1), 00-00.

Hungler, B., & Polit, D. (1999). Nursing research principles and methods.

Ionescu, L. (2012). Corruption, Unemployment, and the Global Financial Crisis. *Economics, Management, and Financial Markets*(3), 127-132.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). *Reverse social engineering attacks in online social networks.* Paper presented at the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

Iyoha, F. (2012). COMPANY ATTRIBUTES AND THE TIMELINESS OF FINANCIAL REPORTING IN NIGERIA. *Business Intelligence Journal (19182325), 5*(1).

Jain, A. K., Flynn, P., & Ross, A. A. (2007). *Handbook of biometrics*: Springer Science & Business Media.

Jaishankar. (2011a). *Cyber criminology: exploring internet crimes and criminal behavior*: CRC Press.

Jaishankar. (2011b). Expanding cyber criminology with an avant-garde anthology. *Cyber Criminology*.

Jegede, A. E. (2010). Globalization, Media Culture and Socio-Economic Security in Nigeria. *Mass Communication A Book of Readings*, 228-247.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). *On technical security issues in cloud computing.* Paper presented at the Cloud Computing, 2009. CLOUD'09. IEEE International Conference on.

Jeremy, K. (2007). Pharming Attack Targeted Bank Customers Worldwide -

Jon, O., Evan, C., & Farnam, J. (2007). *Rethinking Antivirus: Executable Analysis in the Network Cloud.* Paper presented at the HOTSEC'07 Proceedings of the 2nd USENIX workshop on Hot topics in security Berkeley, CA, USA.

Jonathan, F. (2015). Credit Card Scanner, Skimmer, and Reencoder Crimes

Junxiao, S., & Sara, S. (2012). Phishing *CSc 566, Computer Security Research Reports* (pp. 1-14). USA: University of Arizona.

Kahate, A. (2013). *Cryptography and network security*: Tata McGraw-Hill Education.

Kahoka. (2015). Vulnerabilities and Causes of Cybercrime.

Kalinich, K. P., & McGrath, K. (2003). Identifying and Evaluating the Business Impact of Network Risks and Liabilities. *Brief, 33*, 18.

Kannan, K., Rees, J., & Spafford, E. (2009). Unsecured Economies: Protecting Vital Information. *Red Consultancy for McAfee, Inc*.

Kapp, K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*: John Wiley & Sons.

Kar, D., & Panigrahi, S. (2013). *Prevention of SQL Injection attack using query transformation and hashing.* Paper presented at the Advance Computing Conference (IACC), 2013 IEEE 3rd International.

Karen, M., & Theodore, W. (2009). Tools Report on Anti-Malware *Information Assurance Tools Report* (1 ed., pp. 230). IATAC, 13200 Woodland Park Road Herndon, VA, USA: IATAC.

Karlof, C., Shankar, U., Tygar, J. D., & Wagner, D. (2007). *Dynamic pharming attacks and locked same-origin policies for web browsers.* Paper presented at the Proceedings of the 14th ACM conference on Computer and communications security.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security, 24*(3), 246-260.

Kaspersky, L. (2013). The evolution of phishing attacks: 2011-2013. Kaspersky Lab ZAO, Moscow, Russia.

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*: Congressional Research Service.

Kharat, S. P. (2017). Cyber Crime–A Threat to Persons, Property, Government and Societies.

Kim, S. D., & Elazary, L. (2013). System and method for managing server configurations: Google Patents.

Koh, S. J., Chang, M. J., & Lee, M. (2004). mSCTP for soft handover in transport layer. *IEEE communications letters, 8*(3), 189-191.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., . . . Egelman, S. (2011). *Of passwords and people: measuring the effect of password-composition policies.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security, 58*, 39-46.

Kosina, K. (2012). *Wargames in the fifth domain*: Diplomatische Akademie.

Kratchman, S., Smith, J. L., & Smith, M. (2008). The Perpetration and Prevention of Cybercrimes. *Available at SSRN 1123743*.

Krieger, H. (2006). A conflict of norms: the relationship between humanitarian law and human rights law in the ICRC customary law study. *Journal of Conflict and Security Law, 11*(2), 265-291.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE, 4*(1), 33-39.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141-144.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7), 1057-1079.

Kumar, M., Garfinkel, T., Boneh, D., & Winograd, T. (2007). *Reducing shoulder-surfing by using gaze-based password entry.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.

Lam, T., & Hsu, C. H. (2006). Predicting behavioral intention of choosing a travel destination. *Tourism management, 27*(4), 589-599.

Lantz, B., Heller, B., & McKeown, N. (2010). *A network in a laptop: rapid prototyping for software-defined networks.* Paper presented at the Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks.

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*.

Launius, S. (2009). Securing the Network Perimeter Of A Community Bank'. *SANS Institute*, 1-41.

Lazenby, J. F. (2012). *The Spartan Army*: Stackpole Books.

Lee, K., Bae, K., & Yim, K. (2009). Hardware approach to solving password exposure problem through keyboards sniff.

Lemon, S. (2006). Ten Security Security Trends Worth Watching. Retrieved 9/11, 2013, from www.networksworld.com

Lenhart, A., Rainie, L., & Lewis, O. (2001). Teenage life online: The rise of the instant-message generation and the internets impact on friendships and family relationships. *Pew Internet and American Life Project. Retrieved from*

Lesk, M. (2011). Cybersecurity and economics. *Security & Privacy, IEEE, 9*(6), 76-79.

Levy, P. S., & Lemeshow, S. (2013). *Sampling of populations: methods and applications*: John Wiley & Sons.

Liamputtong, P. (2009). *Qualitative research methods*.

Liao, I.-E., Lee, C.-C., & Hwang, M.-S. (2006). A password authentication scheme over insecure networks. *Journal of Computer and System Sciences, 72*(4), 727-740.

Lifars. (2016). US Bank Suffered 513 Trojan Attacks in 2015.

Lincoln, S., & John, S. (2015). The World Wide Web Security FAQ.

Litan, A. (2004). Phishing attack victims likely targets for identity theft: Gartner Research.

Liu, A. X., & Gouda, M. G. (2008). Diverse firewall design. *IEEE Transactions on Parallel and Distributed Systems, 19*(9), 1237-1251.

Loftesness, S. (2004). Responding to" Phishing" Attacks: Glenbrook Partners.

Long, J. (2011). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*: Syngress.

Lu, C., Jen, W., Chang, W., & Chou, S. (2006). Cybercrime & cybercriminals: An overview of the Taiwan experience. *Journal of Computers, 1*(6), 11-18.

Luftmann, J., & Kempaiah, R. (2008). Key Issues for IT Executives 2007. *MIS Quarterly Executive, 7*(2).

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*(1), 52-60.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). Comprehensive study on cybercrime. *United Nations Office on Drugs and Crime*, 38-39.

Manning, R., & Aaron, G. (2013). Phishing Activity Trends Report *1st Quarter 2013*.

Manuel, E., Peter, W., Christopher, K., & Engin, K. (2009). *Defending Browsers against Drive-by Downloads: Mitigating Heap-spraying Code Injection Attacks.* Paper presented at the DIMVA '09 Proceedings of the 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment Springer-Verlag Berlin, Heidelberg.

Marco, C., Christopher, K., & Giovanni, V. (2010). *Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code*. Paper presented at the International World Wide Web Conference, Raleigh, North Carolina, USA.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of research design and methodology*: John Wiley & Sons Inc.

Margaret, R. (2016). Firewall.

Maxim, B. (2015). Denial of Service Attacks.

McCain, J. L. (2015). *Security awareness in practice.* UNIVERSITY OF NEBRASKA AT OMAHA.

McCormick, M. (2008). Data theft: a prototypical insider threat *Insider Attack and Cyber Security* (pp. 53-68): Springer.

Mcleod, & Charles, M. (2011). KING'S COUNSEL: A MEMOIR OF WAR, ESPIONAGE, AND DIPLOMACY IN THE MIDDLE EAST 1. *Mil. L. Rev., 208*, 313-313.

McQuade, S. C. (2006). *Understanding and managing cybercrime*: Pearson/Allyn and Bacon Boston.

Medeiros, J. P. S., Brito Jr, A. M., Pires, P. S. M., & Santos, S. R. D. (2009). Advances in network topology security visualisation. *International Journal of System of Systems Engineering, 1*(4), 387-400.

Meke, E. S. (2012). Urbanisation and Cybercrime in Nigeria: Causes and Consequences.

Millet, A. (2015). *Airlines vulnerabilities to a cyber-attack and the potential consequences.* Utica College.

Missiaen, T., Verhegge, J., Heirman, K., & Crombé, P. (2015). Potential of cone penetrating testing for mapping deeply buried palaeolandscapes in the context of archaeological surveys in polder areas. *Journal of Archaeological Science, 55*, 174-187.

Morris, W. (2004). *American heritage dictionary of the English language*: American heritage.

Murray, J. H. (2017). *Hamlet on the holodeck: The future of narrative in cyberspace*: Mit Press.

Mustaine, E. E., & Tewksbury, R. (1999). A routine activity theory explanation for women's stalking victimizations. *Violence Against Women, 5*(1), 43-62.

Myers, M. D., & Avison, D. (2002). *Qualitative research in information systems: a reader*: Sage.

Nadiah, S. (2014). Causes and Effects of Cyber Crime.

NationalInformationAssurance. (2006). Cross-Domain Solution.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum, 32*(1), 81-94.

NBCNews. (2013). U of Nedraska Data Breach Affecs 650,000 students: University of Nebraska.

Needham, R. M. (1994). Denial of service: an example. *Communications of the ACM, 37*(11), 42-46.

Neuman, W. L. (2013). *Social research methods: Qualitative and quantitative approaches*: Pearson education.

Newman, M. E., Forrest, S., & Balthrop, J. (2002). Email networks and the spread of computer viruses. *Physical Review E, 66*(3), 035101.

Niles, S. G., Sowa, C. J., & Laden, J. (1994). Life role participation and commitment as predictors of college student development. *Journal of College Student Development*.

Noy, C. (2008). Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of social research methodology, 11*(4), 327-344.

Nyoni, J., & Segoe, B. (2013). Critical spective reflectivity on open and distance learning (ODL) assessment rigidity: keeping pace with security measures of assessment modalities. *Mediterranean Journal of Social Sciences, 4*(3), 101.

Obama, B. (2010). *National Security Strategy of the United States (2010)*: DIANE Publishing.

Odiyo, B., & Dwarkanath, M. (2011). Virtual Private Network. *Uppsala universitet (accessed on November 2011)*.

OECD. (2007). Malicious Software (Malware): A Security threat to the Internet Economy (Vol. 5, pp. 106). Seoul, Korea: Organisation For Economic Cooperation and Development; Directorate for Science, Technology and Industry Committe for Information, Computer and Communications Policy.

Ojo, O. V. (2015). AN ASSESSMENT OF NIGERIA'S CYBERCRIMES (PREVENTION, PREVENTION ETC.) ACT 2015. *The Lawyers Chronicles, The Magazine of the African Lawyer*.

Oke, O. O. (2015). An Appraisal of the Nigerian Cybercrime (Prohibition, Prevention Etc) Act, 2015. *Available at SSRN 2655593*.

Olden, M. (2010). *Biometric authentication and authorisation infrastructures.*

Ortmeier, P. (2009). *Introduction to Security*: Upper Saddle River, NJ: Prentice Hall.

Osuagwu, O. E., Ogiemien, T., & Okide, S. (2010). DEPLOYING FORENSICS SCIENCE &TECHNOLOGY FOR RESOLVING NATIONAL CYBER-SECURITY CHALLENGES. *Journal of Mathematics & Technology*(3).

Oyesanya, F. (2004). Nigerian Internet 419 on the loose. *Retrieved May, 25*, 2005.

Pastrana, S., Mitrokotsa, A., Orfila, A., & Peris-Lopez, P. (2012). Evaluation of classification algorithms for intrusion detection in MANETs. *Knowledge-Based Systems, 36*, 217-225.

Paul, G. (2014). Internet for Beginners. Retrieved 2 May, 2014

Phair, N., & Hodges, M. (2007). *Cybercrime: the reality of the threat*: Nigel Phair.

Philipp, V., Florian, N., Nenad, J., Engin, K., Christopher, K., & Giovanni, V. (2007). Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis (pp. 12). Proceeding of the Network and Distributed System Security Symposium Secure Systems Lab Technical University Vienna; Giovanni Vigna.

Pierluigi, P. (2013). The Impact of Cybercrime: IT Security Boot Camps.

Pilling, R. (2013). Feature: Global threats, cyber-security nightmares and how to protect against them. *Computer Fraud & Security, 2013*, 14-18. doi: 10.1016/S1361-3723(13)70081-2

Plan, O. Y. A., Plan-main, O. Y. A., & Stones, S. (2017). Review of the Roots of Youth Violence: Literature Reviews Volume 5.

Polgar, S., & Thomas, S. A. (2011). *Introduction to Research in the Health Sciences E-Book*: Elsevier Health Sciences.

Ponemon. (2012). 2011 Cost of Data Breach Study (pp. 27).

Poonia, A. S., Bhardwaj, A., & Dangayach, G. (2013). Cyber Crime: Practices and Policies for Its Prevention.

Popper, K. (2013). *The poverty of historicism*: Routledge.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Prins, J. (2011). DigiNotar Certificate Authority breach'Operation Black Tulip': September.

Radware. (2015). DDoS Definitions - DDoSPedia.

Rantala, R. R. (2008). Cybercrime against businesses, 2005. *organization, 15*(14), 9.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7), 241-253.

Ringwelski, M. (2008). Effects of Cyber Crime.

Robert, P. (2015). DNS Pharming attacks target .com.

Rogers, M. (2000). Psychological Theories of Crime and" Hacking".

Rosenoer, J. (2012). *CyberLaw: The law of the Internet*: Springer Science & Business Media.

Ross, R. S. (2005). *Recommended security controls for federal information systems*: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Rouse, M. (2010). Search security. *TechTarget,[Online]. Available: http://searchsecurity. techtarget. com/definition/authentication.[Accessed 9 July 2016]*.

Saini, H., Rao, Y. S., & Panda, T. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*, 202-209.

San, T. S., Kirstie, H., & Konstantin, B. (2012). Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures. *Computer and Security*, 19.

Saravanan, k., & Asokan, R. (2011). Distributed Denial Of Service (Ddos) Attacks Detection Mechanism. *International Journal of Computer Science, Engineering and Information Technology, 1*(5), 11.

Say. (2013). IT Security Breaches hit more Small Firms. 2014, from http://www.techradar.com/news/internet/policies-protocols/security-breaches-hit-more-small-firms-1146901

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). *NIST special publication, 800*(2007), 94.

Schaap, A. J. (2009). Cyber warfare operations: Development and use under international law. *AFL Rev., 64*, 121.

Schell, B. H., & Martin, C. (2004). *Cybercrime: A reference handbook*: ABC-CLIO.

Sekaran, U., & Bougie, R. (2010). Research methods for business: A skill building approach. Wiley: London.

Selwyn, N. (2008). A safe haven for misbehaving? An investigation of online misbehavior among university students. *Social Science Computer Review, 26*(4), 446-465.

Sérgio, S. C. S., Rodrigo, M. P. S., Raquel, C. G. P., & Ronaldo, M. S. (2012). Botnets: A survey. *Computer Networks, 57*, 378-403. doi: http://dx.doi.org/10.1016/j.comnet.2012.07.021

Sesan, G., Soremi, B., & Louwafemi, B. (2014). Economic Cost of Cybercrime in Nigeria (pp. 11): University of Toronto.

Shariff, S. (2005). Cyber-dilemmas in the new millennium: School obligations to provide student safety in a virtual school environment. *McGill Journal of Education/Revue des sciences de l'éducation de McGill, 40*(3).

Sharma, & Xie, Y. (2008). Student Experiences of Using Weblogs: An Exploratory Study. *Journal of Asynchronous Learning Networks, 12*, 137-156.

Sharma, V. (2015). Information Technology and Cyber Crime. *IITM Journal of Information Technology, 1*, 75.

Shimomura, T., & Markoff, J. (1995). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaws-by the Man Who Did It*: Hyperion Press.

Shinder, D. L., & Cross, M. (2008). *Scene of the Cybercrime*: Syngress.

Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks, 57*(2), 378-403.

Sinanaj, G., & Muntermann, J. (2013). Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis. *in Proceedings of the 26th Bled eConference: eInnovation, Challenges and Impacts for Individuals, Organizations and Society, June 9-13 2013, Bled, Slovenia*.

Singleton, T. (2013). The Top 5 Cybercrimes. 15.

Smith. (2001). *Authentication: from passwords to public keys*: Addison-Wesley Longman Publishing Co., Inc.

Smith, Rana, R. S., Missiaen, P., Rose, K. D., Sahni, A., Singh, H., & Singh, L. (2007). High bat (*Chiroptera*) diversity in the Early Eocene of India. *Naturwissenschaften, 94*, 1003-1009. doi: 10.1007/s00114-007-0280-9

Sobell, M. G. (2013). *A Practical Guide to Fedora and Red Hat Enterprise Linux*: Pearson Education.

Stallings, W. (2007). *Network security essentials: applications and standards*: Pearson Education India.

Stein, S. (2008). ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Global strategic report (pp. 140). International Telecommunication Union Place des Nations, Geneva, Switzerland.

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks, 54*(8), 1245-1265.

Stihler, M., & Bachtold Jr, J. (2014). A UCONABC Resilient Authorization Evaluation for Cloud Computing. *system, 1*, 2.

Stoll, C. (2005). *The cuckoo's egg: tracking a spy through the maze of computer espionage*: Simon and Schuster.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., . . . Vigna, G. (2009). *Your botnet is my botnet: analysis of a botnet takeover.* Paper presented at the Proceedings of the 16th ACM conference on Computer and communications security.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Information Security Program Roles and Responsibilities (2015).

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication, 800*(82), 16-16.

Stuart, M., & Headlam, N. (2008). *Research Methods Handbook : Introductory guide to research methods for social research*. Manchester, UK: Centre for Local Economic Strategies(CLES).

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications, 34*(1), 1-11.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.".

Symantec. (2012). The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It *The Ongoing Malware Threat* (pp. 1-11). USA.

Symantec Corporation. (2014). Internet Security Threat Report *2013 Trends* (Vol. 19, pp. 97). Mountain View, Carlifornia, USA.

Taft, D. K. (2010). Survey: Infrastructure-as-a-Service Adoption on the Rise-IT Infrastructure-News & Reviews-eWeek. com: Aug.

Tari, F., Ozok, A., & Holden, S. H. (2006). *A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords.* Paper presented at the Proceedings of the second symposium on Usable privacy and security.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society, 31*(1), 6-11.

Thampi, P. K. K., Anand, A., & Balakrishnan, R. (2014). Recovery of Digital Evidence from Social Networking Sites.

Thompson, S. T. (2013). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries, 25*(4), 222-225.

Thornewell, P., & Hughes, J. R. (2014). Secure sockets layer protocol handshake mirroring: Google Patents.

Tongco, D. C. (2007). Purposive Sampling as a Tool for Informant Selection. *Ethnobotany Research and applications : A journal on Plants, People And Applied Research*, 147-158.

Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing information systems security: critical success factors and indicators to measure effectiveness *Information Security* (pp. 530-545): Springer.

Umar-Ajilola. (2010). Fighting Cybercrime in Nigeria.

United Nations Office of Drugs and Crime, V. (2013). Comprehensive study on Cybercrime (pp. 347).

Urbas, G., & Choo, K.-K. R. (2008). *Resource materials on technology-enabled crime*: Australian Institute of Criminology.

Valkenburg, P. M., & Peter, J. (2009). The effects of instant messaging on the quality of adolescents' existing friendships: A longitudinal study. *Journal of Communication, 59*(1), 79-97.

Van Eeten, M., & Bauer, J. M. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management, 17*(4), 221-232.

Verizon, R. (2013). Data Breach Investigation Report (pp. 63).

Viswanath, V., Brown, S. A., & Hillol, B. (2013). BRIDGING THE QUALITATIVE-QUANTITATIVE DIVIDE: GUIDELINES FOR CONDUCTING MIXED METHODS RESEARCH IN INFORMATION SYSTEMS. . *37*(1), 34.

Wacker, J. G. (1998). A definition of theory: research guidelines for different theory-building research methods in operations management. *Journal of operations management, 16*(4), 361-385.

Wada, & Odulaja. (2012a). Assessing Cyber crime and its Impact on E-Banking In Nigeria Using Social Theories. *African Journal of Computing & ICT, 5*, 69-82.

Wada, & Odulaja. (2012b). Electronic Banking and Cyber Crime In Nigeria-A Theoretical Policy Perspective on Causation.

WaII, D. S., & Yar, M. (2010). Intellectual property crime and the internet: cyber-piracy and stealing information intangibles. *Handbook of internet crime*, 255.

Walker, G., Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in Nigeria. *The Electronic Library, 26*(5), 716-725.

Walter, F., Patricio, Z., Marco, S., & Pablo, G. (2011). Alternative Engine to Detect and Block Port Scan Attacks using Virtual Network Environments. *International Journal of Computer Science and Network Security(IJCSNS), 11*(11), 14-23.

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective, 23*(4-6), 172-178.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *The International Journal of Cyber Criminology, 5*, 736-749.

Wasserman, M., & Baker, F. (2011). IPv6-to-IPv6 network prefix translation.

Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection*: John Wiley & Sons.

White, C. (2010). *Data communications and computer networks: A business user's approach*: Cengage Learning.

Whitman, M., & Mattord, H. (2011). *Principles of information security*: Cengage Learning.

Whitman, M. E., & Mottord, H. J. (2012). *Principles of Information Security*.

Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems, 48*(3), 15.

Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.-C. (2006). *Design and evaluation of a shoulder-surfing resistant graphical password scheme.* Paper presented at the Proceedings of the working conference on Advanced visual interfaces.

Winston, R. B. (1990). The Student Developmental Task and Lifestyle Inventory: An approach to measuring students' psychosocial development. *Journal of College Student Development*.

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review, 26*(3), 317-333.

Wong, M. W. (2006). Cyber-trespass and 'unauthorized access' as legal mechanisms of access control: Lessons from the US experience. *International Journal of Law and Information Technology, 15*(1), 90-128.

Woods, M. (2011). Interviewing for research and analysing qualitative data: An overview. [online], available: http://owll.massey.ac.nz/pdf/interviewing-for-research-and-analysing-qualitative-data.pdf

Wool, A. (2010). Trends in firewall configuration errors: Measuring the holes in swiss cheese. *IEEE Internet Computing, 14*(4), 58-65.

WordPress. (2006). Cross Doamin Solution: Ensuring Complete Security. from http://www.crossdomainsolutions.com/cyber-crime/

Wu, K.-g., & Feng, Y. (2006). Proactive worm prevention based on p2p networks. *IJCSNS, 6*(3B), 205.

Wyk, B. (2013). Research Design and Methods Part 1: Post-graduate enrollment and throughput. [online], available: https://www.uwc.ac.za/Students/Postgraduate/Documents/Research_and_Design_I.pdf.

Xu, J., Zhu, W.-T., & Feng, D.-G. (2009). An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces, 31*(4), 723-728.

Yassir, A., & Nayak, S. (2012). Cyber Crime: Threat to Network Security. *IJCSNS, 12*(2), 2555-2559.

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.

Yin, R. (2009). *A case study research: Design and Methods* (third ed. Vol. 5). Thousand Oaks, London, New Dehli: SAGE publications.

Yong-Hong, G. (2011). Study and Application of Operating System security baseline.

Zittrain, J. L. (2006). The generative internet. *Harvard Law Review*, 1974-2040.

APPENDICES

Appendix A: Informed Consent Form to Participants for Interview Guide

UNIVERSITY OF KWAZULU-NATAL

Discipline of Information Systems & Technology

School of Management, Information Technology & Governance

MCom Research Project

Researcher: Bukhari Badamasi (+2780372970, +2348036992294)

Supervisor: Prof. Manoj Maharaj (031-2607051)

Co-Supervisor: Nurudeen Ajayi (033-2606013)

Research Office: Ms P Ximba (031-2603587)

CONSENT

I…… (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire.

For Interview:

I c□sent / do not□nsent to having this interview audio-recorded

Signature of Participant: _____ Date: _____

Appendix B: Interview Schedule

Research Topic: The Effects of Security Protocols on Cybercrime

At Ahmadu Bello University, Zaria –Nigeria

MCom Research Project

Discipline of Information Systems & Technology

School of Management, Information Technology & Governance

University of KwaZulu-Natal

Researcher: Bukhari Badamasi (+27780372970, +2348036992294)

Supervisor: Prof. Manoj Maharaj (031-2607051)

Co-supervisor: Nurudeen Ajayi (033-2606013)

Introduction

My name is Bukhari Badamasi. I am a Masters candidate in the Discipline of Information Systems & Technology, in the School of Management, Information Technology & Governance, at the University of KwaZulu-Natal.

I will like to ask you some questions about the security breaches within the university, with the purpose of investigating the various types of cybercrimes that affects this university (Ahmadu Bello University), how effective the security protocols are in relation to cybercrimes on the university's network.

I hope to use the gathered information to propose security measures that would enable Ahmadu Bello University and other organisations to sustain their respective functions, enhance their processes and structures, manage their Information Systems, provide and manage security, ensure information integrity, confidentiality, and information availability at Ahmadu Bello University, Zaria.

The following key words would be frequently used during the interview:

Cybercrime: Cybercrime may be referred to as the process whereby competing Nations, organisations or selfish individuals get unauthorized access, intercepts and manipulates data.

Cyber security: Cyber security may be defined as the collection of various tools, legislative policies, cyber security concepts, risk management techniques, training, best practices and technologies that can be useful in safeguarding Cyber Security infrastructures and individual assets

Information Systems: Information Systems may be defined as the combination of the Hardware and Software Systems that support data intensive applications and processes.

The interview would be between 45 minutes to 1:00 Hour

The interview schedule questions:

1. **What Types of Cybercrimes is the Ahmadu Bello University Network is Susceptible to?**

i. Please share with me which of the Cybercrimes the Ahmadu Bello University Network is Susceptible to

ii. Tell me which of these cybercrimes has ever been experienced on the Ahmadu Bello University Network

2. **What areas of the University Network are Vulnerable to Cybercrime?**
   i. Please share with me which areas of the Ahmadu Bello University Network is Vulnerable to Cybercrimes
   ii. Share with me the Areas of the Network that has experienced Cybercrimes recently

3. **How effective are the security protocols used by Ahmadu Bello University in protecting their Network from cybercrime**

i. Pease share with me the Security Protocols used by Ahmadu Bello University in protecting their Network from cybercrime

ii. Can you please tell me how effective these security protocols have been in protecting the Ahmadu Bello University Network from Cybercrime.

Is there any issue that you may like to share or mention regarding the network preventive measures and/or effects of security controls on cybercrime?

Thank you for your time – it is highly appreciated!!!

APPENDIX C: Responses of the Interview

		RP	Narratives (Familiarizing with data)	Open Codes (Generating codes)	Related Open Codes	Subcategories (Searching for Themes)	Related subcategories (Reviewing and categorizing themes)	Categories (Refining and naming themes)
RQ1	**What Types of Cybercrimes is the Ahmadu Bello University Network is Susceptible to?**							
Sub Question 1	Please share with me which of the cybercrimes the ABU Network is susceptible to?	1	Ok, thank you. We have Social engineering, spam, malware, software hacking are the types of cybercrime that the university could be a victim to.	1) Ok, there is Social engineering, 2) Spam 3) Software hacking could all be susceptible to university network. 4) System penetration	Social engineering (R1)(R4) Spamming (R1)(R2)(R6) Malware (R1) (R4) Hacking (R1)(R2)(R3)(R5)(R6)(R8)(R10)(R14)	**1. Hacking** **2. Hijacking** **3. Phishing** **4. Illegal Bandwidth usage** **5. Piracy** **9. Fraud** **10. Password cracking**	**Password snipping** **Phishing attacks** **Shoulder**	**Social Engineering**
		2	Website hijacking, Domain Hijacking, Phishing, spamming, illegal bandwidth usage, and portal hacking. On ABU Network, phishing is one of the common attack that criminals used to victimized students. Criminals use to visit most of the digital centres within the university and watch	5) Website hijacking. 6) Domain Hijacking. 7) Phishing. 8) Spamming. 9) Illegal bandwidth usage. 10) Portal hacking.	Hijacking (R2)(R7) Phishing (R2)(R4)(R6)(R8)(R9)(R13) Illegal Bandwidth usage (R2)(R5)(R10)(R12)(R14)(R15)			

			users while entering their log-in credentials in order to get the victim details			**11. SQL Injection** **12. Cross-site scripting** **13. Identity theft** **14. Phonograph** **15. Computer misuse** **16. DoS** **17. Forgery** **18. Pharming** **19. IP-Spoofing** **20. Spamming** **21. IP-Spoofing**	**Surfing** **Forgery** **Social engineering** **Ip-spoofing** **Hacking** **DoS** **Hijacking**	
		3	Piracy, hacking and fraud.	11) Piracy. 12) Hacking. 13) Fraud.	Piracy (R3) Fraud (R3)(R9)			
		4	One very common cybercrime is Social engineering which is common among students, between friends and their classmate and even at Faculties level. We get a lot of spam and phishing. We also have issues of malicious software as well as password cracking.	14) Social engineering 15) Spamming 16) Phishing 17) Password cracking.	Password cracking (R4)			**SQL Injection**
		5	Major security issues that we undergo are website hacking, illegal bandwidth usage, portal hacking. Also during student registration, base on the fact the portal was developed by both staff and students. Some students use that avenue to link out the link to other students. And cybercrime usually happening from within the University.	18) Website hacking, illegal bandwidth usage, portal hacking.				
		6	SQL Injection, cross-site scripting, Identity theft, phishing and email spamming, Malicious Hacking (Attacks). Denial of Service (DoS) is the fundamental key to all the problem we are facing at	19) SQL Injection, cross-site scripting, Identity theft, phishing and email spamming, Malicious Hacking (Attacks). 20) DoS	SQL Injection (R6)(R7) Cross-site scripting (R6)(R7)			

			ABU, specifically ICICT		DoS (6) Identity theft (R6)(R8)(R9)	**22. DoS** **23. Hacking**	**Illegal bandwidth usage**	**Denial of Service Attacks**
		7	Cross-site request forgery (CSRF), Session Hijacking, and SQL Injection.	21) Cross-site request forgery (CSRF), Session Hijacking, and SQL Injection.		**24. Spying**		
		8	Identity theft, Phishing, Hacking, Phonograph, and Computer misuse.	22) Identity theft, Phishing, Hacking, Phonograph, and Computer misuse could victimize ABU Network.	Phonograph (R8) Computer misuse (R8) (R10)	**25. Hijacking**	**Fraud** **Identity theft**	
		9	Phishing, Internet fraud, denial of service attack, hacking, identity theft and forgery.	23) There are issues like Phishing, Internet fraud, denial of service attack, hacking, identity theft forgery that can easily affect the university network.	DoS (R9) (R10) Forgery (R9) (R10)	**25. Illegal Bandwidth Usage**	**Password cracking** **Virus**	
		10	Website hacking and illegal bandwidth usage.	24) Website hacking and illegal bandwidth usage.			**Spamming**	
		11	So, this Crime or cybercrime is in different form, we have both online and offline crime that this University could be a victim to. We have issues like Denial of service attack, network intrusion and computer misuse as well as illegal bandwidth usage.	25) There are issues of denial of service attack, network intrusion, computer misuse and illegal bandwidth usage.		**26. Botnet Attack** **27. Viruses**	**Trojan horse** **Spyware**	
		12	The University network can only be victimize through illegal bandwidth usage.	26) The University network can be victimized illegal bandwidth usage.			**Malware**	**Malware**
		13	Computer crime can be done on the cyberspace by cybercriminals. This could be in a form of phishing and farming.	27) Computer crime can be done in a form of phishing and farming.		**28. Ransomeware**	**Denial of Service attack**	

		14	Hacking of student e-mails, hacking of university portal, illegal use of bandwidth.	28) Hacking of student e-mails, hacking of university portal, illegal use of bandwidth.				
		15	Modern technologies can be used by cybercriminals to victimize the university network. IP-spoofing, illegal bandwidth usage can all affect the university network.	29) University network is done through IP-spoofing, illegal bandwidth usage.	IP-Spoofing (R15)		**Pharmming**	
Sub Question 2	Share with me which of the these cybercrimes has ever been experienced in the Ahmadu Bello University Network	1	Attacks like spamming, IP-spoofing, hacking, spying, and Traffic of Website.	30) The respondent stated spamming, 31) IP-spoofing 32) Hacking 33) Spying	Spamming (R1)(R2)(R4)(R6)(R13) IP-Spoofing (R1)(R4) (R13) Hacking (R1)(R2)(R4)(R5)(R8)(R13)(R14) Spying (R1) Website Traffic (1)	**29. Spamming** **30. IP-Spoofing** **31. Hacking** **32. Spying** **33. Social engineering**	**Piracy** **Website Traffic** **IP Spoofing**	**Pharming**
		2	Website hijacking, portal hacking, spamming, and illegal bandwidth usage	34) Website hijacking 35) Portal hacking 36) Spamming 37) Illegal bandwidth usage	Hijacking (R2)(R7) Illegal Bandwidth Usage (R2) (R5)(R10)(R11)	**34. Hijacking** **35. Illegal Bandwidth Usage**		
		3	Stealing of password,	38) Stealing of password	Stealing of	**33. Stealing of**	**IP-Spoofing**	

			Allocation of Room by insider to students	39) Allocation of Room by insider to students	password (R3)(R4)(R11)(R13) Allocation of rooms (R3)	**password** **34. Allocation of rooms**	**Hacking** **Spying**	**Website Defacement**
		4	We are experiencing a lot of spamming, hacking of other network, issues of password sniffing, IP-Spoofing, surfing, IP-Mark., DoS. We also experienced that a new content on the website always attracacked	40) We are experiencing a lot of spamming, 41) hacking of other network, 42) issues of password sniffing, 43) IP-Spoofing, 44) surfing, 45) IP-Mark.	Web Surfing (R4) DoS Attack (4) (12)(14)	**35. Web Surfing**	**Hijacking** **DoS** **Illegal Bandwidth Usage** **Stealing of password**	
		5	While as I said earlier, portal hacking, illegal bandwidth usage (by downloading some file from tenths of thousand of computers), using of hotspot of someone	46) While as I said earlier, portal hacking, 47) illegal bandwidth usage (by downloading some file from tenths of thousand of computers), 48) using of hotspot of someone			**Allocation of Rooms** **Identity theft** **Electronic Bullying**	
		6	E-mail spam and phishing, identity theft, malicious software. This university seen a lot of port scans on the server infrastructure side. The university network has also seen lots of SYN programs running on their web service that are constantly looking for	49) E-mail spam 50) phishing, 51) identity theft, 52) malicious software 53) Port scan	Phishing (R6)(R8)(R10)(R11)(R14) Identity theft (R6)(R8)(R9)(R12)(R15) Malicious	**36. Phishing** **37. Identity theft** **38. Malicious software**	**Port Scan** **DoS**	

			vulnerabilities to exploit.		software (R6) Port Scan (R6)		**Phishing**	
		7	Cross-site request forgery, session hijacking	54) Cross-site request forgery, 55) session hijacking	Cross-Sire Request Forgery (R7)(R9)	**39. Cross-Sire Request Forgery**	**Malicious Software**	
		8	Experienced phishing, identity theft, and hacking	56) Experienced phishing, 57) identity theft, and 58) hacking			**Pharming**	**Port Scan**
		9	Denial of service attack, identity theft, counterfeiting and forgery	59) Denial of service attack, 60) identity theft, 61) counterfeiting and 62) forgery	DoS attack (R9)	**40. DoS attack**	**Network Intrusion**	
		10	Phishing, phamming, students' harassment, cyberextortion, intrusion, virus attack, illegal use of bandwidth are all forms of crime that affect the University.	63) Phishing, 64) phamming, 65) students' harassment, 66) cyberextortion, 67) intrusion, 68) virus attack, 69) illegal use of bandwidth are all forms of crime that affect the University.	Phamming (R10) Network Intrusion (R10)(R15) Virus attack (R10)	**41. Phamming** **42. Network Intrusion** **43.Virus attack**	**Virus attack** **Cyber Stalking**	
		11	Social engineering, password sniffing, illegal bandwidth usage, phishing. Yes, we also	70) Social engineering, 71) password sniffing,				

			experienced allocation of rooms by some students	72) illegal bandwidth usage, 73) phishing. Yes, we also experienced 74) allocation of rooms by some students				
		12	Identity theft is one of the common type of cybercrime experienced here ABU. The personal information stolen can include the person's data or credit card numbers. This stolen information is then used to obtain new credit cards, access bank accounts or obtain other benefits, such as driver's license, student's registration number.	75) Identity theft is one of the common type of cybercrime experienced here ABU. The personal information stolen can include the person's data or credit card numbers. This stolen information is then used to obtain new credit cards, access bank accounts or obtain other benefits, such as driver's license, student's registration number.				
		13	Issues like spamming, hacking of the university Network, issues of password sniffing, IP-Spoofing, surfing, IP-Mark.	76) Issues like spamming, 77) hacking of the university Network, 78) issues of password sniffing, 79) IP-Spoofing, 80) surfing, 81) IP-Mark.				
		14	Credit theft, electronic bullying and stalking, Hacking for Fun, and phishing.	82) Credit theft, 83) electronic bullying and	Electronic bullying (R14) Cyber stalking	**44. Electronic bullying** **45. Cyber**		

				84) stalking, 85) Hacking for Fun, and 86) phishing.	(R14)	**stalking**		
		15	Credit theft, identity theft, Network intrusion and software piracy. Because university students are very good in copying people's information. Similarly, on the network they good in copying or piracy.	87) Credit theft, 88) identity theft, 89) Network intrusion and 90) software piracy. Because university students are very good in copying people's information. Similarly, on the network they good in copying or piracy.	Piracy (15)	**46. Piracy**		
RQ2	**What Areas of the University Network are Vulnerable to Cybercrime?**							
Sub Question 1	Please share with me which areas of the ABU Network are Vulnerable to Cybercrimes	1	Well, in ABU there are many places that are vulnerable like the whole ABU Network is vulnerable to attack	1) ABU Network	ABU Network (R1)(R2)(R7)(R11)(R14)(R15)	**1. ABU Network**	**Admission Page**	
		2	ABU Network and Admission page	2) ABU Network 3) Admission Page	Admission page (R2)(R10)(R14)(R15)	**2. Admission page**		
		3	University Website and registration page are much more vulnerable to attack	5) University website 6) Registration page	University Website (R3)(R4)	**Registration page**		
		4	One major area that is vulnerable is the whole Registration Portal.	7) Registration Portal	Registration Portal			
		5	Accommodation portal and Registration portal	8) Accommodation portal 9) Registration Portal.	Registration page (R3)(R5)(R6)(R9			

					)(R13) Accommodation page (R8)(R12)			
		6	Registration portal	10) Registration portal				
		7	University Network is always at risk	11) University Network		Accommodation page		
		8	Accommodation page	12) Accommodation page				
		9	Registration page	13) Registration page				
		10	Admission page	14) Admission page				
		11	University Network is always at risk	15) ABU Network				
		12	Accommodation page	16) Accommodation				
		13	Registration page	17) Registration				
		14	ABU Network and Admission page	18) ABU Network 19) Admission Page				
		15	ABU Network and Admission page	20) ABU Network 21) Admission Page				
Sub Question 2	Tell me the Areas of the Network that has experienced cybercrimes recently	1	While, in ABU there are many places that are vulnerable like the whole ABU Network is vulnerable to attack	22) ABU Network	ABU Network (R1)(R2)(R7)(R11)(R14)(R15)	**1. ABU Network** **2. Admission page**	**Admission Page**	

						Registration page		
		2	ABU Network and Admission page	23) ABU Network 24) Admission Page	Admission page (R2)(R10)(R14)(R15)			
		3	University Website and registration page are much more vulnerable to attack	25) University website 26) Registration page	University Website (R3)(R4)			**University Registration Portal**
		4	One major area that is vulnerable is the whole University website.	27) University Website				
		5	Accommodation portal and Registration portal	28) Accommodation portal 29) Registration Portal.	Registration page (R3)(R5)(R6)(R9)(R13) Accommodation page (R8)(R12)			
		6	Registration portal	30) Registration portal			**Accommodation Page**	
		7	University Network is always at risk	31) University Network				
		8	Accommodation page	32) Accommodation page				
		9	Registration page	33) Registration page				
		10	Admission page	34) Admission page				
		11	University Network is always at risk	35) ABU Network				

		12	Accommodation page	36) Accommodation				
		13	Registration page	37) Registration				
		14	ABU Network and Admission page	38) ABU Network 39) Admission Page				
		15	ABU Network and Admission page	40) ABU Network 41) Admission Page				
RQ3	**How Effective are the security protocols used by Ahmadu Bello University in protecting their Network from cybercrime?**							
Sub Question 1	Please share with me the security protocols used by Ahmadu Bello University in protecting their network from cybercrime	1	Use of wireless link by controlling access from the users' end.	1) Use of wireless link, 2) Controlling access	Wireless link (R1) Access control (R1)	**1. Wireless link** **2. Access control**		
		2	On the University Network, there is a monitoring software that monitors every single activity executed by both staff and students. Similarly, Log-in credentials are provided to users of the University Network.	3) Proper Use of monitoring software 4) Log-in credentials	Monitoring software (R2)(R4) Log-in(R2)(R4)	**3. Monitoring software** **4. Log-in**		
		3	There is a set of people who their work is test whether the university network can be penetrate by cybercriminals or not. So, Robustness test and deployment of new technology is always a priority on the University network.	5) Robustness testing 6) Deployment of new preventive mechanism	Robustness testing(R3) Deployment of preventive measures(R3)	**5. Penetration testing** **6. Deployment of security measures**	**Security Base Line**	

		4	On the University Network, there is a monitoring software that monitors every single activity executed by both staff and students. Similarly, Log-in credentials are provided to users of the University Network.	7) Proper Use of monitoring software 8) Log-in credentials				**Security measures**
		5	On the University network, there are a lots of risk, so most often the expert analyse the risk and overcome such risk.	9) Analysing the Risk frequently	Risk analysis(R5)	**Risk analysis**		
		6	Regular training of professionals on the issues related to security	10) Regular Training	Training(R6)	**Training**		
		7	By constantly making users aware of what is does and don't on the university network.	11) Constant awareness	Awareness(R7)	**Awareness**		
		8	Usually, on the university network a fire is set. The firewall could be circuit level firewall, application level firewall or stateful multilayer firewall	12) Proper use of firewall	Firewall(R8)(R15)	**Firewall**		**Security Tools**
		9	Though, the most common and first preventive measures is Anti-virus software.	13) Antivirus software	Anti-virus(R9)(R10)(R11)(R12)(R13)	**Antivirus**		
		10	Usually, on the university network a fire is set. The firewall could be circuit level firewall, application level firewall or stateful multilayer firewall. Though, the most common and first preventive measures is Anti-virus software.	14) Firewall 15) Antivirus software		**Antivirus**		
		11	Anti-virus software is most frequently used on the					

			university network.					
		12	Though, the most common and first preventive measures is Anti-virus software.	16) Antivirus software		**Antivirus**	**Host or Endpoint Based Tools**	
		13	Usually, on the university network a fire is set. The firewall could be circuit level firewall, application level firewall or stateful multilayer firewall. Though, the most common and first preventive measures is Anti-virus software.	17) Firewall 18) Antivirus software		**Antivirus**		
		14	All organisations uses password authentication likewise, Ahmadu Bello University requested every user must use a strong password in order to protect themselves from intruders	19) Provision of password	Password authentication(R 14)	Password authentication		
		15	Usually, on the university network a fire is set. The firewall could be circuit level firewall, application level firewall or stateful multilayer firewall	20) Proper use of firewall		**Firewall**		

Appendix D: Gatekeeper

INSTITUTE OF COMPUTING & ICT
AHMADU BELLO UNIVERSITY, ZARIA, NIGERIA

Vice Chancellor
Professor Abdullahi Mustapha
B.Sc. (Hon) Pharm. (ABU), Ph.D. (London), FPSN
Telephone: (069) – 555251 D1, 550691, 552439
E-Mail: vc@abu.edu.ng

Director
Professor Sahalu B. Junaidu
B.Sc. (ABU), M.Sc. (London), Ph.D. (St. Andrews), MACM, MIEEE
Telephone: 0703-215-4610,0705-518-7856
E-mail: sahalu@abu.edu.ng, iacc@abu.edu.ng

Our Ref: **ICICT/8/3** Date: **June 27, 2014**

Mal. Bukhari Badamasi
School of Management, IT and Governance,
University of KwaZulu-Natal,
Wesville, South-Africa.

Dear Sir,

RE-REQUEST FOR PERMISSION TO CONDUCT RESEARCH AT AHMADU BELLO UNIVERSITY, ZARIA - NIGERIA

Your correspondence of 24th June 2014 addressed to the Director, ICICT, on the above subject refers, please.

I am directed to inform you that the Director ICICT has approved your request to interview and administer questionnaire to some staff of the Institute as part of data collection process for your research work on *The Effect of Physical Security Protocols on Cybercrime.*

Thank you.

Yours faithfully,

INSTITUTE SECRETARY
Institute of Computing & ICT
Ahmadu Bello University,
Zaria- Nigeria.

Usman Shehu Lawal MNIM, MIPA
Asst. Institute Secretary
For: Director

Appendix E: Ethical Clearance

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

18 September 2014

Mr Bukhari Badamasi 212560983
School of Management, IT & Governance
Westville Campus

Dear Mr Badamasi

Protocol reference number: HSS/1105/014M
Project title: The effects of physical security protocols on Cybercrimes at Ahmadu Bello University, Zaria - Nigeria

Full Approval – Expedited Application

In response to your application dated 4 August 2014, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol have been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the 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 a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

.....

Dr Shamila Naidoo (Deputy Chair)
Humanities & Social Sciences Research Ethics Committee

/pm

Cc Supervisor: Professor Manoj Maharaj & Mr Nurudeen Ajayi
Cc Academic Leader Research: Professor Brian McArthur
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (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 / anymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville