COMBATING CYBERCRIME: FRAMEWORK, TOOLS AND PEOPLE

Submitted by

- Dr. O. Osunade
  Reader, Department of Computer Science (CSC)
  08033264855 e-mail: seyiosunade@gmail.com, o.osunade@ui.edu.ng

- Dr. Funmilola O. OMOTAYO
  Lecturer I, African Regional Centre for Information Science (ARCIS)
  08052265285 e-mail: lolaogunesan@yahoo.com

- Deborah D. Adeyemo
  Lecturer II, Department of Public Law, Faculty of Law
  08037395771 e-mail: deborahdadeymo@gmail.com

- O. A. Awujoola
  Assistant Lecturer, Department of Library, Archival and Information Studies (LARIS)
  08181140123 e-mail: abileks132917@gmail.com

- S. O. Oyebamiji
  Senior Systems Analyst, Department of Library, Archival and Information Studies (LARIS), 08038284819 e-mail: so.oyebamiji@ui.edu.ng

Period: June 2019 to September 2020

Amount requested: Four million nine hundred forty-three thousand and five hundred naira only (₦4,943,500.00)

Other Proposed Sources of Funding: West and Central Africa Research and Education Network (WACREN)

EXECUTIVE SUMMARY

Cyber security frameworks and various implementation strategies have been used to combat the challenge of fraudulent acts or crimes using computers or computer network resources. In Nigeria, the framework is just being developed and requires adequate input from all sectors of the economy. Measures to build the framework such as policy and law such as the Nigerian Cybercrime Act of 2015 have recently been completed; however there is a need to domesticate a framework for the education sector.

According to Wild (2018) there are over 250 security frameworks worldwide that have been developed for various organisations. Examples include Control Objectives for Information and Related Technology (COBIT), ISO 27000 Series and NIST SP 800 Series. The frameworks and standards are implemented using cyber security teams called Community Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), and Security Operations Center (SOC).

The quasi-experimental approach will be used to carry out this research. The target population is all Nigerians who use computers and computer network resources. The sample will be tertiary institutions in Oyo State because they are frequent users of computers and computer network resources. Data will be collected using log files from the developed electronic platform and questionnaires at workshops. Analysis will be carried out using simple statistical inferences. The performance of the cyber protection will be evaluated using number of incidents reported, incidents solved, frequency of visitors to online platform and feedback from users. When security incidents are reduced, cybercrime will be reduced or eliminated.

Corruption can be detected, investigated and prevented when electronic resources are used to carry out the act. The domestication of a cyber security framework for Nigeria and specifically for tertiary institutions will provide the much needed guidance for combating cybercrime. The cyber protection unit, personnel training, website and open source software will ensure that the manpower and resources to always prevent corruption through electronic devices such as computers and computer networks are available and sustainable.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ARCIS - African Regional Centre for Information Science

CERT - Community Emergency Response Team

CSIRT - Computer Security Incident Response Team

Cyber – use of computers or computer networks

Cybercrime – this is the illegal use of computers and computer networks

Cyber stalking - this is act of using the Internet to repeatedly harass another person

IT - information technology

UI – University of Ibadan

LARIS - Department of Library, Archival and Information Studies (LARIS)

SOC - Security Operations Center

INTRODUCTION

Corruption in whatever dimension is a fundamental anomaly in all human society. In 2012, Nigeria was estimated to have lost over $400 billion to corruption since independence (Okoye, 2012), with a percentage coming from the use of computers and computer networks. Corruption is a crime against humanity. The potential for corruption and crime using cyber space is great because the communication is non-facial and physical security measures do not apply (DiGiacomo, 2017). There are different types of corruption but germane to this research is cybercrime. Cybercrime occurs when computing and computer network resources, such as the Internet, are used to illegally gain access to resources such as information. Information is a critical resource that can be manipulated, hijacked, distorted and deleted. One of the building blocks of cybercrime is security incidents. Security incidents are instances where users or network providers are attacked by cyber criminals seeking information. There are variety of security incidents from automated to manual; software to hardware; and physical to psychological. Examples include money laundering, sexual exploitation of minors, cyber stalking, and data loss.

Cybercrime has become a great concern and embarrassment to many countries and organisations not leaving out higher educational institutions. It is a widespread phenomenon in developing countries and rampant among students and members of the academic community. This is not because the people are different from other people of the world, but because the conditions are appropriate for it. There may be reasons why this is so, most especially in higher institutions of learning which can include: culture of people towards cybercrime, lack of legal framework to address cybercrime, weak cybercrime enlightenment programmes and absence of cyber security agencies and institutions to check the menace. However, fighting cybercrime in higher institutions of learning requires adopting an applicable framework and committing to the effectual implementation of the framework involving all stakeholders.

According to Wild (2018), there are over 250 security frameworks worldwide that have been developed for various organisations. The proliferation of frameworks, their implementation and sustainability have raised concerns for computer network service providers. The inability of service providers to effectively handle security incidents have led to formation of cyber security teams such as Community Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), and Security Operations Center (SOC) that are being adopted across organisations. There are overlaps in the responsibilities, tasks and resources required to operate each team.

Tertiary institutions provide a large number of cyber users in Nigeria. The tertiary institution community contains a widespread of users that are prone to cybercrimes and cybercrime. The users are active, knowledgeable, economically stable and financially relevant. Thus, this multidisciplinary research aims to prevent cybercrime by creating a cyber security unit within tertiary institutions to detect, investigate, solve, store and share information related to security threats and solutions using a domesticated cyber security framework. When security incidents are reduced, cybercrime will be reduced or eliminated.

STATEMENT OF RESEARCH PROBLEM

The use of computers and computer networks by individuals, tertiary instutions and commercial organizations has increased over the years. Transactions using computers require the creation of electronic profiles for each person or group of persons. The profiles allow access to resources that are financial, educational, entertaining and informative. Profiles can be hijacked, manipulated or re-created in other to obtain an advantage over others by gaining access to the information available to a specific profile. The information illegally obtained is then used to commit fraudulent acts or crimes. The fraudulent acts or crimes are called security incidents and occur on a daily basis with a lot not being reported. Several reasons, such as reputation, culture towards cybercrime, lack of digital evidence and legal framework, have been given for this by victims, service providers and organizations. Cyber security frameworks and various implementation strategies are being used to combat this challenge. In Nigeria, the framework is just being developed and requires adequate input from all sectors of the economy. Measures to build the framework through policy and law led to the Nigerian Cybercrime Act of 2015, which has recently been completed; however there is a need to domesticate a framework for the education sector.

The cyber attacks currently experienced by tertiary institutions such as universities are not treated as serious issues because they are classified as information technology-based problems. This wrong classification has not reduced the frequency of the incidents thus a need to focus on the incidents from a security viewpoint.

Tertiary institutions in Nigeria are lagging behind due to the changes and cost associated with implementing cyber security solutions and frameworks. The frequency, variety of security attacks and resources required to adequately secure information resources and minimize cyber crimes has tripled in the last few years overwhelming the network services team. There is then the need for specialisation, capacity development and legislation in order to adequately combat cybercrime. A cyber security framework that takes into consideration the peculiarities of tertiary institutions would go a long way into combating cybercrimes.

RESEARCH QUESTIONS

The research work will attempt to answer the following questions:

- What constitute cybercrime in a university environment?
- What resources are available and sustainable for combating cybercrime in a university environment?
- How can a cyber-protection unit function within a university environment?
- What is the impact of a cyber-protection unit in a university environment?
- How can cyber protection unit personnel be trained and incidents reported, stored, archived and shared with cyber-protection units in other tertiary institutions?
- Is the Nigerian Cybercrime Act of 2015 sufficient to combating cybercrime in a university environment?

RESEARCH OBJECTIVES

The aim of this multidisciplinary research is to prevent cybercrime by creating a cyber security unit within a tertiary institution to detect, investigate, store and share information security threats and solutions using a domesticated framework.

The objectives for this work include:

i. Identifying and documenting types of cybercrime in the university community
ii. Providing resources to combat cybercrime and developing a cyber security framework/Unit for tertiary institutions
iii. Training of cyber protection unit personnel to detect, prevent and investigate information security threats using open source software tools
iv. Design and hosting of a record storage and archival platform for sharing information security related issues
v. Legal interpretations of cyber security solutions using Nigerian Cybercrime Act (2015)
vi. Evaluation of the cyber protection unit operations using number of incidents, number of visitors to platform, time taken to resolve incidents and adherence to privacy issues as metrics.

LITERATURE REVIEW

Cybercrime involves the use of computer or computer network such as the Internet to perpetuate acts that are criminal or against acceptable processes. Cybercrime is any kind of illegal, unethical and unauthorised behavior in a system which processes information automatically or transfers data. Cybercrime includes but is not limited to e-mail scam, hacking, distribution of hostile software, extortion, fraud, impersonation, theft of data, service attacks, terrorism, stalking (Hassan, Lass & Makinde, 2012 and Awe, 2013). Cybercrime can be perpetuated by people from anywhere in the world and executed irrespective of geographical location.

In Nigeria, cybercrime also known as “yahoo yahoo” or “419” is a menace to the society whose impact cannot really be quantified. It has been a great concern and embarrassment to the country and organisations. According to the Punch newspaper (2018) “mondaq.com reported on December 3rd, 2018, cyber-attacks across Nigeria resulted in total losses of $649 million in 2017, significantly up from the $550 million it cost in 2016, while the 2017 Nigerian Electronic Fraud Forum Report estimated that financial damages from online banking fraud during 2015-2017 amounted to ₦5.571 billion, with mobile payments fraud rising to almost ₦350 million in 2017 and ATM fraud climbing to roughly ₦500 million that same year. The CEO of the Nigerian Communications Commission also disclosed during the 2017 Annual General Conference of the Nigerian Bar Association that the country ranks third in electronic crime globally, surpassed only by the UK and the US, while 91.6 million Nigerian residents have access to the internet.”

Educational institutions are not left out. Students in a Federal University in Nigeria identified phishing, data theft, BVN scam and stalking as the most prominent cybercrimes known to them (Omodunbi, Odiase, Olaniyan and Esan, 2016).

Combating cybercrime requires a framework, legislation that would keep pace with cyber trends, personnel, capacity building, institutional cooperation and coordination of cyber security efforts (NCC, 2015). Awe(2013) on his own part added the need for awareness and cultural reformation of people, need for legal framework, and penalties for actors of cybercrime, and security measures (technical and non-technical) within an institution to fight cybercrime.

In a study carried out by Aransinola & Asindemade (2011) to find out the strategies used for cybercrimes, the following were observed: (1) higher institutions of learning in Nigeria serve as the breeding grounds for cybercriminals. This is in line with the findings of earlier scholars; (2) identification of cybercriminals may be easy in face-to-face interactions because of their sub-cultures and language that could be easily recognized. When the interaction is online, it becomes difficult for potential victims to identify the cybercriminals; (3) the skills employed in cybercrime is demanding and challenging. The perpetrators, therefore, network both locally and internationally; and (4) the law enforcement agents in Nigeria need reorganization. It is no longer strange to hear that security agents aid and abet criminal activities. This work shows that tertiary institutions are not immune from cybercrimes or their actors. It also indicates the need for a special unit to handle cyber security issues, training and cooperation among cyber protection units.

Okeshola & Adeta (2013) in their own work focused on tertiary institutions in Zaria, Kaduna State in Nigeria reported the following: (1) cyber cafés and homes were the places cybercrimes were likely to occur; (2) password hackers and key loggers were the most used tools; (3) hacking, credit card fraud and software piracy were the most common cyber crimes in Zaria; and (4) cyber criminals are mostly male and under 30 years old. This information is not shared amongst the institution thus there is no coordinated effort to combat cyber criminals.

A cyber security framework is expected to provide five functions: identify, protect, detect, respond and recover from incidents. Examples of cyber security frameworks include CIS Critical Security Controls; NIST cyber security framework and ISO 27000 information security management framework. The National Institute of Standards and Technology (NIST) provides a best practice framework that has been translated into many languages and adopted outside the United States of America.

PROPOSED METHODOLOGY

The quasi-experimental approach will be used to carry out this research. The target population is all Nigerians who use computers and computer network resources. The sample for this research will be tertiary institutions in Oyo State because they are frequent users of computers and computer resources. Data will be collected using log files from the developed electronic platform and questionnaire at workshops. Analysis will be carried out using simple statistical inferences. A report of the research work and results will be written and submitted. A cyber security framework for tertiary institutions will be developed from existing frameworks. The framework will be presented at a 3-day workshop comprising of pre-selected security officers, management, academics, university community and information technology professionals. Amendments and exclusions to the framework will be invited.

A platform will be created for users, resources and solutions among participating institutions. The platform will be developed to provide information, receive complaints & incidents, archive security threats and solutions, offer open source tools and report security activities of the cyber security units. The platform will utilise appropriate cataloging systems for easy archival and retrieval. Selected staff of the tertiary institutions interested will be trained to provide cyber security services. The cyber protection services will be advertised and performance measured using appropriate metrics. Cyber protection units will be created at interested tertiary institutions and allowed to operate for six months. A survey will be conducted within the community to determine awareness, effectiveness and impact of the cyber protection unit. The admissibility of evidence gathered, implementation of technical activities and resolution of disputes will be investigated using the Nigerian Cybercrime Act of 2015.

Feedback from the platform and survey will inform training requirements for next workshop. A refresher training workshop will be held for all participating cyber protection units.

A performance review based on metrics such as time to resolve incidents and number of incidents, will be used to determine the impact of the cyber security unit to users, and the tertiary institutions.

REQUIRED INSTITUTIONS AND PERSONNEL

The research work will involve the management, staff, students and guests of tertiary institutions in Oyo State, Internet Service Providers for the institutions, and other relevant units in the institutions.

The research team is made up of the following:

- Dr O. Osunade (OO) – Reader / Principal Investigator
- Dr Funmilola O. Omotayo (FOO) - Lecturer I
- Deborah D. Adeyemo (DDA) – Lecturer II
- O. A. Awujoola (OAA) – Assistant Lecturer
- Sunday Oyebamiji (SO) – Senior Systems Analyst
- Babatunde Seyi Olanrewaju – CSC Postgraduate student
- Omowamiwa Taiwo Olanrewaju – CSC Postgraduate student
- Victoria Bola Fadeyi- LARIS Postgraduate student
- Funmilola Kolajo – LARIS Postgraduate student
- Oreoluwa Fisayo – ARCIS Postgraduate student
- Adekunle Olasubomi Adetutu - ARCIS Postgraduate student

BIO-SKETCH OF INVESTIGATORS

a. Dr Oluwaseyitanfunmi Osunade is a Reader in the Department of Computer Science, University of Ibadan, Nigeria. He joined UI in October, 2000 as Assistant Lecturer. His research interests include data communications, leadership, mobile computing and educational technology. He participated in several trainings organized by the Postgraduate School, UI during his doctoral program. He is a recipient of the Commonwealth Science Travel Grant (2001), Educational Research Network for West Africa and Central Africa (ERNWACA) Small Grants Program (2002), Senate Research Grant (2006), Educational Research Network for West Africa and Central Africa (ERNWACA) Travel Grant (2009) and TETFUND Institution-based Research Grant. He has over 40 publications in local and international journals. He will be the Principal Investigator on this multidisciplinary research.

b. Dr. Funmilola O. Omotayo is a Lecturer I at the Africa Regional Centre for Information Science. She is currently the Sub-Dean (Postgraduate) of the Centre. She joined UI in 2012 as Lecturer II. Her research interests include information policy, information behaviour, social informatics, knowledge management and information marketing. She is a recipient of the Junior Academic Staff Exchange component of the John D. and Catherine T. MacArthur Foundation Project for the Institutional Strengthening. She has published many papers in both local and international journals.

c. Deborah D. Adeyemo is a lecturer in the Department of Public Law at the Faculty of Law, University of Ibadan, Nigeria. She holds a LLB from Obafemi Awolowo and an LLM in Transnational Criminal Justice and Crime Prevention. Deborah is a barrister and solicitor of the Supreme Court of Nigeria and a DAAD scholar of the German Academic Exchange Service. Her primary research interests focus on criminal justice and crime prevention. Her current research interests and publications are in the fields of anti-corruption law and international criminal law. She will handle the legal aspects of the multidisciplinary research.

d. Olalekan Abiola Awujoola is a First Class graduate of the Department of Library, Archival and Information Studies, University of Ibadan. He is currently an Assistant Lecturer and a PhD candidate in the same Department. Awujoola research interest includes crimes and deviant act among library users, emerging technologies and library service provision among others. Awujoola is currently working on collaboration and consortium building among libraries in Nigeria with special consideration on the institutional, legal and ethical factors that foster such collaborations. O. A. Awujoola has published many scholarly articles in both local and international academic journals and a book published by the Lambert Publishing Company in London. He will be investigating the design issues and data storage parameters for the website/platform.

e. Sunday Oyebamiji is a senior system analyst in the Department of Library, Archival and Information Studies (LARIS) University of Ibadan, with a passion for networking and software analysis. He earned a Bachelor's degree in Computer Science, and a Master's degree in view from the University of Ibadan. He joined University of Ibadan in2009 as a system analyst. He is responsible for the management of library software and other electronic products in the library school. He has attended various Internet and Network security Workshops organised in local and international level.

PROJECT IMLEMENTATION PLAN

The research work will take about fifteen (15) months to complete.

	Activity	**Duration**
1.	Framework Workshop 1	1 week
2.	Survey (Pre-intervention)	2 weeks
3.	Online Platform development	2 months
4.	Online Platform hosting	1 week
5.	Memorabilia production	1 month
6.	Training Workshop 2	1 week
7.	Intervention implementation	9 months
8.	Survey (Post-intervention)	2 weeks
9.	Workshop 3	1 week
10.	Data Analysis	2 weeks
11.	Report Writing	1 month
12.	Research Dissemination	1 week

A Gantt chart showing activities and milestones is included as an Appendix.

EXPECTED RESULTS AND IMPACT

This multidisciplinary research work will produce the following:

1. A framework for handling cyber security issues in tertiary institutions and in Nigeria
2. The tools necessary to combat cybercrimes and prevent cybercrime
3. A cyber protection unit within tertiary institutions to combat cybercrime
4. Awareness of a resolution centre for all information and cyber security incidents
5. Trained cyber security personnel to handle security threats and cybercrime
6. Enforcement of service level agreements (SLAs) that tertiary institutions have with their service providers
7. A shared incident platform that allows cyber security personnel of any "trusted" cyber protection unit to have access to incident data, solutions and tools to assist in the war against corruption
8. A shared platform that serves to document cyber security incidents that can be used to create reports for management
9. Reduction in cybercrime activities
10. The outcome of this research will have its special significance in solving various information security related problems of higher institutions, financial institutions, government agencies, the business community and individuals alike.

MONITORING AND EVALUATION PLAN

The following activities will be done to monitor and evaluate the multidisciplinary research:

1. A regular monthly meeting will be held to provide updates and discuss challenges amongst the researchers
2. The project milestones will be used to compare with actual progress
3. Electronic communication (phone call, e-mail, Text messages, WhatsApp) will be used for collaboration and updates from individuals and groups when assigned tasks
4. All financial transactions will be documented
5. Log files from the platform and responses from the survey will be used to determine the progress of the research

DETAILED BUDGET

Table 1 gives a detailed budget for the multidisciplinary research.

Table 1: Detailed Budget

S/N	**Item description**	**Quantity**	**Rate (₦ : K)**	**Amount (₦ : K)**
1.	Office supplies e.g. - paper - toner - External Storage - Antivirus – multiuser - Alternative energy	 5 boxes 5 1 1 100 litres	 7,000.00 10,000.00 15,000.00 9,000.00 145.00	 35,000.00 50,000.00 15,000.00 9,000.00 14,500.00
2.	Workshop – venue, food, logistics, instructors, training package	3	500,000.00	1,500,000.00
3.	Memorabilia for participants e.g. t-shirts,	100	2,500.00	250,000.00
4.	Platform Development	1	200,000.00	200,000.00
5.	Platform hosting	2 years	50,000.00	100,000.00
6.	Survey	lot	200,000.00	200,000.00
7.	Data Analysis	lot	100,000.00	100,000.00
8.	Report Writing	lot	50,000.00	50,000.00
9.	Research Dissemination	4	200,000.00	800,000.00
10.	Honourarium – 12 months - Research Assistants - Researchers	 6 4	 120,000.00 200,000.00	 720,000.00 800,000.00
11.	Local transportation and communications	lot	100,000.00	100,000.00
	TOTAL			**4,943,500.00**

The total amount required for the research is four million nine hundred forty-three thousand and five hundred naira only (₦4,943,500.00) without administrative and tax charges.

BUDGET JUSTIFICATION

Office Supplies: This includes use of paper for documentation, article reproduction and memo writing. Toner for use with a laser printer is included. The cost of protection from virus attacks from the Internet and local disk access is included. Cost of provision for alternative energy when electricity is unavailable is listed.

Workshop: Three workshops will be carried out to (1) develop a framework and operational guide for the cyber security unit; (2) train the personnel to handle security incidents; and (3) advanced security training.

Memorabilia for participants: an iconic item such as t-shirt will be produced for the participants. About a hundred participants are expected.

Platform development: The storage and archival of all security incidents from participating institutions is developed using appropriate cataloging systems. Collaboration, privacy and sharing tools are integrated into the platform. The necessary security mechanisms are built into the platform.

Platform hosting: The security platform will need to be made accessible through the Internet. A two year hosting period is proposed. Additional services such as search engine optimization (SEO) and secured connection will increase the cost of hosting.

Survey: The research team will obtain information from the community to determine the impact of the cyber protection unit. A pre-intervention and post-intervention survey will be conducted. The cost is for questionnaire development, testing and reproduction.

Data Analysis: The data entry, statistical manipulations and interpretations by data analyst will be covered by this cost.

Research Dissemination: The findings from the research work will be presented at local and international conferences by members of the research team. The amount is expected to cover registration, accommodation, feeding and transportation for the duration. Seminars will also be organized locally at UI for knowledge sharing.

Local transportation and Communications: This will cover all costs related to logistics such as fuel for vehicles during local travels, credit for phone calls and so on.

Report Writing: The final report for the project will be submitted for editorial review before submission to the Postgraduate College, UI.

Personnel Cost: This is made up of the honourarium to the six (6) Research Assistants who are postgraduate students and the researchers. The honourarium is to enable them carry out research ideas emanating from the multidisciplinary work. The cost is for the project duration.

SUSTAINABILITY PLAN

The project will continue to provide cyber security services to tertiary institutions through the following activities

1. Fund request through grants and awards
2. Platform hosting by a tertiary institution
3. Intellectual property protection using appropriate mechanisms
4. Adoption of Open Source Software tools for security activities and operations
5. On-going training of security personnel through webinars, how-to videos, blogs and
6. Quarterly face-to-face meeting of cyber security personnel
7. Production of an electronic newsletter to document activities of the cyber security unit
8. Commercialization of cyber-security training to non-educational institutions
9. Collaborating with commercial enterprises on the use of the platform built
10. Scaling up the solution to include all organizations in the south west Nigeria and other geo-political zones in Nigeria
11. Providing cyber-security services to organizations

CONCLUSION

Crime can be detected, investigated and prevented when electronic resources are used to carry out the act. The domestication of a cyber security framework for Nigeria and specifically for tertiary institutions will provide the much needed guidance for combating cybercrime. The cyber protection unit, personnel training, website and open source software will ensure that the manpower and resources to always prevent crime through electronic devices such as computers and computer networks are available and sustainable.

REFERENCES

1. Okoye, R. 2012. Nigeria has lost $400bn oil revenue to corruption since Independence . Daily Post Nigeria. Retrieved 2 January 2019 from http://dailypost.ng/2012/08/31/nigeria-lost-400bn-oil-revenue-corruption-since-independence

2. Awe, J. 2013. Fighting cybercrime in Nigeria. http://www.jidaw.com/itsolutions/security3.html

3. Wild, J. 2018. Five Most Common Security Frameworks Explained. Accessed on 6 January 2019 from https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/

4. DiGiacomo, J. 2017. Cybercrime Now a Bigger Worry Than Physical Crime. Accessed on 6 January 2019 from https://revisionlegal.com/cyber-security/cybercrime-threats/

5. Omodunbi, B. A.; Odiase, P. O.; Olaniyan, O. M. and Esan, A. O. 2016. Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology. vol. 1. 37-42.

7. Nigerian Communications Commission (NCC). 2015. A Summary of The Legislation On Cybercrime in Nigeria. Published by Legislative & Government Relations Unit, Public Affairs Department, Issue #14 - Quarter 3 2015. Accessed on 6 January 2019 from https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria&option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria

8. Punch. 2018. Central Bank of Nigeria issues guidelines to combat rising financial cybercrime. Accessed on 6 January 2019 from https://punchng.com/central-bank-of-nigeria-issues-guidelines-to-combat-rising-financial-cybercrime/

9. Aransiola, J. O. and Asindemade, S. O. 2011. Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. CyberPsychology, Behavior, and Social Networking, 14(12):1-5, DOI: 10.1089/cyber.2010.0307

10. Okeshola, F. B. And Adeta, A. K. 2013. The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research 3(9):98-114

APPENDICES

I – Gantt Chart

II- Curriculum Vitae of Researchers