Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Akinyokun, O. K., Alese, B. K., Oluwadare, S. A., Iyare, O., & Iwasokun, G. B. (2015). Contributory indices to cybercrime activities in Nigeria. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015*, 59-77. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p059-077Akinyokun1556.pdf

Contributory Indices to Cybercrime Activities in Nigeria

O. K. Akinyokun, B. K. Alese, S. A. Oluwadare, O. Iyare, and G. B. Iwasokun
Department of Computer Science, Federal University of Technology, Akure, Nigeria.

akinyokunoluyomi@yahoo.com, bkalese@futa.edu.ng, saoluwadare@futa.edu.ng, oiyare@futa.edu.ng, gbiwasokun@futa.edu.ng

Abstract

The arrival of Internet has turned the world into a global village where geographical location or distance has to some extent ceased to be a major obstacle to communication and movement of goods and services. This development has also brought with it cybercrime and its level of sophistication. A lot of measures and institutions are being put in place to minimize the incidence of cybercrime in different countries; also, efforts are being made to identify the contributing factors to cybercrime. This research however, adopts a factor analytic approach to formulate the indices that may contribute to the perpetration of cybercrime. A total of seventy three (73) indices were formulated and used to design a structured questionnaire which was administered on five classes of respondents, using purposive and simple random sampling techniques. The data obtained were analyzed by means of factor analysis by principal component using Statistical Package for Social Sciences (SPSS). Ten factors were extracted and subjected to orthogonal rotation using promax. The contributing factors identified in this study could assist stakeholders to combat the menace of cybercrime.

Keywords: Cybercrime, factor analysis, contributory indices, security, fraud, criminal

Introduction

The extent of Technology-Enabled crime is always evolving, both as a function of change and as a socio-economic interaction with new technologies. Cybercrime as stated in Longe and Chiemeke (2008) remains difficult to combat as it attempts to hide itself in the face of development. Cybercrime is the use of Information Technology Infrastructure in perpetrating criminal activities including Illegal access, Illegal Interception, System Interference, Data Interference, Misuse of Devices, Fraud and Forgery. These activities which are fast becoming high-profile security issues are described below:

Editor: Eli Cohen

a) Hacking: Malicious/Inquisitive moves to discover information by deception or illegal means.
b) Cracking: Gaining unauthorized access to Computer system to commit a crime, such as digging into the code to make a copy and running a protected program without a password or a valid license string.
c) Piracy: Replication of Protected Software without authorization.
d) Phreaking: Obtaining free telephone calls or having calls charged to a different account through manipulation of a phone system.
e) Phishing: Deployed to pull out confidential information from any organization such as bank or other financial institutions account holders by deceptive means.
f) Cyber Stalking: Harassing selected targets using e-mails and other means.
g) Cyber pornography: Producing and/or distributing pornography with the computer.
h) Cyber grooming: Arousing the emotion of the under-aged through web pages with pornographic contents and video media with the aim of sexually abusing them.
i) Cyber Terrorism: Unlawful attacks or threats of attack by criminals against computers, networks, and the information stored therein to intimidate or coerce government or institution or its people to further the perpetrators ambitions.

Criminal activities of any kind are opposed to progress and development; be it social, economic or educational. Cybercrime could be worse due to the subtlety of its operations and most especially the perceived heavy presence of the youths (the productive age-group) in cybercrime perpetration in Nigeria.

The Internet has enabled new forms of social interaction and activities due to its basic features, like widespread usability and access. It is also a window for leisure activities, with entertaining social and humor-related Usenet groups, receiving much traffic. Social networking websites such as Facebook, Twitter and MySpace, etc, have created new ways to socialize and interact. Users of these sites are able to update information on their respective web-pages, to pursue common interests, and to connect with others.

Nowadays, many Internet fora have sections devoted to games and funny videos. More than 6 million people use blogs or message boards as a means of information communication and/or exchange. The pornography and gambling industries have taken advantages offered by the WWW. The Internet is a major medium of advertising revenue for other websites. Although many governments have attempted to restrict both industries' use of the Internet, this has generally failed to stop their prevalent popularity.

Literature Review

In Aghatise (2006) and Longe and Chiemeke (2008) it was confirmed that Cybercrime increasing at an alarming rate. Nigeria is not left out in the global analysis of cybercrime as electronic fraud (popularly called 419), email scams and other Internet-based fraud originated from there.

The Economic and Financial Crimes Commission (EFCC) former Chairperson; Mrs. Farida Waziri said the horrendous level of corruption has being a threat to Vision 20: 2020 (Waziri, 2009). Cybercrime is one of possible corruptions that can shut the door of progress against the nation. Ajayi (2008) documents that Nigeria, Ghana and South Africa are countries in Africa where Cybercrime is predominant. Cyber Cafés are places where these crimes are carried out and also modems are bought for this purpose.

Apart from the availability and usage of Internet facilities in cyber cafés for scam mails and other fraudulent activities, the growth of fixed wireless services in Nigerian has also aided cybercrimes. Fraudsters pay for Internet connection via fixed wireless lines so as to perpetrate their evil acts within the comfort of their homes. In some cyber cafes, a number of systems/cables

are dedicated to cyber criminals (called "yahoo boys") while others share their bandwidth (popularly referred to as home use) to some categories of customers who acquire systems for home use in order to perpetrate their nefarious activities.

Efforts at preventing financial Cybercrime in Nigeria are on parental, entrepreneurial, private and public pedestals. For café operators, information on possible arrests of fraudsters who send scam mails is circulated. Generally, users are advised not to open or respond to scam mails or mails presenting financial bogus proposals. For the government, the Economic and Financial Crimes Commission (EFCC) and other relevant agencies have been given power to arrest and prosecute individuals, group of individuals and organizations suspected to be involved in promoting cybercrimes. Little work has been done in identifying the contributory indices to cybercrimes in Nigeria. This research is therefore aimed at formulating the indices that may contribute to the perpetration.

The computer plays three (3) major roles in Cybercrime activities; (Akinyokun, 1999; Clough, 2010). They are:

a) Computer as the Weapon: Here Computer is been used as the tool to perpetrate attack. e.g. pornography, Stalking, Copyright infringement and fraud.
b) Computer as a Target: Here the intended attack is on the Computer or Computer Network. e.g. Hacking, Malware and DoS attack.
c) Computer as an Accessory: Here the Computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. e.g. Phone number/address of victim found in the Computer of an offender or phone records of conversations between a victim and an offender before a homicide.

Cybercrime in Nigeria

Most Cybercrimes perpetrated in Nigeria are generally ingenuous as they are aimed at individuals and not the computer systems; hence they require less technical expertise. Human weaknesses such as greed, gullibility inexperience and probably illiteracy are usually exploited. These crimes are similar to theft and have been in existence for many years even before the advent of the Internet. Notwithstanding, Internet has enabled criminals and their activities to increase the number of their unsuspecting victims and this invariably makes it difficult to track them down (Aghatise, 2006).

The challenge in fighting Cybercrimes today relates to the fact that Cybercrimes have been in existence for only as long as the cyber space exists. This explains the unprepared ness of society and the world in general towards combating them. Numerous crimes are committed daily on the Internet with Nigerians at the forefront of sending fraudulent and bogus financial proposals all over the world.

Out of all categories of fraud identified by (Peter and Grace, 2001) are fraud committed against a number of individuals through print or electronic media, or by other means. The following categories of crime are the predominate ones in Nigeria:

*SPAMMING***:** Spamming is the act of sending unsolicited messages to a large number of recipients at a time with the aim of advertising products to potential and unsuspected customers. Spamming can also be used as a form of frustration by singling out an email address and sending numerous emails per second to that address. Spamming is usually random and untargeted but it can be targeted to either a group of people, for example, advertisements that cater for a particular group of people, or certain persons for the purpose of irritating the public.

Contrary to popular belief, spamming has existed in Nigeria even before the advent of the Internet. It's gathered that in the Nigeria Postal Service (NIPOST), Mail Security staff were asked to

make sure that letters sent by some individuals be destroyed upon investigation. Junk mails to postal addresses and annoying door-to-door salesmen are some examples of traditional form of spam. However, the Internet has given spam a much ugly face as what used to be a minor irritation has now become a veritable menace.

PIRACY: Piracy involves the illegal reproduction and distribution of software applications, games, movies and audio CDs. (Longe, 2004). Usually pirates buy an original version of a software, movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner.

Modern day piracy may be less dramatic or exciting but is far subtle and more extensive in terms of the monetary losses the victim faces. This particular form of Cybercrime may be the most difficult to curb as the common man also seems to be benefiting from the crime. A typical African would stop at nothing to download free software, musicals, movies or related items. The reason is that, the taxation system in most African countries is ineffective and people grow up to believe paying tax and other bills are ways in which the government oppresses the poor citizens.

Model Formulation

The contributory indices to cybercrime was formulated and questionnaires were administered to selected institutions of higher learning, cyber cafés, offices of the Nigeria Police, offices of the Nigeria Security and Civil Defense Corps, Law chambers, Law courts, and a handful of others within the selected scenery. Here, confidentiality of information (personal or non-personal) was guaranteed because respondents were required to specify their age, gender and occupation. They were encouraged to provide honest answers while items in the questionnaire involving some Internet technicalities were spelt out in clear terms so that the respondents can understanding each question.

Critical inducement of cyber crime

Most often nontechnical factors play major roles as key contributors to cybercrime. The following parameters are essential to evaluating and assessing the Critical Inducement of Cyber Crime:

> (a) Employment Rate, (b) Standard of Living, (c) Home Background, (d) Research and Development, (e) Inflation, (f) Peer- Pressure.

Educational Background of Cyber Criminals

In committing cybercrime certain technical knowledge must be acquired; therefore, using cybercriminal cases, the perceived cybercriminal education background also plays a vital role considering the following:

> (a) Conventional Literacy, (b) Computer Literacy

National Policy/legislative Framework on Cyber Crime

The weight of the consequences of each crime backed by law pay an important role in debarring such crime in the society. Thus, National Policy/legislative Framework on Cyber Crime is assessed under the following parameters: (a) National Policy on Conventional Security, (b) National Policy on Cyber Crime, (c) Legislature's Framework on Cyber Crime, (d) Regulatory Framework on Cyber Crime, (e) Institutional Framework on Cyber Crime.

National security background

The state of National Security in Nigeria plays a vital role in the survival or otherwise of cybercrime in Nigeria. This is assessed under: (a) Implementation of Conventional Security, (b) ICT Based Security System, (c) Implementation of Cyber Security Policy, (d) Case Filling and Database System, (e) Technical Assistance to Private and Government Agencies, (f) Prosecution of Cyber Criminals.

Security personnel

Security personnel are the machinery used by the government to achieve stated objectives in combating crime. They therefore play immense role and are assessed under: (a) I.T. Literacy, (b) Availability of I.T. Facility, (c) Capacity Building/Staff Development, (d) Research and Development, (e) Procurement/Recruitment and Upgrade, (f) Mobility, (g) Salaries and wages, (h) Rapid Response to Cyber Emergency, (i) Case filling and Database System, (j) Prosecution of Cyber Criminals

Security agencies

The state of the security outfits is assessed under the following parameters: (a) Enabling Law, (b) Trained and Experienced I.T. Personnel, (c) Collaboration between Agencies, (d) Administrative Function, (e) Technical Function, (f) Sustainability/Management, (g) IT Facilities, (h) Research and Development, (i) Case filling and Database System, (j) Response to Cyber Emergency, (k) Cyber Security Awareness and Publicity, (l) Prosecution of Cyber Criminals, (m) Availability of Independent/Private Cyber Security organization

Motive for cyber crime

The probable motive for cybercrime was formulated and assessed with a view to deducing likely aim of committing such crime and this is carried out using the following parameters: (a) Greed/Wealth, (b) Recreation (Notoriety), (c) Vendetta/Revenge, (d) Research and Development, (e) Espionage/Spying, (f) Terrorism (Cyber Terrorism).

Data Survey Method

In view of the large number of local governments, states, cyber cafés, institution of higher learning, law firms, etc, and the limited time for this research, the scenery shown in Table 1 were selected for the study:

Table 1: States and Scenery chosen for Study

State	Scenery
Akwa Ibom	1. University of Uyo, Uyo
Delta	1. Delta State University Abraka 2. Delta State Polytechnic, Agbor
Edo	Benson Idahosa University, Ugbor, Benin City Edo State University, Ekpoma Federal Polytechnic, Auchi Igbinedion University Okada University of Benin, Benin City
Ekiti	College of Education, Ikere University of Ado,

Kogi	Federal Polytechnic, Ida Kogi State University, Ayangba
Lagos	Lagos State University, Ojo Campus University of Lagos, Akoka
Nassarawa,	1. Federal Polytechnic, Nassarawa
Ogun	1. Babcock University, Ilishan Remo 2. Olabisi Onabanjo University, Ago Iwoye Campus 3. Olabisi Onabanjo University, Ikenne Campus
Ondo	1. Adekunle Ajasin University, Akungba 2. Adeyemi College of Education, Ikere 3. Federal University of Technology, Akure 4. FM-CMOS Communications, Oke Ijebu, Akure 5. BetaNet Cyber Café, Adesida Rd., Akure 6. HTRDG COMPUTERS LTD., Alewi Str. Akure 7. Customary Court of Appeal, Oke Eda, Akure 8. Ondo State Judiciary, Oke Eda, Akure 9. Ondo State High Court, NEPA Akure 10. Imafidon & Imafidon, Investment House, Akure 11. OLUDURO, ASANI & Co, NEPA Akure 12. Nigeria Police, Oke Aro Division, Akure 13. Nigeria Security and Civil Defence Corps, Alagbaka, Akure
Oyo	1. The Polytechnic Ibadan 2. A.T Communications, Ibadan
F.C.T	1. University of Abuja

In the sampling instrument, the contributory indices to cybercrime were identified. Five classes of respondents was used in the sampling instrument, they include:

a) Staff and Students of Institutions of Higher learning,
b) Staff and Clients of IT firms,
c) Staff and Clients of Law firms,
d) Legal Practitioners & administrative Staffs of Law Courts and
e) Security Personnel

The transcript of the questionnaires was made adaptive for the five classes of respondents which is presented in Appendices A. In each Location, questionnaires meant for each respondent were administered on a minimum of one per respondent. The questionnaires require the respondents to rate each of the indices associated with him or her using a 5-point Likert Scale of 'excellent', 'very good', 'good', 'average' and 'poor'. Altogether, One hundred and two respondents returned completed questionnaires. The responses were verified and validated by a follow up through personal interviews and discussions with the principal actors. It is remarked that in each of the questionnaires, there were leading quantitative variables such as name of organization, address, local government, age and maximum academic qualification of respondent. The leading quantitative variables are meant to serve as parameters for measuring the sense of judgment of the respondents.

Mathematical Model of Surveyed Data

The data obtained through survey was analyzed using PCA as proposed and implemented in (Akinyokun and Chiemeke, 2004) can be expressed as shown in equation 1.

$$Y_j = \sum_{k=1}^{m} a_{j,k} X_k \quad K = 1,2,3 \ldots M \qquad (1)$$

where Y_j represents the j^{th} respondent, $a_{j,k}$ represents the assessment of the k^{th} variable by j^{th} respondent and X_k represents the k^{th} decision variable. The model is expressed as:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_M \end{pmatrix} = \begin{pmatrix} a_{1,1}X_1 + a_{1,2}X_2 + a_{1,3}X_3 + a_{1,4}X_4 + & \cdots & +a_{1,m}X_m \\ \vdots & \ddots & \vdots \\ a_{n,1}X_1 + a_{n,2}X_2 + a_{n,3}X_3 + a_{n,4}X_4 + & \cdots & +a_{n,m}X_m \end{pmatrix} \qquad (2)$$

The primary objective of factor analysis by PCA is to generate some clusters of contributory indices to cybercrime in Nigeria. Each cluster shall constitute a factor with which cybercrime indicators can be measured. The percentage contribution of each factor to the cybercrime can equally be obtained. The following statistics are derived and used for the purpose of achieving these objectives.

Descriptive Statistics, Correlation Matrix, Component Matrix, Eigenvalue, Communalities, Initial factor loadings, Rotating factor loadings by orthogonal transformation by:

(i) Varimax
(ii) Equamax
(iii) Quartimax
(iv) Promax

The descriptive statistics define the mean and standard deviation of the scores of each decision variable given by the respondents. The correlation matrix shows the degree of pair-wise relationships of cybercrime decision variables. A positive value in the correlation shows a positive relationship while a negative value dictates a negative relationship. Zero value means there is no relationship between variables. In factor analysis, there is a set of factors which is generally referred to as "common factors", each of which loads on some variables. There is another set of factors, which are extraneous to each of the variables. The proportion of the variance of a variable explained by the common factor is called the "communality" of the variable.

The factor loading associated with a specific decision variable is the correlations between the factor and the variable's standard scores. Each factor represents an area of generalization that is qualitatively distinct from that represented by another factor. The degree of generalization found between each variable and each factor is referred to as "factor loading". The farther a loading is from zero in the positive direction, the more we can conclude the contribution of a variable to a factor. The component matrix can be rotated by varimax, equamax, quartimax or promax for the purpose of establishing a high correlation between variables and factors. While the component score matrix of the factors is generated to evaluate the contributions of each of the decision variables to cybercrime, the eigenvalue and percentage variance of the extracted factors are generated for evaluating the contribution of each factor to cybercrime.

The surveyed data were subjected to factor analysis by principal component using SPSS version 15.0 on an IBM compatible microcomputer with Microsoft Windows Operating System as platform.

Evaluation of Assessment

The mean and standard deviation of the rating of Cybercrime on each of the contributory indices by the respondent were determined. The SPSS generates the correlation matrix as a single shown in Appendices B. The analysis of the correlation matrix shows that the highest correlation of 0.593 exists between 'employment rate' and 'standard of living'. The next highest correlation of 0.565 exists between 'societal counter measures of cybercrime' and 're-active (Curative) measures'. The implication of the highest correlation is that 'employment rate' and 'standard of living' is very likely to share same factor. Similarly, 'societal counter measures of cybercrime' is very likely to share same factor with 're-active (curative) measures'. The least correlation of -0.002 exists between 'technical assistance to private and government agencies' and 'computer literacy', this means they are not likely to share same factor.

The Barlett's test produces an X^2 of 4255.827 with a significant level of 0.000, which indicates the adequacy of the sample population. The Keiser-Meyer Olkin (KMO) test produces a measure of 0.578, which also confirms the adequacy of the sample population. The results obtained from the Barlett's test and KMO test are good indicators of the suitability of the application of factor analysis as well. In factor analysis, there is a set of factors which is generally referred to as "common factors", each of which loads on some variables. There is another set of factors, which are extraneous to each of the variables. The proportion of the variance of a variable explained by the common factor is called the "communality" of the variable. The communalities of 'employment' and 'Standard of Living' were determined as 0.824 and 0.811 respectively. These imply that 82.40% of the variance in 'employment' can be explained by the extracted factors while the remaining 17.60% is attributed to extraneous factors. Similarly, 81.10% of the variance in 'Standard of Living' can be explained by the extracted factors, while the remaining 18.90% is attributed to extraneous factors.

Table 2: KMO and Bartlett's Test

	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	.578
Bartlett's Test of Sphericity	Approx. Chi-Square	4255.827
	Df	2211
	Sig.	.000

The initial factor extractions are achieved by two different approaches for replication purpose, namely: mineigencriteruim and noriterium. In critereuim, default was used in determining the number of factors to be retained while in the case ncriterium, the numbers of factors to be retained are specified on the basis of a Social Science rule which states that only the variables with loadings equal to or greater than absolute 0.4 should be considered meaningful and extracted for factor analysis. Applying the Social Science rule on the initial component matrix generated, the extracted factor loadings where: ten factors were extracted, twenty variables did not load on factor 1, eight, five, two, four, three, two, two, and one decision variables load on factors two, three, four, five, six, seven, eight and nine respectively; and,one decision variable load on factor 10.

In order to obtain meaningful representation of variables and factor mapping along principal axis, the resulted principal component is rotated by orthogonal transformation by varimax, quartimax, equamax and promax.

It is observed that promax produces the best meaningful factor loadings.

In an attempt to evaluate the percentage contribution of each factor to Cybercrime, eigenvalue of each factor is generated. The eigenvalue represents the sum of squares of factor loadings used to indicate how well each of the identified factors fits the data from the sample. The percentage contribution denoted by CF of each factor to cybercrime is defined by:

CF = 100(eigenvalue of factor)/(number of decision variables).

Table 3 represents the eigenvalue percentage contributions and cumulative percentage contribution of the extracted ten factors. The ten factors contribute 55.55% to Cybercrime perpetration according to the view of the respondent. The remaining 44.45% is taken to be the contribution of the extraneous factors.

Table 3: Total Variance Explained

Component	Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %
1	13.960	20.836	20.836
2	4.296	6.413	27.249
3	3.230	4.821	32.070
4	2.726	4.069	36.139
5	2.585	3.859	39.998
6	2.472	3.690	43.687
7	2.185	3.261	46.948
8	2.048	3.057	50.005
9	1.876	2.800	52.806
10	1.838	2.744	55.549

Conclusion

Cybercrime as overtime added its quota to the diminishing positive perception of Nigerians by the international community. This has become a menace as it is gradually denting the image of Nigeria in the cyber space. Likewise the integrity of a Nigerian presuming to purchase or market a product on the net is not guaranteed. Depressing still is the mass exodus of the minors into cybercrime and the seemingly acceptance by society as a means of survival due to the stimulating turnover by the perpetrators. Cybercrime is consciously or unconsciously reducing our socio-economic status and marketability to the global world. Thus, the need for the study of cybercrime ("cyber-criminology") and the prompt implementation of the preventive or curative measures if socio-economic advancement and global receipt is anticipated.

The contributory indices to cybercrime were studied and twelve categories of assessment were identified – This formed the basis of seventy three indices. These were assessed by administering questionnaires to the stake holders selected for the research. Factor analysis by principal components of the surveyed data was carried out.

Of the entire assessment, ten factors were extracted and found to contribute 55.55% to Cybercrime in Nigeria. The remaining 44.45% is the contribution of the extraneous factors.

References

Aghatise, E. J. (2006). *Cybercrime definition*. Computer Crime Research Centre. Retrieved June 28 from www.crime-research.org

Ajao, O. D. (2008). *Nigeria, South Africa, Ghana top cybercrime in Africa*. Retrieved from www.davidajao.com

Akinyokun, O. C. (1997). Catching and using the virus. *The Journal of the Institute for the Management of Information System (IMIS)*, *7*(6), 12 -17.

Clough, J. (2010). *Principles of cybercrime*. New York: Cambridge University Press.

Longe, O. B. (2004). Web journalism in Nigeria: New paradigms, new challenges. *Journal of Society and Social Policy*. Calabar, Nigeria.

Longe, O. B., & Chiemeke, S.C. (2008). Cybercrime and criminality in Nigeria - What roles are internet access points playing? *European Journal of Social Sciences,6*(4).

Grabosky, P. N., & Duffield, G. M. (2001). *Red flags of fraud*. Australian Institute of Criminology, Canberra. Retrieved from http://www.aic.gov.au

Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). Nigerian advance fee fraud. *Trends and Issues in Crime and Criminal Justice*, No. 121'.Australian Institute of Criminology, Canberra. Retrieved from http://www.aic.gov.au

Waziri, F. (2009). Anyaoku: Antigraft campaign: The war, the worries. *The Punch*, 1st March 2009, Pg.1.

Appendix A

Questionnaire on Contributory Indices of Cyber Crime in the Scenery of Nigeria

The purpose of this Questionnaire is to evaluate the Causative Factors and Implications of Cyber Crime in the Nigerian with a view to developing a pro-active cyber solution. The survey is a component of a Masters of Technology (M.TECH.) research work in the Department of Computer Science of The Federal University of Technology, Akure. Nigeria. Confidentiality of personal information is guaranteed. We would therefore appreciate your sincere contributions to the research by giving a very accurate and honest response to this questionnaire.

Part 1: PROFILE OF CONTACT PERSONS

1. AGE

2. SEX

3. MAXIMUM ACADEMIC QUALIFICATION

4. OCCUPATION

5. ORGANIZATION

6. LOCATION (local Government and State)

7. COMPUTER LITERATE? (Pls.Tick (√**)** as appropriate**)**

Yes	
No	

8. UNDERSTANDING OF THE INTERNET (Pls. Tick (√**)** as appropriate**)**

Excellent	
Very Good	
Good	
Average	
Poor	

9. UNDERSTANDING OF CYBER/COMPUTER CRIME (Pls. Tick (√**)** as appropriate**)**

Excellent	
Very Good	
Good	
Average	
Poor	

10. HAVE YOU BEEN A VICTIM OF COMPUTER CRIME (Pls.Tick (√**)** as appropriate**)**

Yes	
No	

11. NUMBER OF OCCURRENCE(S) OF THE ABOVE (Pls. Tick (√**)** as appropriate**)**

1-5	
6-10	
11-15	
16-20	
Above 20	

12. MODE OF (10) ABOVE (Pls. Tick/Write as appropriate**)**

Advance fee fraud ("Yahoo Yahoo")	
Forgery (Fake Office Documents, Certificates, etc.)	
ATM (Money Theft Through ATM)	
Piracy (Pirated Software, Video/Audio CDs, etc.).	
Phreaking (Making Fraudulent free calls)	
Spamming (Unsolicited emails)	
Embezzlement (Executive Theft, Salami Shaving. etc.).	
Computer Virus and/or Denial of Service	
Pornography/Cyber Grooming	
Others(Specify) 1) _	

PART 2: ASSESSMENT OF POSSIBLE CONTRIBUTORY FACTORS TO CYBER CRIME

Pls. Tick/Write as appropriate depending on the level/Intensity of Indices using the scale of:

Excellent, Very Good, Good Average or Poor

Section A: Assessment of Critical Inducement of Cyber Crime

Index	Excellent	Very Good	Good	Average	Poor
Employment Rate					
Standard of Living					
Home Background					
Research and Development					
Inflation					
Peer- Pressure					

Section B: Assessment of Educational Background of Cyber Criminals

Index	Excellent	Very Good	Good	Average	Poor
Conventional Literacy					
Computer Literacy					

Section C: Assessment of National Policy/legislative Framework on Cyber Crime

Index	Excellent	Very Good	Good	Average	Poor
National Policy on Conventional Security					
National Policy on Cyber Crime					
Legislature's Framework on Cyber Crime					
Regulatory Framework on Cyber Crime					
Institutional Framework on Cyber Crime					

Section D: Assessment of National Security Background

Index	Excellent	Very Good	Good	Average	Poor
Implementation of Conventional Security					
ICT Based Security System					
Implementation of Cyber Security Policy					
Case Filling and Database System					
Technical Assistance to Private and Government Agencies					
Prosecution of Cyber Criminals					

Section E: Assessment of Security Personnel

Index	Excellent	Very Good	Good	Average	Poor
IT Literacy					
Availability of IT Facility					
Capacity Building/Staff Development					
Research and Development					
Procurement/Recruitment and Upgrade					
Mobility					
Salaries and wages					
Rapid Response to Cyber Emergency					
Case filling and Database System					
Prosecution of Cyber Criminals					

Section F: Assessment of Security Agencies

Index	Excellent	Very Good	Good	Average	Poor
Enabling Law					
Trained and Experienced IT Personnel					
Collaboration Between Agencies					
Administrative Function					
Technical Function					
Sustainability/Management					
IT Facilities					
Research and Development					
Case filling and Database System					
Response to Cyber Emergency					

Cyber Security Awareness and Publicity					
Prosecution of Cyber Criminals					
Availability of Independent/Private Cyber Security organization					

Section G: Assessment of Public-Private-People Partnership

Index	Excellent	Very Good	Good	Average	Poor
Political will					
Industry Contribution					
Funding of Research on Cyber Security					
Societal Counter Measures of Cyber Crime					
Re-Active (Curative) measures					
Pro-Active (Preventive) Measures					
Public/Private Agency Collaboration					
Purchase of Genuine Software					

Section H: Assessment of Computer Network Vulnerability/ Cyber Security (Hardware)

Index	Excellent	Very Good	Good	Average	Poor
Design					
Hardware Compatibility					
Physical Protection					
Scalability of Hardware Production					

Section I: Assessment of Computer Network Vulnerability/ Cyber Security (Software)

Index	Excellent	Very Good	Good	Average	Poor
Internet Protocol and Routing Security					
Adaptive and Scalable Security Protocol					
Operating System Security Protocol					
Password Security					
Cyber Criminal Tracking Software					
Effective Antivirus Software					
Rapid Growth of the Cyber Space					

Section J: Assessment of Motive for Cyber Crime

Index	Excellent	Very Good	Good	Average	Poor
Greed/Wealth					
Recreation (Notoriety)					
Vendetta/Revenge					
Research and Development					
Espionage/Spying					

Terrorism(Cyber Terrorism)					

Section K: Assessment of Cyber Crime Gender Incidence

Index	Excellent	Very Good	Good	Average	Poor
Male					
Female					

Section L: Assessment of Cyber Crime Age Incidence

Index	Excellent	Very Good	Good	Average	Poor
5-10					
11-22					
23-46					
Above 46					

….. THANK YOU

Appendix B

Correlation Matrix

		EMPRT	STDLG	HOMBG	READE	INFLA	PEERP	CONVL	COMPL	NAPCS	NAPCC	LEFCC	REFCC
Correlation	EMPRT	1.000	.593	.103	.239	.092	.436	.268	.122	.025	.189	.048	.095
	STDLG	.593	1.000	.230	.103	.149	.244	.106	.113	.169	.164	.199	.247
	HOMBG	.103	.230	1.000	.032	.030	-.133	.128	-.101	.083	-.094	.097	-.036
	READE	.239	.103	.032	1.000	.106	.177	.243	.054	.029	.167	.065	.129
	INFLA	.092	.149	.030	.106	1.000	.325	.097	.101	.082	.083	.121	-.092
	PEERP	.436	.244	-.133	.177	.325	1.000	.116	.010	-.053	.168	-.163	-.175
	CONVL	.268	.106	.128	.243	.097	.116	1.000	.122	-.102	.034	.098	.004
	COMPL	.122	.113	-.101	.054	.101	.010	.122	1.000	.086	.094	.108	.259
	NAPCS	.025	.169	.083	.029	.082	-.053	-.102	.086	1.000	.206	.438	.353
	NAPCC	.189	.164	-.094	.167	.083	.168	.034	.094	.206	1.000	.371	.353
	LEFCC	.048	.199	.097	.065	.121	-.163	.098	.108	.438	.371	1.000	.539
	REFCC	.095	.247	-.036	.129	-.092	-.175	.004	.259	.353	.353	.539	1.000

	INFCC	.081	.137	.024	.218	.142	-.003	.170	.044	.274	.367	.451	.456
	IMPCS	-.005	.120	-.072	-.024	.031	-.126	-.036	.137	.365	.103	.314	.329
	ITBSS	-.039	-.010	-.114	.099	-.059	-.073	-.069	-.013	.357	.233	.372	.339
	IMCSP	-.009	.107	.135	-.059	.110	-.132	.028	-.041	.330	.222	.427	.306
	CFDBS	-.055	-.095	.080	-.019	.172	-.071	-.126	.047	.221	.144	.236	.247
	TAPGA	-.004	.059	.236	.083	.282	-.152	.171	-.002	.160	.211	.325	.265
	PRCCS	-.103	.026	-.064	-.042	-.077	-.121	-.176	.151	.124	.014	.077	.249
	ITLIT	.223	.101	.081	.265	.149	.277	.092	.098	.103	.315	.195	.237
	AVITF	-.052	-.040	-.021	.091	.060	-.089	.068	-.095	.136	.223	.229	.292
	CBSDV	-.137	-.064	.048	-.088	.143	-.094	-.049	.049	.249	.227	.214	.195
	SREDE	.016	.048	.025	.197	-.036	-.022	.134	-.063	.040	.237	.199	.227
	PRRUP	-.103	.101	.000	.078	.222	-.055	-.041	.046	.138	.114	.200	.027
	MBLTY	-.068	.057	.196	.042	.116	-.182	-.039	.116	.143	.268	.123	.237
	SALWG	-.058	.000	.100	-.121	-.038	-.180	-.075	-.049	.067	.207	.119	.048
	RRECE	.018	.032	-.015	.040	.109	.066	.048	.167	.233	.231	.350	.311
	PCFDS	-.148	-.122	-.030	.002	-.014	.029	-.164	.039	.240	.221	.189	.227
	PPRCC	.002	.092	.036	.068	.205	.097	-.151	-.093	.063	.071	.061	.129
	ENLAW	-.081	.103	.070	-.052	-.021	-.034	.114	-.024	.094	.352	.346	.275
	TEITP	-.010	.055	-.035	.129	.035	.082	.051	.153	.115	.225	.279	.347
	COLBA	.071	.174	.108	.071	-.061	.041	.099	.138	.173	.219	.376	.371
	ADMNF	-.014	.068	.103	-.006	.085	-.019	.020	.214	.128	.125	.289	.248
	TECHF	.006	.048	-.050	-.005	.073	.074	-.085	.143	.234	.205	.429	.283
	SSMGT	-.084	.021	.010	.006	.002	-.093	-.072	-.059	.215	.106	.320	.148

ITFCT	.144	-.005	.019	.067	.152	.171	-.085	.003	.000	.173	.235	.240
ARDEV	.169	.046	.018	.053	.043	.134	-.005	-.058	-.024	.146	.115	.132
ACFDS	-.026	.043	.174	-.037	.129	.046	-.102	.025	.017	.281	.284	.165
RESCE	.042	.056	-.086	.030	.066	.127	-.049	.157	.123	.205	.150	.299
CSAWP	.139	.037	-.025	-.046	.166	.103	-.052	-.012	.344	.259	.213	.115
APRCC	-.079	-.067	-.078	.017	.078	-.101	-.249	-.024	.155	.044	.109	.191
AIPCSO	-.137	-.078	-.041	-.037	-.049	-.199	-.227	-.066	.174	.082	.204	.158
POLWL	.006	.094	.155	.070	.061	-.071	-.095	-.063	.204	.297	.281	.126
INDCN	.078	.177	-.020	.083	.096	-.004	-.085	-.041	.344	.230	.284	.235
FRECS	.056	.064	.042	-.056	-.042	-.071	-.027	.137	.189	.224	.231	.212
SCMIC	-.112	-.124	-.057	-.036	-.020	-.247	-.186	-.010	.275	.140	.254	.226
REACM	-.035	-.022	-.021	-.019	-.028	-.135	-.042	-.011	.219	.202	.210	.180
PRAPM	.112	.064	-.019	.127	.008	.026	-.023	-.033	.315	.350	.229	.336
PPACL	-.012	.073	.025	.006	.225	.005	-.163	.110	.302	.250	.274	.162
PGSTW	.018	-.028	.012	.068	.185	.106	-.062	.128	.242	.201	.258	.181
DESGN	.081	.151	-.014	.037	.057	.003	-.045	.099	.240	.286	.323	.288
HWCMP	.016	.034	-.057	.086	-.049	-.033	-.028	.113	.287	.262	.128	.158
PHYPR	.074	-.028	.026	-.033	.026	-.100	.150	.006	.224	.165	.227	.043
SCHPR	.037	.055	-.014	-.025	.155	.126	-.039	.066	.271	.159	.191	.043
IPRRS	.065	-.004	.002	-.040	.087	-.118	.213	.243	.074	.231	.193	.205
ASSPR	.141	.053	.048	.144	.005	.012	.246	.158	.225	.312	.191	.143
OSSPR	.180	.172	-.119	.142	.130	.108	.075	.155	.136	.099	.149	.085
PASEC	.272	.055	-.025	.019	.102	.224	.184	.059	.041	.242	-.007	-.011

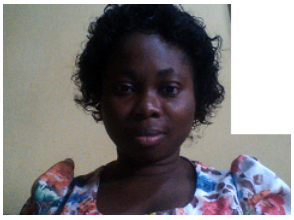
CCTRS	.110	-.135	-.011	.226	.154	-.060	-.115	.032	.061	.249	.128	.014
EFFAS	.085	-.054	-.064	.181	-.118	.091	.168	.041	.085	.321	.240	.285
RGCSP	-.082	-.105	-.015	.022	.015	.052	.085	.091	.211	.243	.197	.092
GRWLT	-.008	.092	.098	-.197	-.050	-.021	-.012	.091	.049	.151	.086	.121
RECRN	.033	.189	.016	.015	.282	.083	.161	.192	-.031	.034	.062	.020
VENDR	.059	-.028	.050	-.215	.057	.041	.108	.214	.314	.271	.253	.113
RESDV	.127	-.016	-.091	.041	.180	.207	-.079	.183	.091	.197	.190	.225
ESPSP	.077	-.077	-.145	-.042	-.078	.241	.035	-.051	.057	.205	.127	.012
TERCT	.201	.003	-.089	.141	.089	.291	.051	.116	.056	.123	.024	-.038

Biographies

Mr O.K Akinyokun is a lecturer in the department of Computer Science, Federal University of Technology, Akure. His areas of research are Information Security and Digital Forensic.

Dr. Alese Boniface Kayode is presently an Associate Professor with the Computer Science Department of the Federal University of Technology Akure, Ondo State, Nigeria. He holds a Ph.D. degree in Computer Science from The Federal University of Technology Akure, Ondo State, Nigeria in 2004. He has several awards of excellence. His areas of research include, Computer and Network Security, Quantum Computing and Digital Signal Processing. He is the current holder of the First Bank Professorial Chair in Computer Science of the Federal University of Technology, Akure, Nigeria.

Dr. S.A Oluwadare is a senior lecturer in the department of Computer Science, Federal University of Technology, Akure. His area of research is Database.



Miss O. Iyare is a lecturer II in the department of Computer Science, Federal University of Technology, Akure. Her areas of research are Computer and network security, softcomputing.

Dr. G.B Iwasokun is a lecturer I in the department of Computer Science, Federal University of Technology, Akure. His area of research is on biometric computing.