International Journal of Science and Technology (STECH)
Bahir Dar- Ethiopia
Vol. 6 (2), S/No14, August, 2017: 53-60
ISSN: 2225-8590 (Print) ISSN 2227-5452 (Online)
DOI: http://dx.doi.org/10.4314/stech.v6i2.4

# Proliferation of Cyber Insecurity in Nigeria: A Root Cause Analysis

**Chigozie-Okwum, Chioma**
Federal College of Land Resources Technology, Owerri
c/o Cees and Zees Integrated Services
No 9 Mbonu Ojike Street, Ikenegbu, Owerri
Phone: +2348038798153
E-mail: chiomaokwum@gmail.com

**Ugboaja, Samuel**
Micheal Okpara University of Agriculture
Umudike, Abia State.

**Micheal, Daniel**
Alvan Ikoku Federal College of Education,
Owerri, Imo State

**Osuo-Genseleke, Macarthy**
ICT Department, Rivers State Secretariat,
Port Harcourt, Rivers State, Nigeria

## Abstract

With increasing access to internet and online resources in Nigeria, an exponential increase is observed in the rate of cybercrimes in Nigeria. Cybercrime rates increase geometrically, hence, giving Nigeria notoriety as a nation with a highly insecure cyberspace, the study aimed at identifying the root cause of the increase in the rate of cyber insecurity in Nigeria. The study adopted a survey methodology in which interview sessions were used for data collection. 50 respondents were purposively sampled. Data collected were analysed using the 5 WHYs method of root causes analysis. The research identified poor promotion of cyber security professionals' recruitment, training, and upgrade in technical knowledge and development in Nigeria; lack of feasibility and workability analysis of the resultant effects of certain policies on the overall economic sector of the nation, sabotage by monitoring and regulation agencies which render the energy sector unfunctional; and sabotage by the elite class for personal gains and poor funding of the security agencies as the root causes of the increase in cyber insecurity in Nigeria. The study further highlighted recurrent prevention strategies to these root causes, such as the establishment of world class cyber security training institutions to train digital forensics investigators, and ethical hackers on global best practice and ways of combating the activities of cyber criminals among other strategies.

**Key Words: cyber security, cybercrimes, root cause, 5whys, proliferation, promotion**

## Introduction

The rapid growth, development and evolution of the internet, including its global acceptance is generating increasing security threats to individuals, corporations, enterprise and the government as a whole. The cyber space creates unlimited opportunities for legal activities in forms of commercial, social, and educational activities. However, the cyberspace has also provided a near-safe haven for societal miscreants to perpetrate their criminal acts.

The term "cybercrime" describes a range of offenses including traditional computer crimes as well as network crimes; it involves a series of organized crimes attacking both the cyber space and cyber security. Carter, (1995) defines cybercrimes as any activity in which computers or networks are a tool, a target or a place of criminal activity. Criminal activities done using computers and the Internet which include anything from downloading illegal music files to stealing millions of dollars from online activities, child pornography, spamming, hacking, espionage among others fall under the category of cybercrimes.

Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Perhaps the most complete definition of Cyber-crime is as given by Laura, (1995) which states that " Cybercrime is a criminal activity involving information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

Ibikunle and Odunayo (2013) submitted that prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet, (Moses-Oke, 2012). Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters (Thompson, 1989).

Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols ethics, information security, digital forensics and ethical hacking. In other to thoroughly investigate a cybercrime, it is important that the investigator is trained and equipped in such a way that he has the expertise, technical knowledge and skills that match and even surpass that of the cybercriminal. Hence the investigator has to have the mind and reasoning similar to that of the cybercriminal in other to understand his method. With cybercrime rates growing at an exponential rate in Nigeria, the study aimed at carrying out an in-depth research with the sole aim of arriving at the root cause of the proliferation of cybercrimes in Nigeria with the aim of proffering solutions.

## Aim and Objectives of the Study

The broad aim of the research is to identify the root cause of the proliferation of cyber insecurity in Nigeria. However, the specific objectives of the study include:

1. to identify the fundamental reason(s) causing the proliferation of cybercrimes in Nigeria.
2. to proffer solution to the identified root cause(es), hence, curbing the menace.

## Research Questions

To further propel the research in the right direction attempt will be made at providing answer to the following research question;

1. Why is there an Increase in the rate of cybercrimes in Nigeria?

2. What are the solutions to help curb the proliferation of cybercrimes in Nigeria?

## Methodology

The research methodology adopted was descriptive research methodology, in which a survey was carried out in South East Region of Nigeria. The survey took us to the five police Area commands within the south-east geopolitical zone namely Abia state area command, Imo state area command Enugu State area command, Ebonyi State Area command and Anambra Area command.

### Population of Study

The population of the study comprises of Police officers within the 'D' Department of the Nigerian police within the South-East zone. The 'D' Department is the Investigation and Intelligence department, comprising of criminal investigation, Interpol, crime prevention policies, narcotics, forensic matters, crime records, prosecution and criminal intelligence.

### Sampling and Sample Size

10 police officers were purposively sampled from each of the five commands visited, giving a total of 50 respondents. Hence sample size is fifty (50).

### Method of Data Collection

Primary data were collected using interview session. The interview sessions were held at 5 of the command headquarters sequentially. The interviews were structured in form of a brainstorming session between the respondents and the researchers.

### Method of Data Analysis

Data analysis was done using the "5 WHYs" method of root causes analysis. In this method of analyzing for the root cause, the first question is asked, a recurrent answer is selected and the answer to the previous question becomes the question for the subsequent level. This method is repeated till the fifth "WHY" is asked. The repetition of the divergent "Whys" asked is aimed at arriving at the root cause.

## Results and Discussions

The tables below show the "5 Why" questions asked by the researchers, the recurrent responses received from the respondents and the inferences drawn from the answers which helped in identification of the root cause of the proliferation of cyber insecurity in Nigeria.

**Table 1: 1st Why**

| Why Question 1 | Recurrent Answer |
|---|---|
| Why is the Nigerian Cyberspace very insecure? | There is a rapid increase in the rate of cybercrimes in Nigeria |

**Source: field data 2016.**

**Table 2: 2nd Why**

| **Why Question 2** | **Recurrent Answer** |
|---|---|
| Why is there a rapid increase in the rate of cybercrimes in Nigeria | 1.Cybercrimes are less risky than other regular crimes<br>2. Cybercrimes are lucrative and more yielding<br>3. There is high rate of unemployment in the country. |

**Source: Field data 2016**

**Table 3: 3rd Why**

| **Why Question 3** | **Recurrent Answer** |
|---|---|
| Why are Cybercrimes less risky than other crimes? | It is very easy for cybercriminals to cover their tracks within the Nigerian Cyberspace. |
| Why are Cybercrimes lucrative? | Cyber criminals always target vulnerable citizens who fall prey so easily. |
| Why is unemployment rate very high in Nigeria? | There are very few job openings in Nigeria now. |

**Source: Field data 2016**

**Table 4: 4th Why**

| **Why Question 4** | **Recurrent Answer** |
|---|---|
| Why is it easy to cover up cybercrimes in Nigeria? | Cybercrimes are not thoroughly investigated and criminals prosecuted and severely punished. |
| Why do citizens fall prey so easily to cyber criminals | The average Nigerian lack the knowledge, method and technique to protect themselves from these cybercriminals. |
| Why are there few job openings in Nigeria | The Nigerian business terrain presently does not encourage and attract new investments while old companies are either downsizing or shutting down completely. |

**Source: Field data 2016**

**Table 5: 5th Why**

| Why Question 5 | Recurrent Answer |
|---|---|
| Why are Cybercrimes not thoroughly investigated and criminals prosecuted? | Nigeria Lacks the required cyber security personnel with the needed technical knowledge, skills and expertise to combat these smart cybercriminals. |
| Why do the citizens lack the required knowledge to protect themselves from cyber criminals? | Nigeria lacks the required cyber security personnel who will create awareness amongst the vulnerable citizens, whilst check mating and protecting them from these malicious criminals |
| Why is the present Nigerian business landscape not attracting new investments nor sustaining older ones? | - Some economic policies of the government are not investor friendly.<br>- Lack of basic infrastructure and support services especially power poses a challenge to investors.<br>- High rate of insecurity in the nation is a factor too inhibiting influx of new investments and security of existing ones. |

**Source: Field data 2016**

**Table 7: Root Cause Versus Recurrent Prevention**

| ROOT CAUSE | RECURRENT PREVENTION |
|---|---|
| Poor promotion of Cyber security personnel's recruitment, training, upgrade in technical knowledge and development in Nigeria today. | Establishment of world class Cyber Security institutions, to train digital forensics investigators and ethical hackers on global best practices in cybercrime investigation, protection, detection, prosecution and conviction. |
| Poor promotion of cyber security personnel's recruitment, training, upgrade in technical knowledge and development in Nigeria. | To train more cyber security personnel who will embark on awareness campaigns to sensitize the citizens on ways of staying safe online the cyberspace and avoid falling prey to cyber criminals. |
| Lack of feasibility and workability analysis of certain policies on the | The nation's economic team should carry through analysis of new policies, comparing |

| | |
|---|---|
| economy before they are implemented. | them with global best practices to avoid implementing economic policies that will trigger a negative ripple effect on the nation and scare investors and job creators away. |
| Sabotage by the monitoring and regulation agencies render the energy sector unfunctional | Overhaul the monitoring agencies to fish out and punish the saboteurs in the energy sector. |
| Sabotage by the elite politicians and poor funding of security agencies lead to insecurity in Nigeria today. | Proper funding of the law enforcement agencies to enable them do their job well and keep the nation Safe, hence attract investors. |

**Source: Field data 2016**

## Summary of Findings

The result from the study is summarized below:

1. The study identified the following as the root causes of proliferation of cyber insecurity in Nigeria;
    - Poor Promotion of recruitment, training, upgrade in technical skills and development of cyber security personnel in Nigeria. This root cause results in shortage of security agents with top notch skills to trail apprehend investigate prosecute and punish cyber criminals. The resultant effect of this creates a near safe haven for these cyber criminals to operate hence making the Nigerian cyberspace very insecure.

    - Lack of proper feasibility by the government before implementing certain economic policies, for example the FOREX policy. Some of these policies render the Nigerian business terrain unfavourable for investors hence old investments pull out or cut down on staff, while there are no new investments coming up. This causes unemployment. High rate of unemployment and poverty now propel the youth to take to cybercrimes. Again, the Nigerian citizens often celebrate criminals and play sycophancy around them just to get miserly peanuts from them. A common scenario where Cyber Criminals who throw money around become mentors to these vulnerable and unemployed youth in the country hence promoting cybercrimes and rendering the Nigerian cyber space insecure.

    - Sabotage by regulation and monitoring agencies render the energy sector unfunctional hence making the country unfavorable to investors, this leads to high rate of unemployment in Nigeria.

- Sabotage by the elite politicians and poor funding of the security agencies cause insecurity which scares investors away leading to unemployment.

2. The study also provided recurrent preventions for the root causes identified to avert these problems from always occurring, these include;

   - Establishment and proper funding of world class cyber security institutions, charged with the mandate to train, upgrade and certify digital forensic investigators, ethical hackers, and other cyber security personnel on global best practices on cybercrime investigation, Protection, detection, prosecution and conviction.
   - Training of cyber security personnel who will embark on massive awareness and public sensitization campaigns to enlighten the citizens on how to protect themselves from cyber criminals.
   - Thorough feasibility should be done before implementation of Government policies to avoid implementing policies that will have a negative impact on the economy to avoid increase in unemployment.
   - Overhaul of the agencies monitoring and regulating the energy sector to eliminate saboteurs.
   - Proper funding of the security agencies to enable them combat insecurity effectively.

## References

Ibikunle. F. & Odunayo. E. (2013). Approach to cyber security issues in Nigeria: Challenges and Solutions. *International Journal of cognitive Research in Science, Engineering and Education.* Volume 1. No 1.

Laura, A. (1995). Cyber-crime and national security: The role of the penal and procedural law. Research Fellow, Nigerian Institute of Advanced Legal Studies. Retrieved from http://nials-nigeria.org/pub/lauraani.pdf.

Moses-Òkè, R. O. (2012). Cyber capacity without cyber security: A case study of Nigeria's national policy for information technology (NPFIT). *The Journal of Philosophy, Science & Law* Volume 12, May 30, 2012, retrieved from www.Miami.Edu/Ethics/Jpsl.

Okonigene, R. E., Adekanle, B. (2009). Cybercrime in Nigeria. Business Intelligence Journal, retrieved from http://www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7.pdf.