International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:5, 2015

# Cyber Security in Nigeria: A Collaboration between Communities and Professionals

K. Alese Boniface, K. Adu Michael, K. Owa Victor

***Abstract*—**Security can be defined as the degree of resistance to, or protection from harm. It applies to any vulnerable and valuable assets, such as persons, dwellings, communities, nations or organizations. Cybercrime is any crime committed or facilitated via the Internet. It is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It includes the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Nigeria like any other nations of the world is currently having her own share of the menace that has been used even as tools by terrorists. This paper is an attempt at presenting cyber security as an issue that requires a coordinated national response. It also acknowledges and advocates the key roles to be played by stakeholders and the importance of forging strong partnerships to prevent and tackle cybercrime in Nigeria.

***Keywords*—**Security, Cybercrime, Internet, Government, Stakeholders, Partnerships.

## I. Introduction

THE coming of Information Technology can be regarded as both "a blessing and a curse" when it comes to security. Despite the fact that many wars are still being fought in the physical and with physical weapons, there are quite many more being fought on information superhighway with digital facilities. Personal, national and international security issues have continued to change over the years in terms of the threats, the risks and combative methods [1]. The internet and digital technologies are bringing many benefits to Nigerians. Increasing connectivity allows us to stay in touch with family and friends, access services and communicate online. However, just as the internet and other new technologies are opening up tremendous possibilities, they also provide opportunities for criminals to commit new crimes and to carry out old crimes in new ways. It is clear that the number, sophistication and impact of cybercrimes continue to grow and pose a serious and evolving threat to Nigeria individuals, businesses and governments. Although it is difficult to quantify the total costs, evidence from operational agencies suggests that economic costs of cybercrime in Nigeria are substantial. As many instances of cybercrime go unreported, it is difficult to give an accurate figure. And there are other costs of cybercrime that cannot be quantified, no monetary value can reflect the harm caused to victims by the distribution of child exploitation material or the compromise of personal information, or the emotional hardship of being left financially destitute. Criminals can commit crimes across multiple borders in an instant and can target a large number of victims simultaneously. Tools that have many legitimate uses, like high speed internet, peer to peer file sharing and sophisticated encryption methods, can also help criminals to carry out and conceal their activities. Despite these challenges, cybercrime is still a form of crime and requires a long term, sustained response from stakeholders in Nigeria most especially, the government. Unlike other threats currently facing the country, cyber-attacks on individual citizens can have instant, wide-ranging consequences for the nation's economic and security interests. No country, industry, community, or individual is immune to cyber risks, and no one government agency, company, or individual can solve the riddle of cyber security but only through collaborative efforts. These are old crimes committed in new ways. The internet and digital technologies provide a platform for committing crimes such as fraud and identity theft on an industrial scale. Our increased connectivity has created new opportunities for criminals, new methods of delivery and new 'business models', bringing the online forms of these crimes within the definition of cybercrime. The anonymity and reach of the internet can also magnify antisocial behaviours which exist in the offline world, such as bullying and harassment. While not all instances of this behaviour are criminal, sufficiently serious instances may be treated as such.

Alese, Boniface K. is an Associate Professor in Computer Science Department and Acting Dean, Students' Affairs, the Federal university of Technology, Akure, Nigeria (phone: +2348034540465; e-mail: bkalese@futa.edu.ng).

Adu, Michael K. is a Senior Lecturer in Computer Science Department, the Federal Polytechnic, Ado Ekiti, Nigeria (phone: +2348066714060; e-mail: memokadu@yahoo.co.uk).

Owa Victor K is a lecturer in Computer Science Department, Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria (Phone: +2348033738090).

## II. Classification of Security Attacks

According to [2], security attacks can be classified into two, which are: passive and active attacks. Passive attacks attempts to hear or use information from the system but does not attack system resources, while active attack attempts to alter system resources or attack their operation. When you monitor phone conversation between two parties, it is a form of passive attack but when you disconnect a line of communication between two parties, it is a form of active attack.

### *A. Passive Attack*

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent as usual, and received in an apparent normal fashion. Neither the sender nor the receiver is aware that a third party has read the message or observed the traffic

pattern. However, it is feasible to prevent the success of these attacks, usually by means of cryptographic schemes. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

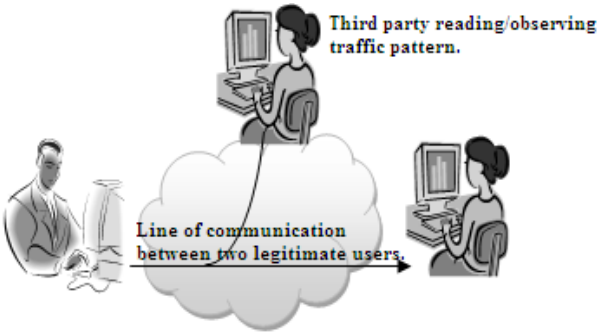


Fig. 1 Passive Attack

*B. Active Attacks*

Active attacks involve some modifications of the data stream or the creation of a false stream, and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

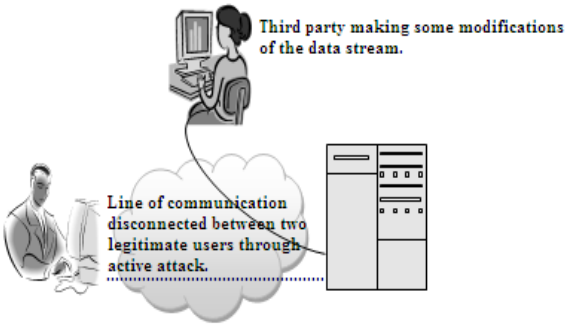


Fig. 2 Active Attack

## III. Software Access Control System

According to [3], software access control falls into two types: point of access monitoring and remote monitoring. In Point of Access (POA), personal activities can be monitored by a PC based application. The application can even be connected to a network or to a designed machine or machines. The application collects and stores access events and other events connected to the system operation and download access rights to access terminals. In remote mode, the terminals can be linked in variety of ways, including the use of modems, telephones lines, and all forms of wireless connections. Such terminals may, sometimes if needed, have an automatic calling at pre-set, or have an attendant to report regularly.

All of these access controls can be in the form of the following services:

*A. Confidentiality*

This relates to the protection of information from unauthorized access, regardless of where the information resides or how it is stored. Information that is sensitive or proprietary needs to be protected through more stringent control mechanisms. Authentication and authorization are two mechanisms used to ensure the confidentiality of information. Policies must be in place to identify what information is confidential and the period of time it should remain confidential. A framework must be developed for classifying information according to its characteristics and should include associated security requirements for each confidentiality ranking. According to [4], confidentiality means only authorized people or system can access protected data. Confidentiality can be very complex as it involves issues like cryptography and steganography.

*B. Integrity*

The integrity service protects data against active threats such as those that may alter it. Just like data confidentially, data in transition between the sending and receiving parties is susceptible to many threats from hackers, eavesdroppers, and cryptanalysts whose goal is to intercept the data and alter it based on their motives. This service, through encryption and hashing algorithm, ensures that the integrity of the transient data is intact. A hash function takes an input message M and creates a code from it. The code is commonly referred to as a hash or a message digest. A one-way hash function is used to create a signature of the message just like a human fingerprint. The hash function is therefore used to provide the message's integrity and authenticity. The signature is then attached to the message before it is sent by the sender to the recipient. Just like the issue of confidentiality has attracted a lot of researches in cryptography and steganography, solutions are being proffered for the matter of integrity through researches in the area of Digital Signature.

*C. Non-Repudiation*

This is a security service that provides proof of origin and delivery of service and/or information. In real life, it is possible that the sender may deny the ownership of the exchanged digital data that originated from him or her. This service, through digital signature and encryption algorithms, ensures that digital data may not be repudiated by providing proof of origin that is difficult to deny. A digital signature is a cryptographic mechanism that is the electronic equivalent of a written signature to authenticate a piece of data as to the identity of the sender.

## VI. Cyber Security Trinity Measures in Nigeria

The problem of cyber security requires committed efforts from every angle right from prevention to detection and response.

*A. Prevention*

Cyber criminals are not different from traditional criminals in a way because they both want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner when armed with a little technical advice and common sense. Many cybercrime attacks can be avoided. Similar to target hardening

for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber-criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target. The following are some of the basic ways that cybercrime can be prevented [5]; keep computer system up-to-date, secure configuration of the system, choose a strong password and protect it, keep firewall turned on, install or update antivirus, protect personal information, read the fine print on website privacy policies and review financial statements regularly.

*B. Detection/ Authentication*

Authentication is a service used to identify user. User identity, especially for remote users, is difficult because many users, especially those intending to cause harm, may masquerade as the legitimate users when they actually are not. This service provides a system with the capability to verify that a user is the very one he or she claims to be, based on what the user is, knows, and has. Physically, we can authenticate users or user surrogates based on checking one or more of the following user items: user name, password, retinal images, physical locations and identity cards. According to [6], the best method/ approach to detecting cyber criminals, is to start from the source of internet service connectivity. This source is usually the internet service provider (ISP) that provides internet service to their subscribers in different forms. Before a subscriber is allowed to connect through any ISP, they must be fully registered with such ISP. Collecting information that truly validates an individual involves; Collecting subscribers Bio-data (e.g. Full name, Age, etc.), Passport photographs, Full address of residence, Biometric Information (e.g. Fingerprint) and Verifying Subscribers genuinely from the state. If all these could be undertaken, the ISP may proceed by assigning a static IP address to the subscriber's line. It should be part of the ISPs agreement that any subscriber whose line is used to process any form of criminal activity would be cut-off without notice. Other service providers like Mobile phone operators must collect the same information as other ISPs before the line is activated for internet connectivity. ISPs should have software in place that monitors the activities of Users/subscribers. Cyber Cafes should put in place software that will monitor the activities of client as they surf the web. Internet hotspots should be modified to prevent the use of proxy on its network. National Communication Commission (NCC) in Nigeria as the case study could be assigned the responsibility of keeping and maintaining the activities of internet users registered through the Internet Service Providers in the central database. The database will have an admin panel where detailed information about all users' activities can be sort for and accessed on demand.

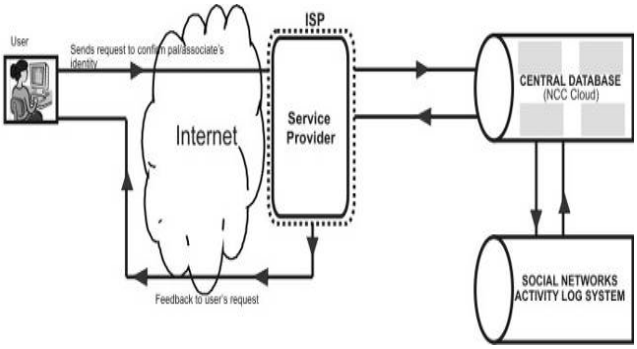


Fig. 3 System Architecture with Activity Log feature for Online Social Networks monitoring

*C. Responses*

A range of government agencies can be put in place to respond to different aspects of cybercrime in Nigeria. Local and State agencies should have primary responsibility for cybercrime that targets individuals, businesses and government systems in their jurisdictions. The National Cybercrime Working Group (NCWG) must be put in place to bring together representatives from Local, State and Federal Governments. Nigeria Law enforcement and justice agencies are to ensure that agency efforts in response to cybercrime are properly aligned. Other agencies are to be involved in responding to cybercrime including Consumer Protection Agency (CPA).


Fig. 4 Cyber security Trinity Diagram

## V. Roles and Responsibilities of Stakeholders in Nigeria

The roles and responsibilities of agencies involved in responding to cybercrime are described in more detail.

*A. Law Enforcement Agencies*

The Nigeria Police needs adequate training in cyber security. The basic mission for which the police exists is to prevent crime and disorder. However, it could be very difficult for any police officer to prevent a crime of which he has no knowledge of, or the instrumentality of operation is unknown to. The Police officer must not only be computer literate but should have adequate knowledge of what a criminal is capable

of using the computer or the internet to perpetrate. The police service in Nigeria must be reorganized to face the reality of the challenges pose by cybercrime. There are 36 states in Nigeria including the Federal Capital Territory, each led by a Commissioner of police. Within a state, there are local government areas of average of 20. It is very difficult to achieve effective policing to prevent cybercrime. Police officers must be familiar with the terrain of operation before he can discharge effectively. The idea of establishing state police will be one of the major steps to mitigate threats of online social media in Nigeria. Local vigilante group and non-profit, voluntary organizations are equally important in this task.

### *B. Government*

It is very germane that serious government policies against cybercrime and threats to online social media must be trusted by all citizens. As trusted leaders they are instrumental in advancing the mission of arming citizens with resources and tools needed to protect themselves, their families, and the nation against growing cyber threats [7]. Government should establish the following agencies/centres to assist the police.

1. Nigeria Cybercrime Task Force

The task Force should prioritize investigative cases that involve some form of electronic crime by bringing together state and local law enforcement agencies, prosecutors, private sector interests and academia in an effort to prevent cyber-crime and identity theft. They should educate the public on how to respond to credit card fraud, identity theft and other online crimes.

2. Internet Crimes Complaint Center

The centre will operate as a partnership between Cybercrime Task Force, the Police and other agencies like the Economic and Financial Crime Commission to provide a central referral mechanism for complaints involving internet related crimes for law enforcement and regulatory agencies at the federal, state, local, and international level. The Centre will also lead efforts to improve the nation's cyber security posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation. It will respond to incidents; provides technical assistance to information system operators; and disseminates timely tips and notifications regarding current and potential security threats and vulnerabilities. The centre will additionally educate and empower citizens to use the Internet safely and securely.

### *C. Individuals*

As with crime in the physical world, no amount of action by governments and the private sector can prevent every cybercrime. Those who use digital technologies have to take responsibility for their own security and safety online and exercise safe online practices. Most instances of financially-motivated cybercrime can be prevented by taking simple steps or by knowing what to look out for. Governments and industry can assist users to understand these steps and to recognise the warning signs. Every user must be aware of the risks of cybercrime, take steps to protect themselves and know where they can get help if they fall victim to cybercrime.

## VI. Partnerships and Shared Responsibility

Tackling cybercrime is, and always will be a shared responsibility between individuals, industry and government. This means forging mutually beneficial partnerships to share information and combine efforts to combat cybercrime [8]. Governments will also explore other partnership arrangements, including with overseas law enforcement agencies and with key industry sectors, such as internet service providers (ISPs), online service providers and the tertiary education sector. All societies and organizations whose activities and interest are tailored toward Information and Communication Technology must be involved. They include Nigeria Computer Society (NCS) and Computer Professional (Registration Council) of Nigeria (CPN) among others.

## VII. Conclusion

Criminals are quick to find ways to exploit new technology of the internet to further their illicit activities. Government at all levels, agencies, industries and academics must stay up-to-date with whatever methods that can be employed by the perpetrators especially as proposed in this paper. The collaboration and partnership between every one and agencies will enable sharing quality, timely and adequate information and intelligence along with law enforcement agencies. This is expected to lead to a better understanding of cyber-crime by Nigerians and more effective responses to enable cyber security. The Information and Communication Technology society and professional bodies are expected to help in developing a better understanding of cybercrime in Nigeria by providing a centralized national online facility to safe guide the public and report cybercrime. The facility is to be hosted and maintained by the National Communication Commission (NCC). It is expected that data from Consumer Protection Agency, National Cybercrime Work Group and the Economic and Financial Crime Commission (EFCC) as detail in this paper will enable the expected collaboration and provide a framework for effective cyber security. Nigeria government must recognize that it is better to prevent cybercrime from happening than to respond to it after it has occurred. In many cases, effective preventive measures are relatively low cost and easy to implement. Users need to take steps to avoid falling victim to cybercrime and governments and industry need to be proactive in anticipating where new threats might emerge. The internet is built upon the freedom, creativity and innovation of users. In striving to create a more secure online environment and take action against cyber criminals, it should be noted however that our response must balance the rights of all citizens to freely roam, create and interact on the internet, and uphold individuals' right to privacy.

## REFERENCES

[1] B.K Alese, "Security Issues in Nigeria: Getting Ready for the Digital Challenge", First Bank of Nigeria Plc Professorial Chair in Computer Science Annual Lecture, 2014.
[2] W. Stallings "Network Security Essentials", Prentice Hall, 2002.
[3] J.M. Kizza "A Guide to Network Security", Springer Publishers, 2009.
[4] B.K. Alese and A. Adetunmbi " Privacy, Trust and Security Framework for Pervasive and Large Systems (Case Study; e-health application)", International Conference on Science and Technology, 2005, 729 – 732.
[5] M. Babu, and M.G. Parishatb "What is Cybercrime" http://www.ncpc.org/resources/files/pdf/internet-safety, 2012.
[6] B.K. Alese and M.K. Adu, "Curbing Cybercrime by Application of Internet Users' Identification System (IUIS) in Nigeria, XI International Science Conference, International Research and Innovation, Singapore, 2014, 560 – 563.
[7] A National Plan to Combat Cybercrime; Achieving a Just and Secure Society, www.ag.gov.au.
[8] Law Enforcement and Cyber security; Homeland Security, Norton Cybercrime Report, 2012.