International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Cyber Security in Nigeria: Issues, Challenges and Way Forward

UWADIA Francis[1], ETI, I. Friday[2]
[1, 2]Department of Computer Science, Delta State Polytechnic, PMB 5. Ozoro, Delta State Nigeria
Email address: [1]francisuwadia@gmail.com

Abstract*—Internet is the connectivity of computer across the globe. Cyber is the surfing of internet with a view of get information, processing, retrieving, saving, upload, download and so on. Cyber insecurity is a challenge to the overall development and appreciation of internet services. Cyber security refers to preventative methods used to protect information from being stolen, compromised or attached (Daniel et al., 2017). It requires an understanding of potential information threats such as viruses, malicious code, and hackers' etc. This paper addressed the issues of such as capable to mire the data integrity when engaging on other internet activities such as social media, use of search engines when working on information on which security matter most. This paper stands to say that every internet user should be aware of the challenges pose by hackers and give possible solutions to cyber insecurity in Nigeria*.

***Keywords*—** *Cyber, security, challenges, hackers, internet*.

I. INTRODUCTION

Cyber is the surfing of internet with a view of get information, processing, retrieving, saving, upload, download and so on. The internet is an Integral part of the lives of millions of people around the world (Wikibooks, 2010). Internet provides governments, businesses, and individual across the globe, services and capabilities they should depend to improve performance of their works. This has revolutionized the modern age by providing real-time communications, electronic financial transactions, data transfer, and access to information of any sort and so on. Life has been made easy by cyber in way of carrying of the palm top, android and others anywhere you go. This electronics has the capability of processing a full library of book, online activities is computerized. This is why everybody wants to be on the internet. As a result of this, intruders have also made themselves available on the internet to breach the privacy of users to their own benefit and the detriment of the owner.

Cyber security is the branch of computer security with measures and rules against attacks over the internet According to Wikipedia, Cyber security is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. This has brought risk of people losing their confidence on the internet value. However, the Nigeria cyber security outlet, (2014), predicted that "The 31,536,000 seconds that made up the year round the world is used effectively by hackers in planning attacks and exploiting vulnerable people, systems, and processes" With each cyber-attacks, companies lose millions trust by consumers get eroded, and troves of confidential information are published. Fortunately, government has begun to recognize the implications of these risks and taken measures to address them resulting in a variety of efforts devoted to cyber security. The national Assembly of Nigeria made a bold move in the war against cybercrime when the senate passed the cybercrime bill (cyber security law, 2015). These accomplishments in addition to the cyber security strategy and policy documents introduced by the office of the National Security Adviser (NSA) are attributes that defines the awakening of Nigeria to cyber insecurity

Based on the current events in both social and economics realms in Nigeria, therefore, we hereby state that users of internet should as matter of fact use uneasy to predict password and never a time should be shared. Un-password system should be seen a house on the road side with great values inside without doors. There is no how passers-by will not be tempted to take something from inside since there is no watchdog or password. Another precaution is to avoid careless or care-free altitude of trusting everybody and leave laptop anywhere later to find out that the information has been tampered.

1.1 Issues in Cyber Security in Nigeria

The increase in cyber insecurity in Nigeria could be linked to the following issues:

- *Poor safety measure of handling laptop*

The care-free life of some people in Nigeria, their ignorant of regular security breach and negligence of information has left our worthwhile information or gadget into the hand of cybercriminal (Wayback Machine, 2016). Some people leave their gadget anywhere later to find out that somebody has made away with it and such exposing information into wrong hands that can use it for something evil. Unfortunately, too many users don't deploy the privacy settings on the device

- *Assigning more than one password to people.*

People or organization transfer password for certain motives. This can be influence by trust or nature of job. According to Sungardas Availability Services, (2014), password sharing by IT professionals was one of their top security concerns. There are two different, but very important, password sharing concerns. First is sharing a single password among multiple sites or access points. If someone guesses that password he will gain access to a lot of materials because of the negligence of organization. Second is sharing a password with your co-workers. Somebody can to gain access to many unauthorized sites because fellow employees share their password with him.

UWADIA Francis and ETI, I. Friday, "Cyber Security in Nigeria: Issues, Challenges and Way Forward," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 2, pp. 351-354, 2018.

- *Use of flimsy/trivial or stress-free to predict password*

Stress-free to predict passwords are not good for security purpose. However, passwords are going to continue to be the first point of validation for a long time. Trivial password is like no password, any password that resolves around the name of owner of organization, name of organization or acronym of organization can easily be predicted by hacker or people. It can then become an issue of what password should be used for security bearing in mind that owner of password always want what they can remember. The owner of system should think of what cannot easily be predicted regardless of how it will be recall by the individual. (Montoro and Massimiliano, 2009).

- *Always shut down computer*

Computer should be shut down when not in use or on your way out of the computer room otherwise exposes the computer to malicious attack which may cause bandit to carry away computer thereby exposing the information into a wrong hands. This can also make hackers to use undue privilege to attack the system (Ovidiu and Peter, 2016).

- *Negligence to firm or association security progams:*

This negligence is recorded mostly when security measures are neglected by trained computer application IT staff or employees (Rouse and Margaret 2018). They may disregard the company security programs because they want to revenge at their uproar on them or even delay in salary. It could be none of the aforementioned issue but wickedness of people. People can overlook setting security measures (Ed Gelbstein (2013). They get familiar with the society that they neglect security measures. Some of them will end up crying heard I know.

- *Social media:*

The social media contains the good and bad. Engaging the social media while doing serious company job exposes your information of hacker or intruder unknown to you. Social media is a hotspot embedded with malwares and vices that may affect organization. Jim Finkle (2014).

1.2 The Way Forward in Tackling Cyber Insecurity in Nigeria

(1) Cybercrime Prosecution:

The cybercrime Act 2015 support prosecution as a way forward to curb cyber insecurity in Nigeria. The cybercrime bill passed by senate has provided legal ground to organization for prosecuting cybercrime.

a). The Nigerian Cybercrime offers the President the power to assign computer systems, networks, and information infrastructure relevant to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furtherance of security. Examples of systems, which could be designated as such, include transport, communication, banking etc.

b). The Cybercrime Act 2015 states that, when hackers are found guilty of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (subject on the purpose of the hack). The same punishment is to be suffered by Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

c). Death penalty is advocated by The Nigerian Cybercrime Act 2015 for an offence committed in contrast to a system or network that has been labelled critical national infrastructure of Nigeria that results in the death of an individual (amongst other punishments for lesser crimes).

d). The Cybercrime Act 2015, Makes provision for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment. An example of identity fraud would be the individual who impersonated.

e). Precisely, Creates Child Pornography site is punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing, and possession of child pornography.

f). Crooks Cyber-stalking and Cyber-bullying prescribe punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.

g). The Nigerian Cybercrime Act 2015, prohibits cyber squatting, which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.

h) It forbids the use of threats of violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin and prohibits the distribution of racist and xenophobic material to the public through a computer system or network (e.g. social network. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than N10 million or to both fine and imprisonment.

i). The act mandates that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional Right to privacy, and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

j). Allows for the interception of electronic communication, by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings.

The above is just a high-level overview of certain interesting provisions in the newly passed legislation. The Act itself contains 43 sections, and is a very important piece of legislation to foster the development of the nascent ICT sector in Nigeria. You can read the full provisions of the Act here – Cybercrime (Prohibition, Prevention, etc) Act 2015

(2) 24-Hour camera:

This camera (Closed Circuit Television Camera), CCTV can produce images or recording for surveillance purpose, capable in capturing even a fast running vehicles (Dempsey and John, (2008). The mounting of CCTV is widely accepted as there is wireless, wired on that could fit into 1the walls, pass-way, street etc. (BBC. 11 March 2002). CCTV connected to the global positioning system (GPS) can get any location in the world. This will make easy to get any move that is against security.

(3) Use antivirus program:

Antivirus is a program that counters the program written by intruders to have illegal access to the system. The antivirus has the ability to discover this malicious software, quarantine it and possibly delete to avoid further attack. Although virus is on the increase on a daily bases so all there is counter attack to destroy the virus. This is the use of anti-virus. Christos K, (2012).

(4) Security setting must not be disabled:

You must be able to adjust the security setting. You should know what you allow into your computer. The prosper management of the security setting will prevent intruder and eliminate harm to the information. (Rossouw and Johan, (2013).

(5) Use genderless screen name:

When you choose a gender less screen name you may not be give any consideration by people. The intruders may ignore it because they are anonymous.

(6) Don't disclose your detail:

Be careful with whom you give your full names or address. When you disclose some close detail of your life you may hurt yourself. This information may be used as spoofing to somebody that knows you thereby attacking the person (Marcel *et al.,* 2014).

II. CONCLUSION

Cyber is the surfing of internet with a view of get information, processing, retrieving, saving, download and so on. Internet is the interconnectivity of computer across the globe. Cyber has become an integral part of lives of millions of people around the world. Cyber security is challenge to the overall development and appreciation of information and communication technology. The issue of cyber security is enormous. Today, hackers and cyber criminals can spend a lot of time on the internet to get their subject or target. As a result of cyber-attack there is always a great lose by organization or individual. In Nigeria cyber in security has become rampant with the growing unemployment and quick to get rich motive of the society. The national assembly of Nigeria made a bold step in the war against cybercrime when the senate passed the cybercrime bill. However, this research has outlined the solution to combat this criminal act. Cybercrime must not be underestimated as the seeming deductions are that, the hackers are always one step ahead; this gap must be bridged. Organization should put measure in place to track down cyber criminals. According to Lawrence Snyder, (2003) states that right of people to choose freely under what circumstances and extent they will reveal themselves, their attitude, and their behavior to others.

Therefore, we hereby state that users of internet should as matter of fact use uneasy to predict password and never a time should be shared. Un- password system should be seen a house on the road side with great values inside without doors. There is no how passers-by will not be tempted to take something from inside since there is no watchdog or password. Another precaution is to avoid careless or care-free altitude of trusting everybody and leave laptop anywhere later to find out that the information has been tampered. Cyber insecurity is a challenge to the overall development and appreciation of internet services. The issue of cyber security is enormous. Hackers and cyber criminals can spend a lot of time on the internet to their subject or target. Use of stress free password, forget to shutdown, poor safety measure of se data on the internet are more propone to attack than standalone computer. We are likely to see more collaboration between organization in tackling cybercrime as the central bank of Nigeria (CBN) drives the Nigerian e-fraud forum (NeFF) where banks meet to share experience on fraud and mitigating factors (NeFF, 2016). The sharing of cyber security intelligence in the financial sector is growing and would serve as model for other areas of the economy.

REFERENCES

[1] BPS/DIR/GEN/CCD/02/009 (2016) Annual Report of Nigeria Electronic Fraud Forum (NeFF) Published 7/5/2017 Retrieved 8/5/2018.
[2] Christos Kalloniatis (2012) Security Enhanced Applications for Information Systems - InTech ,
[3] Daniel, et al., (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 7 May 2018.
[4] Dempsey and John S. (2008). Introduction to private security. Belmont, CA: Thomson Wadsworth. p. 78. ISBN 9780534558734
[5] Gelbstein E.D (2013). Good Digital Hygiene: A guide to staying secure in cyberspace publishing Bookboon.
[6] "Internet of Things Global Standards Initiative". ITU. Archived from the original on 26 June 2015. Retrieved 26 June 2015.
[7] Jim Finkle, (2014). "Hacker says to show passenger jets at risk of cyber attack". Reuters. Archived from the original on 13 October 2015. Retrieved 8/5/2018
[8] Lin and Tom C. W. (2017). "The New Market Manipulation". Emory Law Journal. 66: 1253. SSRN 2996896 Freely accessible.
[9] Montoro and Massimiliano, (2009). "Brute-Force Password Cracker". Oxid.it. Retrieved 8 May 2018.
[10] Marcel, Sébastien; Nixon, Mark; Li, Stan, (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Springer. Doi: 10.1007/978-1-4471-6524-8. ISBN 978-1-4471-6524-8. ISSN 2191-6594. LCCN 2014942635. Retrieved 8 October 2017 – via Penn State University Libraries.
[11] Ovidiu, V. and Peter F. (2016) "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems" (PDF). River Publishers. Retrieved 8/5/ 2018.
[12] Rouse, Margaret. "Social engineering definition". TechTarget. Archived from the original on 5 January 2018. Retrieved 6 May 2018
[13] Snyder Lawrence (2003) Fluency with Information Technology Skills, Concepts, Capabilities preliminary edition by Pearson Education.
[14] Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; Ko, Hajoon; Eyers, David (2015). "Twenty Cloud Security Considerations for Supporting the Internet of Things". IEEE Internet of Things Journal. 3 (3): 1–1. doi:10.1109/JIOT.2015.2460333
[15] Summers, G. (2004). Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5
[16] Wikibooks, (2010) Information Security in Education

[17] Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Wayback Machine.

WEB REFERENCE

[1] http://blog.sungardas.com (2014) think-you-don't-work-in-information-security-think- again/#sthash.HIRkvr2E.dpbs) Retrieved on 8/5/2018

[2] https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention, etc)_Act,_2015.pdf Retrieved onRetrieved on 15/2018

[3] Computer security Wikipedia: https://en.wikipedia.org/wiki/Computer_securityRetrieved on 8/5/2018