Global Scientific JOURNALS

GSJ: Volume 11, Issue 4, April 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

CYBERSECURITY ISSUES IN NIGERIA: CHALLENGES AND CONTROL MEASURES

ZAMAN, Chongkon Haruna
Ph.D. Student in the Department of Electrical and Computer Engineering
Morgan State University, Baltimore, Maryland, USA
Chzam1@morgan.edu

Abstract

Cybercrime is perhaps the most evolving high-technology crime of the twenty-first century. Cybercrime refers to a series of organized crimes attacking both cyberspace and cybersecurity. Cyber Security protects information and information systems such as networks, computers, databases, data centers, and applications with appropriate procedural and technological security measures. Security countermeasures help ensure information systems' confidentiality, availability, and integrity by preventing severe asset losses from Cyber Security attacks. As the internet and associated technologies increasingly permeate every aspect of human activities, so do the vulnerabilities to cyber victimization. Recently, Cybersecurity has emerged as an established discipline for computer systems and infrastructure, focusing on protecting valuable information stored on those systems from adversaries who want to obtain, corrupt, damage, destroy or prohibit access to it. In Nigerian today, many youths have reacted to the increase in the unemployment rate in a negative way by indulging in cybercrime. The recent unprecedented outbreak of cybercrime in Nigeria is quite alarming, and the negative impact on the country's socio-economy is disturbing. This paper seeks to overview cybercrime and cyber-security, outline some challenges, and proffer solutions.

Keywords: Cyber-space, Cyber-security Cyber-crime, Internet

Introduction

“The science of today is tomorrow’s technology,” says Edward Teller. Cyber Security protects information and information systems such as networks, computers, databases, data centers, and applications with appropriate procedural and technological security measures. Computer security protects the items you value, called the assets of a computer or computer system. Many types of assets involve hardware, software, data, people, processes, or combinations. To determine what to protect, we must first identify what has value and to whom. Cyberspace is "the environment in which communication over computer networks occurs. Cybercrime refers to the series of organized crimes attacking both cyberspace and cybersecurity.

The Internet is one of the fastest-growing areas of technical infrastructure development. In today’s business environment, disruptive technologies such as cloud computing and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting business online. According to Vairaprakash Gurusamy and Bhargav Hirani (2018), more than 80% of commercial transactions are done online, so this field requires high-quality security, transparency, and the best trades.

Research has shown that the first recorded cyber murder was committed in the United States. According to the Indian Express, in January 2002, an underworld don in a hospital was to undergo minor surgery. His rival hired a computer expert who altered his prescriptions by hacking the hospital’s computer system. An innocent nurse administered him the altered drug, which resulted in the patient’s death (Mohsin, A. 2006). Statistically, all over the world, there has been a form of cybercrime committed every day since 2006 (Schaeffer, B. S. et al. 2009). Before the year 2001, the phenomenon of cybercrime was not globally associated with Nigeria. This resonates with Nigeria realizing the internet’s full potential right about that time. Since then, however, the country has acquired worldwide notoriety in criminal activities, especially financial scams, facilitated through the Internet.

(Roseline, O. Moses-Òkè 2012). Nigerian cyber criminals are devising new ways of perpetrating this form of crime daily, and the existing methods of tracking these criminals are no longer suitable to deal with their latest tricks.

In Nigeria and the world, in terms of business, industry, government, to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, and customized and generic report generation in a real-time processing mode. However, unfortunately, it has also brought unintended consequences such as criminal activities, spamming, credit card fraud, ATM fraud, phishing, identity theft, and a blossoming haven for cybercriminal miscreants to perpetuate their insidious acts.

Cyber-attacks have increased in Nigeria in the wake of COVID-19 restrictions and lockdowns. In 2018, commercial banks in Nigeria lost a cumulative N15 billion (US$39 million) to electronic fraud and cybercrime. This was a 57% increase in the N2.37 billion loss recorded in 2017. Over 17 600 bank customers and depositors lost N1.9 billion to cyber fraud in 2018, with fraud rising by 55% from the previous year. Nigeria’s Consumer Awareness and Financial Enlightenment Initiative have projected a US$6 trillion loss by 2030 to cybercrime within and outside Nigeria. These crimes are committed chiefly through phishing and identity theft (Maurice Ogbonnaya, 2020).

With a significant rise in internet penetration in Nigeria to about 47.1 % in 2018 to the Nigerian Bureau of Statistics (2019), some Nigerian youths have chosen a negative way of acquiring wealth through various forms of cybercrime. Therefore, the recent outbreak of cybercrime in Nigeria is quite alarming, and the negative impact on the country's socio-economy is alarming.
Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace and growing unease about cyber and personal security.

The victims also show increasing naivety and gullibility at the prospects incited by these fraudsters. Since the issue of cybersecurity is raising several questions in the minds of Nigerians, it is only fair that we answer these questions.

Literature Review

Security is a principal and continuing concern that restricts customers and organizations from engaging with online business; The cyber-crime issue has been discussed by many researchers with various perspectives on it, most coming at it from different sides than others.

Overview of Cybercrime

Cybercrime is a new trend gradually growing as the internet penetrates every sector of our society, and no one can predict its future. Therefore, crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories:
1. Crimes that affect computer networks and devices directly. Examples are malicious code, computing viruses, malware, etc.

2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or devices. Examples include Cyber Stalking, Fraud and identity theft, phishing scams, and information warfare.

Nature of Cybercrime

Cybercrime is categorized into four by a leading cybercrime scholar, Wall (2001, p.3-7): cyber trespass, cyber deception/theft, cyber pornography, and cyber violence. Cyber trespass entails crossing into other people's property online to cause damage. Examples include hacking, defacement, and virus attack. Cyber deception/theft has to do with stealing money or property online. Examples include credit card fraud, phishing e-mails, or the violation of intellectual property. Cyber pornography has to do with violating obscenity and decency laws online—for example, child pornography. Finally, cyber violence refers to causing psychological harm to or instigating physical harm against others online and, in so doing, violating human rights laws. Examples include online hate speech, cyber stalking, etc.

Bendovschi (2015, p.25) outlines the various types of cyber-attacks that have been examined in the international literature as follows:
Ø *Man, the middle attack* occurs when the attacker interferes between the two communication ends. Thus, every message sent from source A to source Breaches the attacker before reaching its destination. The risk further posed by this attack includes unauthorized access to sensitive information or the possibility for the attacker to alter the information/message that reaches the destination.
Ø *Brute Force Attack*: This has to do with repeated attempts to gain access to protected information via, for example, password, encryption, and so on until the correct key is found, thereby enabling access to information.
Ø *DDoS (Distributed Denial of Service*). This attack compromises data availability by flooding the victim (e.g., server) with commands, thus becoming inoperable.
Ø *Malware*: This is a generic term to describe types of malicious software used by the attacker to compromise the confidentiality, availability, and integrity of data. The most common types of malware include viruses, worms, Trojans, spyware, ransomware, adware, and scareware/rouge ware;
Ø *Phishing*: This is a technique that is used to steal private information from internet users by masquerading as a trustful source (e.g., website);

Ø *Social engineering*: This generally describes the techniques used to gain unauthorized access to information through human interaction.

It should be noted that while Bendovschi's list is not exhaustive, it provides valuable insights into the themes that have, over the years, dominated international discourse around cybercrime and, specifically, cyber-attacks. Individual Internet users, organizations, and law enforcement agencies must be aware of the nature of cybercrime and the various techniques cybercriminals use to perpetrate it.

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cyber-crime (Hassan, 2012)

a. Unemployment is one of the major causes of Cybercrime in Nigeria. It is known that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they participate in criminal activities for survival.

b. Quest for Wealth is another cause of cybercrime in Nigeria. Youths nowadays are greedy; they are not ready to start small and strive to level up with their affluent counterparts by engaging in cybercrimes.

c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crimes knowing they can always go uncaught. Therefore, there is a need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

d. Incompetent security on personal computers. Some personal computers do not have proper or competent security controls; they are prone to criminal activities, so their information can be stolen.

Some Effects of Cyber Crime in Nigeria

- Results in 0.08 percent of the GDP loss of the country (Obarafor Victor, 2019)
- Financial loss: Cybercriminals are like terrorists or metal thieves because their activities impose disproportionate costs on society and individuals.
- Loss of reputation: Most companies have been defrauded or reported to have been faced with cybercriminal activities and complaints of clients losing faith in them.
- Reduced productivity: This is due to awareness and more concentration being focused on preventing cybercrime and not productivity.
- Vulnerability of their Information and Communication Technology (ICT) systems and networks.

Need for Cyber Security

The following are the objectives of cybersecurity.

- To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
- To help individuals and institutions develop and nurture a culture of cybersecurity.
- Work collaboratively with public, private, and international entities to secure cyberspace.
- To help understand the current trends in IT/cybercrime and develop practical solutions.
- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality.

Solutions for Curbing Cyber Crime in Nigeria

- Cyber awareness or sensitization of the populace will go a long way in educating the masses on preventing common forms of cybercrimes like email fraud, malware attacks, and limitations in accessing sexually explicit content from children and young people.
- Education: 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; hence We need to educate citizens that if they are going to use the internet, they need to maintain and update the security on their system continually. We must also educate corporations and organizations on the best practices for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Therefore, automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.
- Establishment of Programs and IT Forums for Nigerian Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employment for these youths and set up IT laboratories/forums where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria. At the same time, they could be rewarded handsomely for such novelty.
- Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like the United States) matches the address where the cardholder's billing statements are mailed.
- Interactive Voice Response (IVR) Terminals: This new technology is reported to reduce chargebacks and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.
- IP Address tracking: Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.
- Use of Video Surveillance Systems: The problem with this method is that attention has to be paid to human rights issues and legal privileges.
- Antivirus and Antispyware Software: Antivirus software consists of computer programs that attempt to identify, thwart, and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor programs, Trojans, and other spy wares from being installed on the computer.
- Firewalls: A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination. A network firewall typically guards an internal computer network against malicious access from outside the network.

- Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending postal mail to another party with a lock code on the envelope, which is known only to the sender and the recipient. Several cryptographic methods have been developed; some are still not cracked.
- Cyber Ethics and Legislation Laws: Cyber ethics and laws are formulated to stop cybercrimes. It is the responsibility of every individual to follow cyber ethics and cyber laws so that the increasing number of crimes will reduce. Security software like antiviruses and anti-spy wares should be installed on all computers to remain secure from cybercrimes. Internet Service Providers should also provide high security on their servers to protect clients from viruses and malicious programs.

Conclusion

As the general population becomes increasingly refined in their understanding and use of computers and the technologies associated with computing become more powerful, cybercrimes may become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cybersecurity must be addressed seriously as it is affecting the country's image in the outside world. A combination of suitable technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cybercriminals. Information attacks can be launched by anyone from anywhere. The attackers can operate without detection for years and remain hidden from countermeasures". This emphasizes the need for government security agencies to note the need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind cybercriminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. There is a need to create a security-aware culture involving the public, the ISPs, cybercafés, the government, security agencies, and internet users. Also, in terms of strategy, it is crucial to address issues relating to enforcement thoroughly. Mishandling of enforcement can backfire. Cybercrime is an evolving twenty-first-century social problem that has attracted global attention but has received relatively less attention regarding its awareness among internet users in Nigeria.

References

AHMED, A. T. I. S. (2018). Hiding Secret Text in Image Using RC2 and Serpent Algorithm. *Journal of The Iraqi*

Ali, Z., A. H. B. M. Aman, and R. Hassan. "Cloud query processing analysis: encryption and decryption." In *3C*
annotated bibliography. *Journal of Cybersecurity Education, Research and Practice*, *2016*(2), 4.

B. A. Omodunbi, P. O, Odiase, O. M Olaniyan and A. O. Esan (2016). Cyber-crime in Nigeria, Analysis, Detection, and Prevention

Back, S., Soor, S., & Jennifer LaPrade (2018). Juvenile hackers: An empirical test of self-control theory and social bonding theory. International Journal of Cybersecurity Intelligence and Cybercrime,

Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in Computing," ISBN 978-0-13-408504-

Choi, K.-S. (2015). Cybercriminology and Digital Investigation. LFB Scholarly Publishing LLC.

Choi, K.-S., Lee, C. S. & Cadigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber resource considerations. *Electronic Commerce Research*, *13*(1), 41–69.

Context of Autonomous Driving. In *2019 IEEE International Conference on Connected Vehicles and Expo* cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

Dr. Ibikunle Frank, and Eweniyi Odunayo,(2013). Approach to cyber security issues in Nigeria: challenges and solution Vol. 1, No.1 www.ijcrsee.com

Ewepu G, (2016). *Nigeria loses N127bn annually to cyber-crime* — NSA available at: http://www.vaat: http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/RetrievedBI. (n.d.). Cyber Crime. Retrieved from https://www.fbi.gov/investigate/cyber.

Florence Bola-Balogun (2019). The Evolution Of Cyber Security In The Nigerian Banking Sector http://www.mondaq.com/Nigeria/x/799360/Security

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International* from cyberspace. *Information & Communications Technology Law*, *23*(3), 220-237.

Giver, D. (2018). An argument for interdisciplinary programs in cybersecurity. International Journal of Cybersecurity Intelligence and Cybercrime, 1(1), 71–76. *Information Security*, *10*(4), 10. *Journal of Cognitive Research in Science, engineering, and Education*, *1*(1).
Journal of Computer Science and Information Security, *14*(1), 129.
Kankaanranta, A. (2018). *Threat mitigation in industrial internet: Case variable-frequency drive* (Master's thesis).

Koschuch, M., Sebron, W., Szalay, Z., Török, Á., Tschiürtz, H., & Wahl, I. (2019, November). Safety & Security in the

Kostopoulos, G. (2017). *Cyberspace and cybersecurity*. CRC Press.
Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional

Kubiat Umana (2015). Forms and Types of Cyber Crimes in Nigeria.

Kyung-Shick Choi(2018). The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity. International Journal of Cybersecurity Intelligence and Cybercrime, Vol. 1, Iss. 1, Page. 1-4.

Mousa, H. M. (2018). Chaotic genetic-fuzzy encryption technique. *International Journal of Computer Networks and*

Ndible N., (2016*). Practical Application of Cyber Crime* Issues Retrieved on May 6, 2016, available at: http://ijma3.org/Admin/Additionals/Cybercrime/Nibal%20Idlebi%20 Presentation.pdf

Maurice Ogbonna (2020). Cybercrime in Nigeria demands public-private action.

Nir Kshetri (2019). Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77–81, DOI: 10.1080/1097198X.2019.1603527 of Cybersecurity Intelligence and Cybercrime, 1(1), 71–76.

Ostrowski, J. (2020). OS Hardening.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: Global trends in *Security Challenges Through Data Analytics and Decision Support* (Vol. 47, p. 308). IOS Press.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International*

Shahbazian, E., & Rogova, G. (2016, November). Critical aviation information systems cybersecurity. In *Meeting*
Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, pp. 65-75. 2019.

Thomas, N. (2009). Cyber security in East Asia: Governing anarchy. *Asian Security*, *5*(1), 3–23.
University, (40-1), 594-604.

Vairaprakash Gurusamy(2018). Cyber Security for Our Digital Life
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2012). *Hands-on information security lab manual*. Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2016). Threats to Information Protection-Industry and Academic Perspectives: An