**Cybersecurity and Cybercrimes in Nigeria: An Overview of Challenges and Prospects**

Yakubu Aliyu Ibrahim
Department of Computer Science, Bingham University

Karu, Nigeria yakubu.ibrahim@binghamuni.edu.ng

Adelaiye Oluwasegun Ishaya
Department of Computer Science, Bingham University

Karu, Nigeria oluwasegun.adelaiye@binghamuni.edu.ng

Yusuf Musa
Department of Computer Science, Bingham University

Karu, Nigeria yusuf.musa@binghamuni.edu.ng

Adamu Sulaiman Usman

*Department of Computer Science, Bingham University, Karu, Nigeria*
adodass@binghamuni.edu.ng

Ipole Nancy
Department of Computer Science, Bingham University

Karu, Nigeria nancy.ipole@binghamuni.edu.ng

Ann Hassan Bijik
Department of Computer Science, Bingham University

Karu, Nigeria annebjk@binghamuni.edu.ng

Sunday Folusho Aiyedogbon
School of Computing ,

 Robert Gordon University

UK,

 s.f.aiyedogbon@rgu.ac.uk

*Abstract- This paper seeks to provide comprehensive overview of the challenges and potential developments within the realm of cybersecurity and cybercrime in Nigeria. The unintended consequence of internet’s growth in Nigeria has been the inadvertent facilitation of a haven for cybercriminals. Addressing this issue is of paramount importance due to escalating threat posed by cybercriminals both within the nation and on a global-scale. This study delves into an assessment of the impact of cybercrime, highlighting key indicators that contribute to its rise. This assessment is juxtaposed with the present state of technology utilization, particularly the prevalence of computing devices and communication methods within Nigeria. Through statistical analysis of the four stages of a cyber-attack, reconnaissance, weaponization, delivery and exploitation. This paper dissects their effects on the Nigerian cyber landscape. In response to these threats, effective countermeasures are explored, drawing attention to strategies that have demonstrated efficacy in mitigating cyber risks. Additionally, the paper underscores the significance of understanding common vulnerabilities and the necessity of conducting risk assessments, drawing insights from the Mitre framework. Considering the international nature of cybercrime, the importance of collaboration on global-scale is emphasized, highlighting initiatives that can aid Nigeria’s efforts in tackling this issue. The paper examines the existing legal and policy framework related to cybersecurity and cybercrime in Nigeria, identifying potential areas for enforcement. By encompassing comprehensive analysis of these factors and themes, this paper contributes to better understanding of the challenges posed by cybercrime and proactive measures that can be undertaken to safeguard Nigeria’s digital landscape.*

Keywords: Cybersecurity, Cybercrime, Internet, and Computer system.

Introduction

The global community increasingly sees the Internet as an important factor for socio-economic development, but it also has its drawbacks, such as cybercrime. However, governments in Nigeria and around the world recognize the power of digital transformation to reduce cybercrime rates and thereby improve the prosperity and well-being of its citizens. In this regard, they recognize that cybersecurity must be part of technological progress. Cybersecurity is basically the protection of computers and its networks from attacks by malicious actors that may lead to unauthorized disclosure of information, theft or damage of hardware, software or data, and disruption or misdirection of the services provided. Due to the scale of cybercrime, it is critical that governments have robust cybersecurity systems in place to mitigate threats and increase confidence in the use of electronic communications and services. It is therefore clear that cybercrime has a direct impact on its ICT growth and its illegal and malicious use. To thwart this impact, cybersecurity is becoming increasingly important among decision-makers in Nigeria, with cybersecurity principles established in Nigeria and nearly every country in the world. However, clear gaps still exist in Nigeria in terms of awareness, understanding, knowledge and ability to deploy appropriate strategies, skills and programs for the safe and appropriate use of ICT as an enabler of economic development.

Literature Review

Cybersecurity is the process of protecting the information and communication technology assets of nations, organizations, individuals and users by identifying and responding to threats that may compromise data stored or transmitted on systems [1]. The purpose of cybersecurity is to protect data and information from unauthorized users, protect data from modification, and ensure that only authorized users have access to data at all times. Cybersecurity ensures the security of corporate resources and protects these resources from certain physical threats in the cyber world [2]. The need to educate users about cybersecurity, and recognition in this context, involves engaging relevant stakeholders to educate them about current activities in cyberspace and to protect individuals, organizations, and information devices stored [3]. Cybersecurity awareness is usually organized for a specific audience, considering which communication medium is most effective. Channels for running cybersecurity campaigns include webinars, jingles, flyers, billboards, posters, in-person workshops and conferences [4]. Currently, most organizations use the Internet to conduct transactions, serving as a tool that can contribute to national and socio-economic development. Therefore, increasing the cybersecurity awareness of employees and users is a mandatory requirement. Adopting a cybersecurity policy is one of the standard practices that enable nations to build a secure cyberspace. Above all, the Federal Government of Nigeria has developed cybersecurity policies and strategies to enhance business success in Nigeria through digitization [4].

Types of Cybercrimes

A. Cyber ​​terrorism: A cyber-terrorist can be described as someone who launches attacks against governments and organizations in order to tamper with or gain access to information stored on computers or their networks. B. Malware: Malware is viruses, Trojan horses, worms, and other software that enter your computer without your knowledge. C. drug trafficking: Drug trafficking is another well-known cybercrime. It is a global trade in the cultivation, manufacture, distribution and sale of substances subject to drug bans. D. Cyberstalking: Cyberstalking is essentially using the Internet to repeatedly harass another person. e. Spam/Phishing: Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. F. Fraud - Identity Theft:

Fraud is the criminal act of someone impersonating another person to obtain important information about someone else. G. Logic Bomb: A typical logic bomb tells a computer to execute a set of instructions at a certain date and time or under certain specified conditions. H. Password sniffing:

A password sniffer can monitor all traffic within your network area [5].

Challenges of Cyber Security in Nigeria

There are several Technical challenges facing cybersecurity in Nigeria [6]. Some of them are:

1. The increasing complexity of AI models makes them more difficult to apply and implement in cybersecurity.

2. Successfully develop and implement human-AI collaboration to improve cybersecurity.

3. Developing and improving simple user authentication mechanisms suitable for resource-constrained devices, also known as wearables and IoT biometrics.

4. Privacy remains a major concern when it comes to the design, development and use of biometrics.

5. Cyber ​​forensics for IoT devices and cloud computing is still in its infancy, and there are many issues such as the complexity and diversity of IoT devices, evidence collected in cloud environments as data is distributed across nations and within data centers, etc. I am facing a challenge.

6. This process must be fully automated for successful analysis and detection of major malicious programs.

7. Design, development and implementation of in-cloud malware analysis.

8. Applying machine learning to hardware security faces several challenges. One of the main limitations in applying machine learning to hardware reverse engineering is the lack of extracted features that can be generalized to other chips.

9. Code obfuscation, smart fuzzing, and secure programming languages ​​are some of the challenges facing software security. Next-generation cybersecurity began using innovative technologies to improve detection and response to emerging threats and build a safer society [6].

Further analysis presented in Figure 1(a - d) illustrate the seriousness of the threat.

(a) (b)

(c) (d)

Figure 1: Reconnaissance, Weaponization, Delivery and Exploitation in Nigeria

Table 1 further explains in details the information summarized in the graphs presented in Figure 1. These results are sourced from reports from the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA). This is due to the fact that Nigeria hardly has a well-documented statistic of cybercrime and cybersecurity activities [9].

Table 1: Findings on Reconnaissance, Weaponization, Delivery and Exploitation in Nigeria (FBI, 2021)

|  |  |
| --- | --- |
| Stage | Key Statistics and Insights |
| Reconnaissance | Phishing attacks for information gathering increased by over 70% from July 2021 to June 2022  |
| Business email compromise cases often start with phishing or social engineering for reconnaissance  |
| Nigerian cybercriminals heavily utilize opensource intelligence and social engineering tactics  |
| Weaponization | Malware infections increased by 24% and ransomware increased by 12% in Nigeria in 2021  |
| Nigerian cybercriminals rapidly adopting ransomware, spyware, banking trojans, and other malware  |
| Delivery | Phishing, social engineering, and drive-by downloads were top vectors for malware delivery in Nigeria  |
| Majority of ransomware delivered through phishing emails often impersonating businesses  |
| USB drive infections increased as a delivery method, capitalizing on COVID distancing  |
| Exploitation | Estimated $450 million in annual losses from cybercrime exploitation in Nigeria  |
| Compromised email accounts and credentials were the main vectors to exploit organizations |
| Ransomware payments totaled about $24 million in 2021 in Nigeria  |
| Nigerian banks spent an average of $217 million annually combating cybercrime  |

Multiple sources are also queried to identify the cyberattacks recorded and the financial implications of these attacks and the varying attack vectors utilized and their popularity.

Table 2: Statistics on Cyber Attacks in Nigeria (FBI, 2019; FBI, 2021; SurfShark, 2022; TechTimes, 2022)

FBI highlight an escalating trend of cybercrime in Nigeria, substantiated by key statistical findings. Nigeria stands as the world's third-highest country in terms of cybercrime victims, contributing to about 10% of global victims. The FBI's Internet Crime Complaint Center documented 26,379 complaints from Nigerian victims in 2021, reflecting an alarming 31% surge compared to the previous year, resulting in over $139 million in reported losses, a 48% increase. Business Email Compromise (BEC) schemes, accounting for 54% of Nigeria's reported cybercrime, led to $110 million in losses, positioning Nigeria as the fourth highest country globally for originating BEC attacks. TechTimes also reported an estimated annual cost of $450 million, approximately 0.08% of Nigeria's GDP, while research from Surfshark revealed that Nigeria ranked 16th worldwide in data breaches in 2021, with 61 breaches exposing about 9.7 million records [10]. These statistics collectively underscore a significant and rising cyber threat in Nigeria, with substantial financial implications.

EXISTING MITIGATION METHODS

Examples of these innovative technologies are [6]:

i. Multi-factor authentication is the use of a personal identification number (PIN), biometrics (fingerprint, face, etc.), or a combination of passwords.

ii. analyze the behavior of malicious programs to detect anomalies;

iii. Sandboxing, i.e. creating an isolated and safe environment for testing malicious programs and links.

iv. Forensics. Using scientific methods and expertise to collect and analyze evidence that can be used in criminal or other forensic investigations.

v. Apply artificial intelligence (AI) to improve and solve tough cybersecurity problems.

Reasons why cybercrime is on the rise in Nigeria:

a. Security measures when handling computers are insufficient: The easy life of some people in Nigeria, ignorance of regular security breaches, and carelessness in providing information have left valuable information and devices in the hands of cybercriminals [7].

b. Assign multiple passwords to users: Individuals or organizations send passwords for specific reasons. This can be influenced by trust and the nature of the work. Password sharing by IT professionals has been one of the biggest security concerns. There are two different but very important concerns when it comes to password sharing. The first is sharing a single password across multiple websites or access points [7].  c. Stress-free password prediction: Guessing passwords using Stress-Free is not recommended for security reasons. However, passwords will be the first point of verification for a long time to come. A simple password is the same as no password. Passwords centered around organization owner names, organization names, and organization acronyms are easily guessed by hackers and others [7]. d. Shut down your computer; Computers should be shut down when not in use or when leaving the office. Failure to do so may expose your system to malicious attacks, allowing hackers to take over your computer and put your information into the wrong hands [7]. c. Ignoring Security Programs: This negligence is mainly documented when IT staff trained in computer applications fail to implement security measures [7]. They become familiar with a society that disregards safety measures. d. Social media: Social media has both advantages and disadvantages. Using social media while performing critical tasks exposes company information to hackers [7].

*The Way Forward/Prospects*

In Nigeria, the landscape and scope of cybercrime is changing rapidly, and a new phenomenon called Yahoo Plus is just emerging. Yahoo Plus is an advanced form of Yahoo Yahoo that uses traditional amulets, most commonly body parts, to defraud victims. This Yahoo Plus is widely used by online scammers who cannot get any money from their illegal activities. Young women were the main victims of the embarrassing incident of Yahoo Plus.  Parents no longer bother asking why their kids in higher education, who should be focused on graduating first in class, drive around in the latest cars and have no clear source of income. There are many cases where the parents of these cybercriminals aided their atrocities. Some parents even refer children involved in this crime to an herbalist to help prepare spells that enable the crime.  Cybercrime has caused enormous damage to Nigeria's international reputation, so the intelligence and skills used to carry out this cybercrime should be used in a lawful and appropriate manner that is more beneficial to society. Most law enforcement agencies in Nigeria, including the police, are ill-equipped to deal with online crime due to the complex and complex nature of investigations and the rapid advancement of new technologies. As our society becomes more and more involved in cybercrime, the public expects law enforcement to be up to date with the latest technology to combat all types of cybercrime.

The following suggestions will help Nigeria eliminate the threat of cybercrime and restore Nigeria's tarnished reputation.

i. Job offers:Due to the high rate of youth unemployment in Nigeria, the majority of them turn to cybercriminals for a living. Young people may not feel the need to engage in criminal activity if they have the right jobs and employment opportunities.

ii. Actively apply electronic skills: Another way to fight cybercrime is to teach young people how to use their computer skills for good instead of doing evil, such as scamming people online.

iii. More severe penalties for scammers: Another reason why many young people engage in cybercrime is that they are not fully aware that the punishment for cybercrime is low.

iv. Appropriate cybercrime education: Parents, religious leaders, and institutions of higher education all have a role to play in educating adolescents about the impact of cybercrime. Such behavior should be discouraged through parenting, religious lectures, and academic rules and regulations. Related to the advice above, society as a whole should also contribute to reducing the pressure on young people to get rich young.

Conclusion

In Nigeria, rising unemployment, especially among young people, and a get-rich-quick social motive have made cybercrime rampant. The Nigerian Parliament took a bold step in fighting cybercrime when the Senate passed the Cybercrime Bill. However, the study reveals a solution to combat this crime. Cybercrime should not be underestimated as the obvious conclusion is that hackers are always one step ahead. This gap must be filled. Cybersecurity continues to improve, but today people are more vulnerable than ever. However, Internet users should, of course, only use passwords that are difficult to understand and should not pass them on to third parties. Cybercrime poses a serious threat to cyberspace, the internet and computer systems and requires immediate public action. In Nigeria, unemployment, poverty, decay of social morals and values, peer pressure, and cyber awareness, despite the fact that the “get rich quick syndrome” of Nigerian youth is often attributed to cybercrime. The lack of security, especially lax penalties for cybercrime, also contributes to the unwanted proliferation of cybercrime. Fighting cybercrime requires everyone's participation. All members of society have a responsibility to end the cybercriminal madness that undermines social values. In this regard, most of today's average Nigerian youth believe that internet fraud is the only path to prosperity. Most of these young people no longer feel the need to focus on education or acquire skills.

References

[1] A. A. Garba, & A. M. Bade, “The Current State of Cybersecurity Readiness in Nigeria organizations, Educational Research” (IJMCER), 3(1), 2021, pp. 154-162.

[2] M. G. Pallavi, “A Literature Review of Cyber Security, IJRAR April 2019, Volume 6, Issue 2 www.ijrar.org.

[3] C. A. Moturi, N. R. Abdulrahim, and D. O. Orwa, “Towards adequate cybersecurity risk management in SMEs”, International Journal of Business Continuity and Risk Management, 11(4), 2021, pp. 343-366.

[4] F. E. Ikuero, “Preliminary Review of Cybersecurity Coordination in Nigeria”, Nigerian Journal of Technology (NIJOTECH) Vol. 41, No. 3, May, 2022, pp. 521-526.

[5] M. Olusola, O. Samson, A. Semiu & A. Yinka (2013): Cyber Crimes and Cyber Laws in Nigeria, The International Journal of Engineering and Science, Volume 2, Issue 4, pp. 19-25.

[6] S. Alam, “Cybersecurity: Past, Present and Future. Department of Computer Engineering” Adana Alparsalan Turkes Science and Technology University. pp. 7-15, (2022).

[7] F. Uwadia and, I. F. Eti, “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.

[8] “Federal Bureau of Investigation Internet crime report 2021”. Washington: Internet Crime Complaint Center. Available at: <https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf> (Accessed: 5/6/2023)

[9] “Federal Bureau of Investigation Internet crime report 2019”. Washington: Internet Crime Complaint Center. Available at: <https://pdf.ic3.gov/2019_IC3Report.pdf> (Access: 5/6/2023).

[10] “Surfshark Data Breach Report Data breaches rise globally in Q3 of 2022”. Available at : <https://surfshark.com/blog/data-breach-statistics-2022-q3> (Accessed: 5/6/2023).

[11] TECHTIMES “Online Scams: How to Be Your OWN First Line of Defense”, Issue 02, 2022, Advanced Network Professionals 1103, 38th Avenue West Spencer, IA 51301

712-584- September 2022.