REGULATORY FRAMEWORK ON CYBERSECURITY IN NIGERIA

Chiamaka I. Owuamanam *

Abstract

The evolving digital age has raised worldwide concern for cybersecurity and Nigeria is no exception. The need for cybersecurity arose with the advent of the internet in Nigeria with different sectors of the economy rapidly embracing digitalization. The consequential result of this progress is the increased vulnerability to cyber threats. However, there were no clear steps in the area of cybersecurity, policies or regulatory framework until 2003. This was not until a murder incident at a Nigerian embassy in 2003, which was connected to an Internet crime. A 72-year-old Czech, who was a victim of an email scam purportedly by a Nigerian, shot the late Nigerian diplomat Michael Lekara Wayid at the Nigerian Embassy in Prague. This incident exposed the critical need for a cybersecurity framework to ensure the safety of citizens, businesses and foreigners who interact in the cyberspace. The journey toward the developing of a robust legal framework for cybersecurity in Nigeria, reflects a gradual recognition of the need to address the risks posed by cyber threats and crimes. This paper attempts to provide an overview on the regulatory framework on cybersecurity in Nigeria[1]. This includes both legal and institutional frameworks. This also examines an evolution of cybersecurity policies in Nigeria using the doctrinal approach, to highlight key milestones and legislative development, while providing further recommendations for a safer cyberspace.

KEYWORDS – Cybersecurity, Crime, Economic and Financial Crimes Commission, Internet, Technology.

1. INTRODUCTION

The world is witnessing a rapid advancement in the use of technology and there is a growing reliance on digital system, these have consequently resulted in a global transformation of societies and economies. In Nigeria, there are visible gains brought about by this digital revolution, these include improved communication, financial inclusion, enhanced public service delivery and effective data storage. As one of Africa's largest digital economies, the country has witnessed a significant increase in the adoption of digital platforms for commerce, communication and governance. However, the advent of technology and digitalization also created nerve-racking issues of cybersecurity threats like hacking, cyber fraud, data breaches and identity theft. Having

***Chiamaka I. Owuamanam**, LL.B, B.L, Legal Associate, Aderemi Olatubora And Co, House A4, Apex Garden Estate, Kukwaba District Abuja; owuamanam.amaka@gmail.com; +2348160222786.

[1] In 2015, there was a turning point in Nigeria's cybersecurity legal framework with the enactment of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, by the National Assembly

recognized the economic and social implications of these threats, steps have been taken to establish legal and institutional frameworks to address cybersecurity issues in Nigeria. The regulatory framework for cybersecurity in Nigeria is not only important for safeguarding the nation's critical information infrastructure but also for fostering trust in its digital economy. This is to ensure economic growth, national security, protection of the rights of citizens and data privacy.

This study examines the regulatory framework of cybersecurity in Nigeria, it traces the evolution of cybersecurity laws, assessing its effectiveness and identifying gaps that ought to be addressed; with the objective of providing and understanding of how Nigeria is navigating the complexities of cybersecurity governance.

2. EVOLUTION OF CYBERSECURITY LAW AND POLICY IN NIGERIA

Prior to the mid-1990s which heralded the advent of internet in Nigeria, the laws at that time were focused on traditional crimes, with no consideration for crimes committed through digital or electronic means. Criminal activities like fraud, theft and impersonation were covered under the Criminal Code Act[2] and Penal Code Act[3][4]. With the birth of the internet in Nigeria which opened door to the problems of cyberfraud, hacking, identity theft and majorly advance fee fraud scams(419), which gained international notoriety, casting a shadow on Nigeria's global reputation; it became glaring that general fraud provisions in the existing laws and the legal system were inadequate to handle the complexities of cybercrimes.

A step towards a panacea for cybercrimes was the passing of the Economic Financial Crimes Commission Act 2002 which established the Economic Financial Crimes Commission(EFCC). However, the focus of the EFCC was primarily on financial crimes which included financial crimes perpetrated through the internet, which are internet-related fraud, particularly money laundering involving electronic transactions.

[2] Criminal Code Act Cap C38 Laws of the Federation 2004, sections 418 -439(fraud), sections 382 – 400 (stealing), sections 467 -489 (forgery and personation).
[3] The Penal Code (Northern States) Federal Provisions Act, sections 320 – 325 (cheating and personation), sections 286 – 290 (theft).

The first major action in the regulation of cybercrimes in Nigeria was with the setting up of a National Cyber security Initiative (NCI) in 2003 by the then President of Nigeria, Chief Olusegun Obasanjo (GCFR). To achieve the objectives of the National Cyber Security Initiative, in addition, the Nigeria Cybercrime Working Group (NCWG) was also formally constituted on 31st March 2004 with the mandate of examining all associated problems of cyber criminality in Nigeria and make appropriate submissions to government on how to curb it.

The membership of the Nigeria Cybercrime Working Group (NCWG) was drawn from all the critical law enforcement, security, intelligence, and ICT agencies of the government. The group also included major organized private ICT sector stakeholders as members. The effort of the group worked out a foundation for cybercrime law in Nigeria with the development of the draft Cybercrime Bill. The Bill proposed a substantive law that would criminalize the following kinds of conduct: (i) Conducts against information and communication technology (ICT) system, (ii) Conducts using ICT systems as tools for committing crime, and (iii) Legally prohibited conducts that have essential ICT infrastructures as targets. It also proposed some procedural provisions that deal with investigation of crime, collection of evidence relating to cybercrime as well as procedures for searches, seizures and interception of digital communication. Furthermore, the proposed Bill suggested the following: (i) promote and develop specialized units to deal specifically with ICT offences, as units of existing law enforcement formations, (ii) facilitate cooperation between industry and law enforcement agencies, (iii) create an advanced ICT centre to collect, collate, analyze, and circulate relevant technical information to and for other relevant Agencies, and (iv) if need be, create an entirely new cybercrime and cyber security agency at par with other specialized agencies like EFCC, NDLEA, ICPC and NAFDAC.

Subsequently, in 2006, the Federal Government through the Office of the National Security Adviser created the Directorate of Cybersecurity to uphold the work of NCWG and coordinate cybersecurity activities in the country.[5] In this regard, the job description of the Directorate of Cybersecurity was to implement the objectives of NCI which include establishment and development a framework for National Computer Emergency Response Team; establishment and collaboration with Computer Emergency Response Teams globally; establishment of a National

[5] H O Quarshie and A Martin-Odoom, 'Fighting cybercrime in Africa' [2012] 2(6) *Computer Science and Engineering*, 98-100.

Digital Forensic Laboratory; coordinating the training of Security and Law Enforcement Agencies in Nigeria and their utilization of the facility; Conduct sensitization campaign for Non-Governmental Organizations; Sponsor passage of the Computer Security and Critical Information Infrastructure Protection Bill in Nigeria's National Assembly.[6]

In 2015, there was a turning point in Nigeria's cybersecurity legal framework with the enactment of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, by the National Assembly. The objectives of the Act include to provide an effective regulatory and institutional framework for preventing cybercrimes in Nigeria, ensure the protection of Critical National Information Infrastructure and promote cybersecurity Promote the protection of computer systems.

Nigeria also has its national cybersecurity policy and strategy. The National Cybersecurity Policy and Strategy was initially developed in 2014, and reviewed in 2021 in line with *Section 41(1b)* of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015. The policy document is intended to ensure the formulation and effective implementation of an all-inclusive cybersecurity framework for Nigeria. The National Cybersecurity Policy and Strategy provides a roadmap and action plan for enhancing Nigeria's security posture in cyberspace.[7]

3. LEGAL FRAMEWORK ON CYBERSECURITY IN NIGERIA

3.1 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

The Cybercrimes (Prohibition, Prevention, Etc.) Act was signed into law on May 15, 2015. The objective of the Act include: - (i) To provide an effective and unified legal regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. (ii) To ensure the protection of critical national information on infrastructure and (iii) promote cyber security and the protection of computer system and networks, electronic communication data and computer programs, intellectual property and privacy rights. [8] The Act criminalizes certain acts and omissions, provides best practices and provision of procedural guidelines for the investigation of such offenses. The Act also provides punishment for all kinds of computer related fraud, computer related forgery, cyber pornography, cyber –stalking

[6] *ibid.*
[7] *ibid.*
[8] *Section* 1 Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015

and cyber-squatting. More so, the Act gives the President the power on the recommendation of the National Security Officer to designate certain computer systems, networks and information infrastructure vital to the national or economic security of Nigeria or the economic and public health and safety of its citizens as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furthermore of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.[9] The major highlights are as follows:

i. It creates of child pornography offences, with 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.[10]

ii. It outlaws Cyber-stalking and Cyber-bullying and prescribes punishment ranging from a fine to terms of imprisonment depending on the severity of the offence.[11]

iii. It 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 fine of not less than N5 million or to both fine and imprisonment.[12]

iv. It forbids the distribution of racist and xenophobic material to the public through a computer system or network (e.g. Facebook and Twitter), it also prohibits the use of threats or violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. 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.[13]

[9] *ibid*, s 3
[10] *ibid,* s. 23
[11] *ibid*, s. 24.
[12] *ibid*, s. 25
[13] *ibid*, s. 26.

v. The Act penalizes all forms of electronic card related fraud[14], manipulation of ATM/POS terminals[15], use of fraudulent device or attached emails and websites[16], phishing, spamming and spreading of computer viruses[17]

vi. The Act provides for the duties of service providers. It 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.[18] It also provides the duties of financial institutions.[19]

vii. The Act 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.

vii. The Act establishes the Cybercrime Advisory Council to advise the government on cybercrime policy and the office of the National Security Adviser(ONSA) as the coordinating agency for cybersecurity initiatives.[20]

The *Cybercrimes (Prohibition, Prevention, Etc.) Act* provides a significant impact on the Nigeria cyber space, by serving as a deterrent against cybercrime, encouraging businesses to prioritize cybersecurity and boots confidence in Nigeria's digital economy.

3.1.1 Criticism of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

The *Cybercrimes (Prohibition, Prevention, Etc.) Act* 2015 has been a subject of criticism by digital rights advocates, legal expert, journalists and civil societies. The criticism border on restriction of right to freedom of expression, potential abuse by government authority, vague and generic provisions, and so on.[21] The provision of *section 24* of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 which creates the offence of cyberstalking, is argued to be vague, too subjective

[14] *ibid, s. 33*
[15] *ibid, s. 30*
[16] *ibid, s. 36*
[17] *ibid, s. 32*
[18] *ibid, s. 38.*
[19] *ibid, s. 37.*
[20] *ibid, ss*. 42 and 43.
[21] EFG, Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' [2016], 6(1) *Journal of International and Information System* 1 -12.

and thereby giving room for abuse and misinterpretation by authorities. This section criminalizes the use of a computer system to send messages considered "grossly offensive," "obscene," or that "cause annoyance, inconvenience, or anxiety". It is opined that this provision has been used to stifle the voice of activists, journalists, and dissenting voices, online activism and legitimate criticism of public officials could be unfairly targeted, thereby raising concerns about its impact on freedom of expression.

The issue of the abuse of fundamental human rights, is not only limited to the possible infringement of right to freedom of expression, there are concerns that the right to privacy may be affected by the provision that gives authority for the interception of electronic communication. This is because there are no checks and balances to prevent abuse of the extant provision by authorities. Furthermore, the Act focuses on punishment over prevention of crime. A more balanced approach involving education and proactive measures is needed to foster a cyber-aware society.[22]

3.2 The Economic and Financial Crime Commission Act, 2004

The *Economic and Financial Crime Commission Act*, *2004* provides the legal framework for the establishment of the Commission and protection of economic and financial crimes. Some of the major responsibilities of the Commission in relation to the prevention to cybersecurity and punishment for cybercrimes include; the investigation of all financial crimes, including advanced fee fraud money laundering, counterfeiting, illegal charge, transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam among others; the coordination and enforcement of all laws against economic and financial crimes with a view to identifying individual, corporate bodies, or groups involved; the coordination of all investigating units for existing economic and financial crimes, in Nigeria.[23] The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1994; *The Failed Bank (Recovery of Debts) and Financial Malpractices in Banks Act 1994*, as amended; *The Banks and other financial institution Act* 1991, as amended, and miscellaneous offences Act and any other law or regulation relating to economic and financial crimes, including the *Criminal Code* and *Penal Code*.[24]

[22] *ibid.*
[23] Economic and Financial Crimes Commission (Establishment) Act 2004, s. 6
[24] *ibid*, s.7

3.3 The Criminal Code Act 1990

Although cyber crime is not mentioned in the *Criminal Code, the Criminal Code Act of* 1990 criminalizes any type of stealing of funds in whatever form. The specific provision relating to cybercrime in *the Criminal Code* is *section 419* which is covered under *Chapter 38* of the Act, which deals with obtaining property by false pretenses or cheating. *Section 418* gave a definition of what constitute an offence under the Act. *Section 418* states that any representation made by words, writing or conduct of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence. *Section 419* states that any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

3.4 Nigerian Data Protection Act 2023

The *Nigeria Data Protection Act 2023* establishes the legal framework for the regulation, processing and protection of personal data in Nigeria. The Act replaces the Nigerian Data Protection Regulations (NDPR).[25] *Section 40(2)* of the *Nigerian Data Protection Act* requires data controllers or possessors, within 72 hours of becoming aware of a data breach incident, to notify the Nigeria Data Protection Agency of such breach.

3.5 National Cybersecurity Policy

The *National Cybersecurity Policy* was launched in 2014 by the Office of the National Security Adviser due to the overwhelming activities of cybercrime perpetrators and the increasing Nigerian cybercrime statistics. The 2014 version of the *National Cybersecurity Policy* and Strategy was further reviewed in 2021. This policy is a vital response element for safeguarding the nation. It helps to enlighten the citizens on the components that are to be used to empower the nation to understand, respond and collectively deter cyber threat activities. Five key cyber threats have been identified and listed as posing significant challenges to Nigeria and inimical to national growth

[25] KPMG 'Nigeria Data Protection Act Review' <https://assets.kpmg.com> accessed 23 November 2024.

and security. They are: a) Cybercrime b) Cyber-espionage c) Cyber conflict d) Cyber-Terrorism e) Child Online Abuse & Exploitation.[26]

3.6Central Bank of Nigeria Guidelines and Frameworks

The Central Bank of Nigeria (CBN) issued the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions This was issued in furtherance of the CBN's commitment to ensure the security of the banking sector. The Framework contains cybersecurity programs and mechanisms designed to combat modern cyberattacks that financial institutions face.

The Framework provides the minimum level of cybersecurity for all Other Financial Institutions (OFIs). Under the Bank and Other Financial Institutions Act 2020 (BOFIA), OFIs are defined to include all Discount Houses, Bureau de Change, Credit Bureau, Finance Companies or Money Brokerage, International Money Transfer Services, Mortgage Refinance Companies, Mortgage Guarantee Companies, Credit Guarantee Companies, Financial Holding Companies. It is pertinent to note that though the BOFIA defined Payment Service Providers **(**PSPs) as OFIs, it appears that PSPs are not covered by this Framework. PSPs are, however, regulated under the 2018 CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. The framework provides the following:

1. OFIs are required to establish cybersecurity governance which includes: a. ensuring cybersecurity is a standing agenda in the Board meetings and Senior Management meetings of all OFIs; b. ensuring a quarterly report on the cybersecurity status of the OFI is prepared by the Senior Management and reviewed by the Board of Directors; c. preparing a cybersecurity framework which will be submitted to the Director of Other Financial Institutions Supervision Department of the CBN (the "**Director**").[27]

2. *Appointment of a Chief Information Security Officer (CISO)*: Every OFI is required to appoint a CISO who shall be primarily responsible for the day-to-day cybersecurity

[26] *Article* 1.2 *National Cybersecurity Policy* 2014.
[27] *Article* 2.1 – 2.5 of the *Risk-Based Cybersecurity Framework and Guidelines* for other Financial Institutions 2022

activities. However, for small OFIs such as Unit Tier 2 MFBs, the head of IT or a part-time consultant may be appointed as the CISO.[28]

3. *Establishment of an Information Security Steering Committee (ISSC):* All OFIs with over 30 employees are required to establish an ISSC responsible for enforcing policies developed to manage cybersecurity risks in the organisation. For OFIs with less than 30 employees, the responsibility of the ISSC can be carried out by a relevant management committee provided that the CISO shall be a member and shall lead all cybersecurity issues.[29]

4. *Implementing a Cybersecurity Risk Management System:* Each OFI is required to implement a cybersecurity risk management system based on the threats, vulnerability and tolerance of the OFI.[30]

5. *Resilience Assessment and Internal Audits*: OFIs are required to conduct regular Cybersecurity Resilience assessments and internal audits to mitigate the risk exposure and ascertain the adequacy of the cybersecurity measures in place.[31]

6. *Returns to the CBN*: A report of the cybersecurity self-assessment signed by the CISCO shall be submitted every year on or before March 31 to the Director. OFIs are also required to promptly report all potential cyber-threats to their information assets, to the Director.[32]

7. *Compliance with other CBN Guidelines*: OFIs are to ensure compliance with all other CBN directives and all relevant laws including the Cybercrimes (Prohibition, Prevention etc) Act 2015.

Earlier in 2018, the CBN had released Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs). This has similar provisions with the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions

[28] *Article 2.6-2.7 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*
[29] *Article 2.8 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*
[30] *Article 2.9 - 3 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*
[31] *Article 4 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*
[32] *Article 4.3 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*

2022. In Appendix IV of the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs), provides the minimum controls required for DMB./PSP to continue to support and provide business services even in the event of cyberattack. It provides controls on access right management, secure system configuration, cybersecurity awareness, data loss prevention, system life cycle management, vulnerability management, continuous security monitoring, and enhancing incident response capabilities.[33]

4. INSTITUTIONAL FAMEWORK FOR CYBERSECURITY IN NIGERIA

4.1 National Information Technology Development Agency (NITDA)

National Information Technology Development Agency (NITDA) was created in April 2001 to implement the Nigerian Information Technology Policy and co-ordinate general IT development in the country. The National Information Technology Development Act 2007 mandate the Agency to create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria.

NITDA has a cyber security department which has the objective to ensure effective regulation of the sector through development of standards and guidelines to enhance Nigeria's cybersecurity resilience; enlighten all Nigerians on what to do and avoid while in cyberspace; ensure that Nigeria has mechanisms for building enormous human capacity to defend our cyberspace and perform offensive operations when necessary; ensure that Nigeria's rating in international indices is improve. The functions of the cybersecurity department are; to track local and global cyber activities/programmes/incidences/research, analyze and share findings and mitigations with Nigerians; to develop policies and guidelines on how to identify, protect, respond and recover from threats in cyber space, particularly as it affects MDAs; to institute mechanisms for monitoring compliance with such guidelines; coordinate nationwide participation to realize national strategy

[33] *Appendix IV* of the *Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers 2018*[33] *Article 4 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*
[33] *Article 4.3 of the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022*
[33] *Appendix IV of the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers 2018*

and cybersecurity objectives; facilitate the establishment of a national PKI with internal structure and governance mechanisms to ensure effectiveness of a dependable trust chain for online transactions; conduct studies to decipher global direction of cyber activities and knowledge requirements, and provide the enabling environment for active participation of all, to produce a constant stream of quality manpower for servicing internal needs and exporting skilled human capacity; develop framework for institutional capacity for professional skills development and align it with certification authorities globally, and broker alliances with local vendors for mutual benefits; keep track of such capacity in a national database and repository where needy agencies could access it; conduct research into risks and opportunities inherent in the business landscape of the Agency; and formulate guidelines on Business continuity for MDAs and businesses, including recovery mechanisms so as to forestall service outages.

4.2 Nigerian Computer Emergency Response Team (ngCERT)

Nigerian Computer Emergency Response Team (ngCERT) has a mission to achieve a safe, secure and resilient cyberspace in Nigeria that provides opportunities for national prosperity. ngCERT serves as the Coordination Centre responsible for managing cyber incidents in Nigeria as provided for in *Section 42 (c)* of Cybercrime Act, 2015. ngCERT is created to prepare, protect, and secure the Nigerian cyberspace in anticipation of attacks, problems, or events. ngCERT is saddled with the responsibility of reducing the volume of future incidents. The Proactive service of ngCERT is carried out to help prepare, protect, and secure the Nigerian cyberspace in anticipation of attacks, problems, or events. These services will directly assist ngCERT to reduce the volume of future incidents. The services include: Technology Watch which the ngCERT does by monitoring and observing new technical developments in Information Technology, intruder activities and related trends to help identify future threats; Intrusion Detection Services which the ngCERT does by monitoring IDS of organizations that host information systems that are considered Critical National Information Infrastructure(CNII) to the Nigerian Government. It also reviews existing IDS logs and analyse in order to initiate a response for any events that meet ngCERT specified threshold; Vulnerability Assessment and Penetration testing which is one of ngCERT's on-demand services, perform to protect information systems that are considered Critical National Information Infrastructure(CNII) which may be owned by either public or private sectors of Nigeria. This service is designed to properly secure such information

systems; Announcements by ngCERT include but not limited to intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools.

In 23rd June 2024, the ngCERT issued an urgent security advisory regarding a critical vulnerability within Microsoft Windows Wi-Fi drivers, designated as **CVE-2024-30078**. This severe Remote Code Execution (RCE) flaw affects all current Microsoft Windows versions, with particular emphasis on Windows 10 and 11. An attacker, without requiring authentication, can exploit this vulnerability by transmitting a malicious network message to a vulnerable Wi-Fi driver, leading to arbitrary code execution on the target system. This may result in unauthorized malware installation, complete system compromise, and the potential theft or manipulation of sensitive information. Users were strongly advised to implement the latest security updates from Microsoft, addressing this critical issue.[34]

4.3 Nigeria Data Protection Commission (NDPC)

Under *section* 40(2) of the Nigerian Data Protection Act requires data controllers or possessors, within 72 hours of becoming aware of a data breach incident, to notify the Nigeria Data Protection Agency of such breach. Where a data controller or processor is in breach after conclusive investigations, the NDPC may issue a compliance and/or enforcement order in line with the National Data Protection Act to curtail the breach. Such orders may include: payment of monetary damages; revocation of regulator-issued operational licences; closure of business operations; ordering the data controller or data processor to account for the profits realized from the violation; and issue public notice to warn the public to desist from patronizing or doing business with the affected party. In January 2023, the NDPC's head of legal enforcement revealed it was carrying out investigation into some Nigerian banks for data breaches involving alleged unauthorized disclosure, access and processing of personal banking records.

4.4 Office of the National Security Adviser

The Office of the National Security Adviser is responsible for the leadership, management and

[34] Available at <https://csirt.ncc.gov.ng/index.php/resources/security-advisories> accessed 15th October 2024

capacity development of the security architecture of the Country. *Section 41 (1) (b)* of the *Cybercrime (Prohibition, Prevention, etc) Act, 2015* mandates the Office of the National Security Adviser (ONSA) to "ensure formulation and effective implementation of a comprehensive National Cybersecurity Strategy and a National Cybersecurity Policy for Nigeria". *Section 41* of *the Cybercrimes Act 2015* provides the responsibilities of the Office of the National Security Adviser as follows: (a) provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria; (b) ensure formulation and effective implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria; (c) establish and maintain a National Computer Emergency Response Team (CERT) Coordination Center responsible for managing cyber incidences in Nigeria; (d) establish and maintain a National Computer Forensic Laboratory and coordinate utilization of the facility by all law enforcement, security and intelligence agencies; (e) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria; (f) establish appropriate platforms for public private partnership (PPP); (g) coordinate Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into the global frameworks on cyber security; and (h) do such other acts or things that are necessary for the effective performance of Co-ordination and enforcement. the functions of the relevant security and enforcement agencies under this Act.

The ONSA has the power to intercept electronic communications in order to prevent or mitigate the impact of cyber-attacks. *Section 4* of the *NCC's Lawful Interception of Communications Regulations 2019*, makes it lawful for any authorized Agency(such as the office of the National Security Adviser) to intercept any communication, pursuant to any legislation in force, where: (a) the interception relates to the use of a communications service provided by a Communications Licensee to persons in Nigeria; (b) the interception relates to the use of a communications service provided by a Communications Licensee to a person outside Nigeria, provided that the licensee shall not be liable in any civil or criminal proceedings for damages, including punitive damages, loss, cost or expenditure suffered or to be suffered, either directly or indirectly, for any act or omission done in good faith in the performance of a duty imposed under paragraphs (a) or (b) of this regulation.

4.5 National Communications Commission (NCC)

In alignment with its mandate to ensure a secure cyberspace that is safe for operators and consumers of communications services and infrastructure in Nigeria,[35]the Nigerian Communications Commission (NCC) employs a multifaceted approach to address the evolving challenges of cybersecurity in Nigeria. This approach involves both reactive measures proactive strategies channeled towards anticipating and mitigating emerging threats. By fostering a culture of continuous improvement and innovation, the NCC seeks to stay ahead of cyber adversaries and minimize potential disruptions to the country's communications infrastructure. The NCC also recognizes the importance of public-private partnerships in strengthening cybersecurity governance and fostering collective resilience. Through collaborative initiatives with industry stakeholders, including telecommunications operators, internet service providers, and technology companies, the NCC promotes information sharing, capacity building, and joint initiatives to combat cyber threats. By leveraging the expertise and resources of both public and private sectors, the NCC aims to create a coordinated and cohesive cybersecurity ecosystem that can effectively respond to and mitigate cyber risks. Through these collaborative efforts, the NCC endeavors to uphold its mandate of ensuring a secure and trusted cyberspace for all stakeholders in Nigeria's communications sector.[36]

The NCC set up a cybersecurity unit, the NCC Computer Security Incidence Response Team (CSIRT), which is tasked with the responsibility of releasing periodic information/publications warning the public against certain corrupted software utilized by cybercriminals to perpetrate fraud. This information can be found on the NCC website.[37]

4.6 Central Bank of Nigeria

The Central Bank of Nigeria regulates the banking sector in Nigeria. Beyond regulating payments companies and banks, it is important to maintain security standards, in accordance with international best practices, with all the other players in the ecosystem including other financial institutions. This is to prevent targeted attacks at these bodies that may compromise the whole

[35] 'CybeSecurity'<https://ncc.gov.ng/technical-regulation/Cybersecurity#projects-activities-3> accessed 25 November 2024.
[36] *ibid*
[37] 'National Communications Commission' <https://csirt.ncc.gov.ng/index.php/resources/security-advisories> accessed 25 November 2024.

ecosystem or adversely impact the interests of the end-users, consumers and customers of these institutions and the ecosystem at large. As part of its regulatory function, on June 29, 2022, the Central Bank of Nigeria (CBN) issued the *Risk-Based Cybersecurity Framework and Guidelines* for Other Financial Institutions (the Framework). This was issued in furtherance of the CBN's commitment to ensure the security of the banking sector.

Earlier in 2018, the CBN had released Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs). This has similar provisions with the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions 2022. In Appendix IV of the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs), provides the minimum controls required for DMB/PSP to continue to support and provide business services even in the event of cyberattack. It provides controls on access right management, secure system configuration, cybersecurity awareness, data loss prevention, system life cycle management, vulnerability management, continuous security monitoring, and enhancing incident response capabilities.[38]

4.7 Attorney General of the Federation

Section 41(2) of the *Cybercrime (Prohibition, Prevention, etc) Act, 2015* provides that the Attorney – General of the Federation shall strengthen and enhance the existing legal framework to ensure – (a) conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards; (b) maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and (c) effective prosecution of cybercrimes and cyber security matters. (3) All law enforcement, security and intelligence agencies shall develop requisite institutional capacity for the effective implementation of the provisions of this Act and shall in collaboration with the Office of the National Security Adviser, initiate, develop or organize training programmers nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.

[38] *Appendix IV of the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers 2018*

5. Recommendations

It does not only stop at enacting laws and creation of institutional bodies to prevent cybersecurity, there is a need to educate citizens on the continual maintenance and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. 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. It is recommended that programs and Information Technology forums be established for Nigerian youths in order to create employment which has contributed significantly to the spate of internet related crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where young persons could come together and display their skills. This can be used meaningfully towards developing Information Technology in Nigeria at the same time they could be rewarded handsomely for such novelty.

IP Address tracking software that could track the IP address of orders is recommended. This software can be applied to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders. Cryptography is also recommended as a way of curbing cyberthreats. Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. A number of cryptographic methods have been developed and some of them are still not cracked.

Antivirus, anti-spyware software and firewalls are also recommended. Antivirus software consist of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer. A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.