ADAPTING TO CHANGE: THE IMPACT AND CHALLENGES OF CYBERCRIME IN NIGERIA AND THE WAY FORWARD

INTRODUCTION

In today's interconnected world, where digital technologies infiltrate every aspect of society, the importance of cybersecurity cannot be overstated. From personal data protection to national security, the integrity of digital systems is paramount. In Nigeria, like many other countries, the rapid evolution of technology has brought about unprecedented opportunities and new challenges. As the nation increasingly relies on digital infrastructure for communication, commerce, and governance, the threat landscape has become more complex and diverse.

With significant growth in internet penetration and mobile phone usage, Nigeria has witnessed increased digital connectivity, fostering economic development and social interaction. However, alongside this growth comes a rise in cyber threats, ranging from hacking, cyber stalking, phishing attacks, insider threats, social engineering, supply chain attacks, data breaches and ransomware incidents, all targeting individuals, businesses, and government agencies alike. While Nigeria has taken legislative steps to address cyber threats through laws such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, gaps remain in the legal framework, necessitating further improvements and a pressing need to fortify its legal framework to address emerging cyber threats effectively.

Existing Cybersecurity Laws in Nigeria

Prior to the enactment of the Cybercrime (Prohibition, Prevention etc.) Act in 2015, in 2014, the National Cybersecurity Policy (“the Policy”) and the National Cybersecurity Strategy (“the Strategy”) were issued by the Office of the National Security Adviser (“ONSA”). The Policy was issued to facilitate an effective legal framework and governance mechanism for Nigeria's presence in the cyberspace as well as to develop an information security and control mechanism for the protection and safety of Nigeria's national Critical Information Infrastructure (“CII”) and the Strategy comprises of short, medium, and long-term strategies aimed at addressing Nigeria's cyber-risk exposure.

Shortly after the issuance of the Policy and the Strategy, in 2015, the Cybercrime (Prohibition, Prevention etc.) Act 2015 was enacted. It expanded on the Strategy & policy which now includes the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights, including the retention of records and protection of personal data.

The National Data Protection Act (NDPA) was also introduced in June 2023, establishing the Nigeria Data Protection Commission (NDPC) as the country's independent data protection authority. The legislation expands the scope of personal data coverage while recognizing legitimate interest as a basis for processing data. Major organizations must register with the NDPC, which has the power to enforce compliance through regulations, approved international data transfer codes, and fines within prescribed limits.

IMPACT OF CYBERCRIME ON INDIVIDUALS, BUSINESSES AND NATIONAL SECURITY

Impact on Individuals

Cyberattacks can result in the theft of personal information, including bank account details, social security numbers, and credit card information. This stolen data is often used by cybercriminals to commit identity theft and financial fraud, leading to unauthorized transactions, drained bank accounts, and damaged credit scores. Individuals may suffer from the loss of personal data, such as photos, emails, and documents, due to data breaches or ransomware attacks and as a result, they may experience reputational damage.

Also, cyberattacks can have profound psychological effects on individuals, causing stress, anxiety, and emotional trauma. Victims may experience feelings of violation, helplessness, and fear, impacting their mental well-being and overall quality of life. Recently at a hearing which held on January 31, 2024, the CEOs of Meta, X (formerly Twitter), Snap, Discord, and TikTok testified before the US Senate Judiciary Committee regarding online child safety. The hearing addressed concerns about the role of social media platforms in protecting minors from online threats such as child sexual exploitation and the CEOs were made to apologize to families of children who had lost their lives due to the inadequacy of such protective structures. Also, In August 2019, Business Day reported that the Nigerian Yellow Card website was hacked wherein personal and sensitive data was leaked. The website contained sensitive health information for Nigerian air travellers who had been vaccinated against Yellow Fever.

Impact on Businesses

Ransomware attacks can result in significant financial losses for businesses, both directly through ransom payments and indirectly through business disruption and downtime. Data breaches and cybersecurity incidents can tarnish a company's reputation and erode customer trust. Negative publicity, media scrutiny, and public perception of inadequate security measures can discourage customers and damage long-term relationships with stakeholders.

Businesses may face legal and regulatory repercussions following cybersecurity incidents. This can lead to fines, penalties, lawsuits, and regulatory sanctions, further exacerbating financial losses and reputational damage. An example of where cybercrime had impact on a business is, in January 2022, where the Nigerian Police Force (NPF) arrested 11 alleged members of a prolific cybercrime network as part of a national police operation coordinated with INTERPOL. Upon their arrest by officers of the NPF Cybercrime Police Unit, many of the suspects were thought to be members of 'SilverTerrier', a network known for Business Email Compromise (BEC) which have financially scammed thousands of companies globally. Also, in May 2022, barely days after launching in Nigeria, MoMo Payment Service Bank suffered a breach that reportedly led to $53 million in losses following 700,000 unauthorized transfers to about 8,000 accounts in 18 Nigerian commercial banks. The company said it stopped the transfers after noticing them on May 25th, leading to a temporary service suspension that was eased within 24 hours.

Impact on National Security

Cyberattacks targeting critical infrastructure, such as power grids, transportation systems, and healthcare facilities, can disrupt essential services and threaten public safety. This can lead to widespread chaos, economic losses, and social unrest. Breaches of government systems and theft of sensitive information pose significant risks to national security. Access to classified data, intelligence reports, and military secrets can be exploited by adversaries to undermine national interests and security.

Cyberattacks carried out by state-sponsored actors or hacktivist groups can pose threats to national sovereignty and geopolitical stability. Disruption of government operations, manipulation of public opinion, and interference in elections can have far-reaching consequences for political stability and international relations. For instance, in 2019, the Lagos Internal Revenue Service (LIRS) was accused of exposing personal data online through its web portal and was fined ₦1 million Naira by NITDA.

SOME OF THE CHALLENGES AFFECTING THE IMPLEMENTATION OF THE CYBERCRIME ACT

Absence of collaboration between private sectors and the Nigerian Government

The Cybercrime Act mostly contains punitive measures, such as investigations, lawsuits, and imprisonments/fines. While those considerations surely are an important component, the federal government has failed to take proactive steps to work with companies to improve cybersecurity throughout the public and private sectors. Such collaboration is particularly necessary and common in cybersecurity because public and private cyber infrastructure often is interconnected.[1] For instance, in the United States, after years of heated debate, Congress in late 2015 passed, and President Obama signed, the Cybersecurity Act of 2015. The Cybersecurity Act has a number of components, including the affirmation of companies' ability to monitor and defend their networks. This law created a greatly expanded platform by which private companies and the government can exchange information about cyber-threat indicators and defensive measures.[2]

Difficulty in prosecution and law enforcement

The challenge in prosecuting cases of cybercrimes usually emanate from the identification of a cybercrime perpetrator. Dr. Yakubu Makeri[3] stated that a hostile party using an internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is therefore often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national and international boundaries is problematic.

[1] Jeff Kosseff, 'Cybersecurity Law' (2020) © John Wiley & Sons, Inc., xxvi.

[2] Jeff Kosseff, 'Cybersecurity Law' (2020) DHS Information Sharing, 273.

[3] Dr. Yakubu Ajiji Makeri, Cyber Security Issues in Nigeria and Challenges, Makeri International Journal of Advanced Research in Computer Science and Software Engineering 7(4), April- 2017, pp. 315-321.

Gaps in addressing emerging and evolving Cyber Threats

The Cybercrime Act provides for electronic communication which includes communications in electronic format, instant messages, short message service (SMS), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager. This provision does not consider the present forms of communication available and the constantly emerging technologies. Additionally new technologies have created new concepts which currently, have no legal equivalence or standing.

Lack of National Functional Databases

National Functional Databases could serve as a means of tracking down the perpetuators of these heinous acts by checking into individual records and tracing their movements, however such central databases do not exist now, making such tracking almost impossible.

Examples Of Cybercrime Cases in Nigeria

Notwithstanding the above, there have been a few cases instituted under the Cybercrime Act in Nigeria, some of those cases include:

Julius v FRN (2021) LPELR -54201 (CA)

The case is about an appeal against the judgment of the Federal High Court in Nigeria, where the defendant was convicted and sentenced under the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. The defendant was charged with seven counts of offenses related to computer forgery, fraud, cyberstalking, cybersquatting, racism, and xenophobia. The trial court found the defendant guilty of disseminating unverified information on his Facebook page with the intent to deceive the public and cause mayhem in the state. The defendant was sentenced to three years imprisonment or a fine of ₦7,000,000.00. The court adopted the lone issue of the respondent, which was whether the trial court rightly convicted and sentenced the appellant under the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. The court upheld the decision of the trial court.

IYEN v FRN (2018) LPELR – 49863 (CA)

This appeal borders on the Offences of Conspiracy, Forgery and Cybercrimes. The offence in issue here was a cyber fraud which was committed through the use of a computer, portals and website addresses or internet generally. The Appellant got involved in advertising the sale of United States Postal Money Order through an internet website known as Carder Portal.

The Appellant used the screen name of "Nosa2" on a dedicated IP address. The American USPIS (United States Postal Inspection Service) had picked the advertisement and took a screenshot of it and sent it to an Officer of the EFCC- Ahmed Sa'ad Abubakar on the 10th of February 2006. Then an undercover operation was initiated where an agent of the USPIS office in response to the advertisement, placed an order to purchase from the Appellant, he swallowed the bait and $1000 was sent to him (Peter Nosa lyen), he cashed it in Benin and sent the fake postal orders to the agent. The undercover then forwarded their investigation report to the EFCC along with computer printouts. Further investigations revealed the brain behind the internet fraud. The internet protocol address used by the Appellant was traced to Peen Cyber Cafe at No. 1, Afolabi Street, Akoka, Yaba, Lagos owned by the Appellant's father. The fake postal orders were also confirmed in the US and in Nigeria by the Immigration Service.

The Respondent through the EFCC arraigned the Appellant, alleging that he used the internet to deal in the sale of fake postal orders. He was tracked down and arrested at his place of business.

The trial Court found the Appellant guilty of the charge with 12 counts of forgery, conspiracy, exportation, offering for sale international Postal Money orders, inducement and uttering of United States Postal Money orders. Dissatisfied with the judgment, the Appellant filed an appeal at the Court of Appeal.

In the final analysis, the appeal failed and was dismissed. Accordingly, the judgment of the trial Court was affirmed.

Considering the above, it therefore follows that with more sensitization, people who have fallen victim to cybercrime in Nigeria can institute actions under the Cybercrime Act and get the justice they deserve.

RECOMMENDATIONS

Borrowing a Leaf from the Cybersecurity Ecosystem

According to a fraud prevention software company called Seon, the data from the Global Cyber Strategies Index and recent cybercrime statistics obtained in 2023, determined that the three most secure nations were Denmark, Germany, and the United States of America respectively.[4] Other countries with a strong cybersecurity system are China, Russia, United Kingdom. Below are some of the ways they have made their cybersecurity systems effective:

a. **Effective legislation and regulations:** Countries with strong cyber security legislation and regulations are better able to detect and quell cyber-attacks. Currently, in Africa, South Africa is one of the countries with very strong cyber security regulations. The South African Government has enacted the Cybercrimes and Cybersecurity Act in 2021 and the Protection of Personal Information Act No. 4 of 2013. Also, Mauritius is ranked among the top African Countries for Cybersecurity according to the Global Cybersecurity Index from the International Telecommunication Union (ITU). Both countries have a higher enforcement rate compared to Nigeria by the development of their technical staff to achieve certain goals. Mauritius for instance has established the Government Security Incident Response Team (G-SIRT) which focuses on capacity building under the Information Technology Security Unit (ITSU) of the Ministry of Technology, Communication, and Innovation.

[4] https://studyonline.unsw.edu.au/blog/top-three-cyber-secure-countries-and-how-they-prepare-against-cyber-attacks

b. **Government commitment:** Countries with a strong government commitment to cybersecurity are more likely to invest in the necessary resources to protect their networks and systems. For instance, The United States has a comprehensive cybersecurity framework established by various government agencies, including the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Cybersecurity and Infrastructure Security Agency (CISA). The country continuously invests in cybersecurity research, education, and public-private partnerships.

c. **Public awareness:** Countries with a high level of public awareness and sensitization on cybersecurity are less likely to fall victim to phishing attacks and other social engineering techniques. Countries such as the United Kingdom, through organizations like the National Cyber Security Centre (NCSC) and Cyber Aware, conduct awareness campaigns and provides online resources to educate citizens about cybersecurity threats and preventive measures. These efforts include guidance on password security, phishing awareness, and safe online practices.

d. **Education and training:** Countries with strong cybersecurity education and training programs are better able to produce a skilled workforce that can defend against cyber-attacks. An example of a country with strong cybersecurity education is Singapore, the government actively promotes cybersecurity awareness through various initiatives, including campaigns, workshops, and educational programs targeting different age groups. The government also collaborates with industry partners and educational institutions to disseminate information and resources on cybersecurity.

e. **Technology:** Countries with access to the latest cybersecurity technologies are better able to protect their networks and systems from attacks. Germany for instance, has a robust cybersecurity industry and is known for its expertise in areas such as industrial cybersecurity, automotive security, and secure software development. The country's research institutions and technology companies collaborate to develop advanced cybersecurity solutions, leveraging technologies such as blockchain, quantum cryptography, and secure hardware.

While Cybersecurity laws are often associated with punitive measures, as earlier stated, preventive measures ought to be introduced and incorporated in the already existing cybersecurity laws to reduce the incidents of cybercrimes. For instance, adopting a cybersecurity framework with a view to reducing cyber risk. According to Eric Cisternelli on Bit sight (a cybersecurity ratings company that analyses companies, government agencies, and educational institutions), a cybersecurity framework provides a common language and set of standards for security leaders across countries and industries to understand their security postures and those of their vendors. With a framework in place that follows common cybersecurity standards, it becomes much easier to define the processes and procedures that organizations and indeed the country must take to assess, monitor, and mitigate cybersecurity risk.

CONCLUSION

It is no doubt that Cyberspace has become an integral part of the lives of millions of people around the world and several changes have emanated in technology. Thus, to adapt to these changes and there is need for strengthened cybersecurity laws in Nigeria to strike the much-needed balance in Cybersecurity. Also, Nigeria's cybersecurity landscape is characterized by a need for enhanced legal and regulatory frameworks, a growing recognition of the importance of cybersecurity, and the presence of general and sector-specific legislations to address cyber threats and data protection.

Thus, adapting laws to address evolving cybersecurity threats in Nigeria is paramount, for safeguarding national security, protecting citizens' privacy, and fostering a conducive environment for economic growth and digital innovation. With the rapid advancement in technology and the increasing sophistication of cyber threats, outdated laws risk leaving critical systems and personal data vulnerable to exploitation. On the other hand, the emerging changes in cybercrime must not be underestimated as the seeming deduction is that hackers and cyber attackers are always one step ahead; hence this gap must be bridged.