THE USA JOURNALS
THE AMERICAN JOURNAL OF POLITICAL SCIENCE LAW AND CRIMINOLOGY (ISSN- 2693-0803)
VOLUME 06 ISSUE09

PUBLISHED DATE: - 23-09-2024
DOI: - https://doi.org/10.37547/tajpslc/Volume06Issue09-07 PAGE NO.: - 64-84

RESEARCH ARTICLE Open Access

EFFECT OF DATA PROTECTION FRAMEWORKS AGAINST CYBERCRIMES ON CYBER SECURITY IN NIGERIA

Abiodun Adebanjo (DoP)
PhD Student City University, Cambodia

Gloria Chigbu
Lecturer ESFAM-BENIN University, Benin Republic

Christopher M Osazuwa
PhD Student City University, Cambodia

Abstract

The paper Effect of Data Security Frameworks against Cybercrimes and Cyber Security in Nigeria critically examines the various data protection frameworks in Nigeria and how these are impacting curtailing cybercrimes in the country. The paper examined the institutions responsible for data security and how they carry it out. The work utilized both the secondary and primary sources of data collection. Key Informant Interview (KII) and the observation method were deployed to collect primary data for the study. Information on data protection was also collected from (NDPC) and other relevant agencies. Information from reports from the internet, scholarly articles in journals, and information from websites and books were used in the paper. The paper utilised the Social Strain Theory (SST) as the theoretical framework for the study. The paper observed that data protection regulations in Nigeria make it mandatory for all Public Institutions (PIs) in Nigeria to have a comprehensive cyber security framework, which is to protect against unauthorized access. Several factors are responsible for data insecurity and the attendant increase in cybercrimes in the country. These include, among others: i. Lack of knowledge on the part of most officers of the penalty for data breach allowed by them. ii. Poor dissemination of the content of the NDPA. iii. The poor economic condition of the country makes many officers to seek means of getting extra money, this also includes their volunteering information that they should not disclose in the first place. The paper observed that though cyber security in Nigeria is not within the mandate of the EFCC, the Commission plays very important role in dealing with the threat of cybercrimes in Nigeria. Records shows that of the 12,394 convictions of the EFCC from inception till 31st December 2023. Over 80% of them are on cybercrime and related offences. The paper concluded that inspire of the efforts of the EFCC and other agencies in tackling cybercrimes in Nigeria, the failure of the data protection frameworks in the country in ensuring confidentiality, integrity and security of the data at their disposal is the reason for the spiralling of cybercrimes in the country. The paper recommends that the Nigerian government adopt the best practice policies and regulations, promote awareness, and continuously update cyber security practices, which is germane to enhancing data protection in the country.

KEYWORDS: Cyber Crime, Youth, Data Protection Framework, Cyber Security, Economic and Financial Crimes Commission (EFCC).

INTRODUCTION

The increasing economic shift to digital and online models has created threats that have outpaced traditional business security approaches. The continuous developments of cyberspace have given rise to malicious uses of cyberspace. More than ever, governments and organizations need to be proactive in creating and adapting systems to face these threats. By safeguarding their own operations, the information of people who use their services will also be better protected. This becomes pertinent because of the insecurities and use of cyberspace as a platform for malicious activities. The use of a secure and robust digital identification system that can protect privacy is an essential, reliable and user-friendly element for a strong cyber resilience strategy and is a source of new business opportunities and applications for governments across the world and the private sector (Afifuddin, and Adriyanto 2023).

The march towards digital identity is well underway; therefore, the focus should be on both the adoption and adaptation of the new structures and regulations. These are needed to govern the associated services and transactions as well as establish laws that enforce penalties for violations (Sule, Mary, Zennaro & Thomas 2021).

Sule, Mary, Zennaro & Thomas (2021) posited that it is pertinent to note that understanding Cyber security starts with the basic assumption that in cyberspace (a generic name for all online or electronic platforms), we all are attractive targets for attacks by cybercriminals. The intended objects could be our money or data and also range from usernames, passwords, documents, emails, and online presence, among others. Most cyber-attacks are generic and can happen to anybody, although personalised attacks do occur. One basic and common enabler of cyber-attacks is human error (Sule, Mary, Zennaro & Thomas 2021). These enablers could be very simple as trusting the electronically sent instructions in a phishing email, to as complex as criminals posing as clients, vendors or even employees or professionals to gain access to your assets (both financial and others). There is, therefore, the need for computer security against these attacks (Sule, Mary, Zennaro & Thomas 2021).

According to the United Nations Office on Drug and Crime (UNODC) there are key issues in data protection. This covers the generation, collection, storage, analysis, use, and sharing of personal information. This is important because the right to privacy is not only impacted by the examination or use of information about a person by a human or an algorithm. On a daily basis cyber-attacks are perpetrated; the aim of which is to steal valuable and sensitive information from individuals, businesses, institutions, and government organizations.

Blanchfield, (2023) argues that the increased sophistication of these has highlighted the importance of data protection to prevent costly breaches and data leaks. Data protection has therefore become a primary goal of cybersecurity, and it's a major component of compliance and privacy. The use of appropriate set of systems and strategies among government institutions and private organizations alike can prevent attackers from stealing data, thereby safeguarding against data loss and continuity disruptions. Digital Identity Ecosystems (DIE) depends on computer or some digital systems infrastructure (Blanchfield 2023). Due to these infrastructure challenges in Africa, the scalable infrastructure solution to provide cost savings (reduced cost) and effective service in the Digital ecosystem is the cloud infrastructure technology.

Putting the problem of data insecurity in Africa into context Komminoth, (2023) opined that the continent's burgeoning digital economy is rife with opportunities for growth, but also has a number of challenges that must be addressed if the continent is to enjoy the benefits of therof. Komminoth, (2023) postulated that one of the most significant challenges facing Africa is the lack of digital security infrastructure. While many countries in the continent he said are focused on building reliable electricity and internet networks to grow their start up ecosystems, cyber security is often not given the priority it deserves. He presented some current statistics, when he said as at 2023, approximately 90% of African businesses are operating without cyber security protocols in place, making them vulnerable to cyber threats, such as hacking, phishing, and malware attacks.

Komminoth, (2023) observed that the economic consequences of digital insecurity are already substantial. In the continent it is estimated that it costs South Africa $570m a year, Nigeria $500m and Kenya $36m Komminoth, (2023:2). African Business magazine in 2023 carried out a survey and the result shows that CEOs in Africa have found that businesses are more reluctant than individuals to adopt and use the internet for e-commerce as a result of fear of insufficient data security. The prospects of e-commerce is said to hold a projected revune of $180bn a year by 2025 (African Business Magazine). The lack of digital security in Africa is not just an issue for existing businesses, but also for start-ups. With the increasing use of digital technologies in areas such as healthcare and education, the security of personal data has become paramount. Data protection remains a challenge among computing infrastructure and digital systems. Data protection remains a challenge among the continent's computing infrastructure and digital systems.

Statement of the Problem

Cybercrime is a common occurrence in Nigeria. According to the report from the Nigerian Communication Commission (NCC) Nigeria loses about $500m yearly to cybercrime. This accounts for 0.08 percent of the country's Gross Domestic Product. Nigeria is ranked 16th among the victims of cybercrimes in the world (Nigerian Communication Commission Report, 2023). Investigation reveals that most cases of cybercrimes in Nigeria are a result of unauthorised access to the private data of individuals. It is not uncommon for people to receive emails, sms, chats and even voice calls detailing their private information. The question is how do the fraudsters gain access to this information?

Statistics from the Economic and Financial Crimes Commission (EFCC) show that it has a total of 12,394 convictions from inception to 31st December 2023 (EFCC, Annual Report compilations). It is interesting to note that over 85% of these convictions are on cybercrimes and related offences. Inspired by this, cybercriminals are increasingly using sophistication to carry out their nefarious acts. This becomes a serious cause for concern. To this end, evidence abounds that cybercriminals get access to the private data of people. Investigation into some celebrated cases of cybercriminals like Obinwanne Okeke, popularly known as Invictus Obi, Ismaila Mustapha, aka Mopmha and Ramon Olorunwa Abbas, alias Hushpupp etc., proves that there are institutional gaps that need to be addressed.

To prevent criminals from accessing private data, bank information, and other personal information, the Nigerian government put in place measures to promote data protection in the country. Section 37 of the Constitution of the Federal Republic of Nigeria (FRN) guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. In order to implement this and prepare Nigeria for the digital economy. The Nigerian Government to enact the Data Protection Act (2023). The Act created the Nigeria Data Protection Commission (NDPC) to regulate the processing of personal information, promoting data processing practices that safeguard the security of personal data and the privacy of data citizens, institutions, and organisations. NDPC is also to provide means of recourse and remedies in the event of a breach of the data subject's rights, strengthen the legal foundations of the national digital economy, and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data etc.

Despite the enactment of this legislation the issue of date security is still a problem and the reason for the increase in cybercrimes in the country. The paper critically examines the various data protection frameworks in Nigeria and how these are impacting cyber security in the country and curtailing cybercrimes, which is at the heart of cyber security in the country. The paper examined the institutions responsible for data security and how they carry it out. The paper also suggests strategies that can contribute to preventing the incidence of cybercrimes in Nigeria.

Literature Review

Conceptual Review

Cyber Security in Perspective

Sharp (2023) asserts that increased migration of the world to the digital space and use of digital devices implies that threats to businesses and individuals are increasingly moving to cyberspace. For this reason, research is increasing on how to protect digital devices, networks and users from exposure to cyber-attacks. This led to the development of cyber security. As a result of the reality that our contemporary daily life is more dependent on technology more than ever before, the benefits of cyber security cannot be over-emphasised. The development of cyberspace has made near-instant access to information on the Internet to the modern conveniences provided by smart home automation technology and concepts like the Internet of Things.

The development of technology has made people more reliant on automated service. This therefore has increased the exposure of people to the new potential insecurity threats that lurks behind every device and platform. Despite society's perception of modern advances, cyber security threats presented by modern tech are a real danger. As we are aware, a steady rise in cybercrime highlights the flaws in devices and services the world has come to depend on. This concern forces people to ask what cyber security is, why it's essential, and what to learn about it. Kelley (2023) opined that cyber security is the protection to defend internetconnected devices and services from malicious attacks by hackers, spammers, and cybercriminals. Cyber security is used for example by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses. He went on to posit that cyber security covers a wide range of areas which includes the implementation of different defenses in an organization's software and services against a diverse range of threats. Subdomain of cyber security requires cyber security experts to write secure code, design secure application architectures, implement robust data input validation, and more, to minimize the chance of unauthorized access or modification of application resources (Kelley 2023).

According to IT Governance (2023) cyber security encompasses a broad range of practices, technologies, and measures designed to protect computer systems, networks, data, and programs from theft, damage, unauthorized access, and other cyber threats. It involves safeguarding information technology (IT) assets and ensuring the confidentiality, integrity, and availability of digital resources. Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The UN General Assembly passed a Resolution in 2010 on cyber security. The Resolution addresses cybercrime as a major global challenge. According to a Publication by International Telecommunication Union (ITU) cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being.

According to the International Telecommunication Union (ITU) (2023) deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. Cyber security is the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against security risks in the cyber environment. The general security objectives are as follows: Availability and integrity, which may include authenticity and confidentiality. The key components and areas that cyber security entails are information Security, Network Security, Endpoint Security, Application Security, Cloud Security, Identity and Access Management (IAM), incident response and Security Awareness and Training (ITU, 2023).

Furthermore, Cisco (2023) posits that a successful cyber security approach has multiple layers of protection spread across the computers, networks, programmes, or data that one intends to keep safe. In an organization, the people, processes, and technology must complement one another to create an effective defence from cyber-attacks. A unified threat management system can automate integrations across selected layers. Security products and accelerate key security operations functions include detection, investigation, and remediation. The following are the major players in cyber security:

People: Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

Processes: Organizations must have a framework for how they deal with both attempted and successful cyber-attacks. One well-respected framework can be a useful guide. It explains how people can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

Technology: Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber-attacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

Cyber Crimes in Perspectives

The Council of Europe Convention defines cybercrime as: "a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements". There are various crimes which criminals perpetrate in the cyber space. The following are the various forms in which they occur. The various forms and nature in which cybercrimes occur makes it important for a proper grasp of their manifestations. While most cybercrimes are carried out with the expectation of financial gain by the attackers, it must be added that the intent and motivation for each attack varies. Gambo and Adebanjo (2021) presented a concise summary of types and forms of cybercrimes that I consider apt for this paper:

i. Cyber Extortion: Cyber extortion is a crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. It is the art of attacking a network to obtain money from the network provider or user. A major form of this is the ransomware attack.

ii. Crypto Jacking: Crypto Jacking is stealing online by high-tech hackers. They deploy mining software on the victim's system or network, which then steal these currencies to their own wallets. These attacks are most successful when JavaScript codes that does in-browser mining sites are placed on a network. Once a user's browser has a tab or window opened, the programme goes to work.

iii. Identity Theft: People store a lot of information online, which criminals target. If a person's social security number (our version of National Identity Number—NIN in Nigeria) is obtained, it can be used to commit fraud and other heinous crimes.

iv. Credit Card Fraud: This is a form of identity theft in which a hacker infiltrates a network and steals customers' banking details or credit card information to defraud them. By either stealing the money or using it to buy things online or on other platforms. The credit card information, or what we call ATM information in popular parlance in Nigeria, could be sold to criminals for a fee. Criminals steal this information and sell it to other criminals on the dark web who use it for heinous crimes, such as illegal arms purchases, terrorism financing, etc.

v. Cyber Espionage: This is the act of spying on a network to gain confidential information about a person or an organization, or to gain information about a country.

vi. Software Piracy: This is the counterfeiting of software and its sale at a cheap price in the dark market. It is the illegal copying, distribution, and use of cyber and other resources like CD plates, e-books, etc. It involves Trademark violations, patent violations, and copyright infringements.

vii. Cyber Stalking: This simply is harassment of a person by another in the cyber space. Usually the cyber stalker is familiar with the victim. Stalkers do this via the social media and other online channels. It could also be through phone calls or email.

viii, Cyber Bullying: This occurs when a person decides to make an internet user uncomfortable by harassing, embarrassing or targeting the user's gender, religion, sexual orientation, race, physical differences, etc.

ix. Business Email Compromise (BEC): This occurs when criminals target persons within firms that authorizes financial transactions, tricking them into making scheduled payments to themselves instead of the original recipients. These criminals often research into the identified organisation in order to understand its workings. They then target the payment schedule of the organisation's executives, employees, customers, business partners potential business partners, etc (Gambo and Adebanjo (2021: 91-95).

Gambo and Adebanjo (2021: 95-98) present the following as the most common types of cyber-attacks:

a. Distributed Denial of Service (DDoS) Attacks.

b. Spread of malware on Systems.

c. Ransomware.

d. Phishing Campaigns.

e. Credentials Attack.

f. Website Hijack.

g. Man-in-the-middle (MITM) Attack.

h. Drive-by Downloads.

i. Watering Hole Attack.

j. Others: Other examples of cyber-attacks include solicitation, production and distribution of child pornography, illicit gambling, sales of counterfeit or pirated products, illegal sales of weapons, drugs, etc.

Causes of Cybercrimes in Nigeria

According to Hassan, (2012) the following are some of the identified causes of cybercrime in Nigeria:

a. Unemployment is one of the major causes of Cybercrime in Nigeria.

b. Quest for quick wealth.

c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught.

d. Incompetent security on personal computers.

According to Proshre in an article in 2020 titled: "Cybercrime in Nigeria: Causes and Effects," Nigeria is experiencing a surge in cybercrimes as a result of the prevailing economic conditions. The articles identified; high rate of unemployment and the quest for quick wealth are the two major factors which drive individual's towards cybercrime. This threat poses a great risk, which can only be eliminated through the strict enforcement of cybercrime laws, provision of lucrative opportunities in the economy, information sharing etc. However, in the medium to long term, increasing awareness could help mitigate the cyber threats, if action is taken.

Empirical Review

According to Onadeko & Afolayan (2015) the digital and information technology age has created new avenues and tools for committing traditional crimes and new forms of crimes. The architecture of the digital world challenges law enforcement institutions and the criminal justice system to device measures and procedure to contend with digital or cybercrimes. In Nigeria, there had overtime been a significant increase in internet-based advance fee fraud. Onadeko & Afolayan (2015) observed that there are cases of hacking into emails, website and infringement on privacy rights of persons and institutions which call for urgent solution. Onadeko & Afolayan (2015) observed opined that legislation on advance fee fraud is among the earliest intervention by the Nigerian Government on cybercrimes. This led to the Advanced Fee Fraud Act of 2006. They opined that the law is inadequate to meet the intricacies of technological development. This led to the enactment of the Cybercrimes (Prohibition and Prevention etc) Act, 2015. The objectives of this Act include the provision of an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act is designed to ensure the protection of critical national information infrastructure and to promote cyber security, protect computer systems and networks, electronic communications, data and computer programmes, intellectual property and privacy rights (Cybercrimes Prohibition and Prevention Act, 2015)

Adeshina (2017) on the other hand opined that there is a nexus between poverty and cybercrime in Nigeria While one can blame cybercriminals in Nigeria as being lazy or greedy, the stark reality is that most of them perpetuate the act as a means of escaping the reality of poverty. Adeshina (2017) argues that yahoo yahoo business is a means of survival. According to him the popular maxim, "The idle hand is the devil's workshop"; the situation whereby majority of the people are poor and hungry and a lot of youths are jobless and unemployed, will, doubtlessly, lead to high crime rate in the country. Adeshina (2017) went on to say that there is no doubt that cybercrime has negative impact on the economy as well as the image of the country. With the increased use and dependence on technologies. Adeshina (2017), posits that there is an increase in the risk posed by cybercriminals. Thus, there is need for a holistic approach to combat this crime in all ramifications. He maintains that the Nigerian public needs to be educated on the ills of cybercrimes. Additionally, Adeshina (2017) said that strong legislation on cybercrime is imperative for combating crime.

Therefore, there is a need to ensure the effectiveness of the 2015 Cybercrimes Act.

Adeshina (2017) recommends that cybercafés in the country must be properly regulated. It must be ensured that they are properly registered with the relevant agencies like the Corporate Affairs Commission. Surveillance hardware that will help in keeping tab on internet usage and detect cybercrime must be put to proper use. Also, the country's intelligence agencies must be equipped with the right skills and equipment that will facilitate detection and handling of cybercrime in the country. Furthermore, while law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Adeshina (2017) opined that domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. More international coordination and cooperation are, therefore, essential in fighting the scourge of cybercrime. Finally, he concludes that vigilance can go a long way in the fight against cybercrime. A significant percentage of cybercrimes can be prevented by just getting the cyber basics right such as updating software, having strong passwords and regular system back-ups.

Wang, Nnaji & Jung (2019) on the other hand in a research findings suggest a high level of cyber security breaches in the Nigerian banking industry. More banks suffer, in general, from cyber-dependent breaches, such as virus, worms, and Trojan infections, and hacking, than cyber-enabled breaches. Of course, some cyber-enabled breaches, e.g., electronic spam mail, continue to rise at a high rate. Other types of cyber-enabled breaches are, however, experienced less by banks in this sample. Wang, Nnaji & Jung (2019) posited that cyber security breaches targeting Nigerian banks are becoming more technologically sophisticated. In sharp contrast, while the banks are trying to protect themselves and their customers, their current security practices are no longer adequate to combat the increasingly sophisticated cyber-dependent breaches that they experience. Wang, Nnaji & Jung (2019) argued that there is, in particular, a significant lack of advanced technologies to prevent cyber security threats, and also to respond to cyber security breaches after these have been detected. They conclude that cyber security breach remains one of the biggest security risks in the banking industry in Nigeria. Their research provided some insights into the current state-of-the-art of cyber security breaches, practices and capability of the Nigeria internet banking industry.

Wood, et al (2022) opined that data protection harms can arise through the use or misuse, or loss of personal data, or from an inability to exercise data rights effectively. Data protection harms may have various impacts on individuals, ranging from financial loss, emotional distress and even physical harm. They may also have an impact on society as a whole, including on judicial and democratic processes. However, the risk of these harms occurring, and the severity of the impact are not always well understood. Wood et al. (2022) presented a study based on the United Kingdom (UK); they observed that in the UK, the Information Commissioner's Office (ICO) is responsible for promoting and enforcing data protection law. ICO liaises with relevant government and private sector companies to help deal with the issues of data insecurity in the UK.

Wisniewski & Page (2022) argued that privacy, particularly within the Information Systems (IS) field, is often defined as "the ability of individuals to control when, to what extent, and how information about the self is communicated to others". Even with the different conceptualizations of privacy, one commonality among many fields is the unilateral emphasis on privacy as it relates to information disclosures. Viewing privacy as control over one's information disclosures treats privacy as a somewhat dichotomous boundary between private and public information disclosures. Wisniewski & Page (2022) observed that several information privacy models have been developed; a commonality among these frameworks is that the focus has been on privacy as withholding or divulging information. Wisniewski & Page (2022) contends that concern for information privacy (CFIP) is based on 4 dimensions: collection, errors, secondary use, and unauthorized access to information. Each dimension represented a privacy concern for a type of information misuse. People differed in their concern for (1) data collection, (2) whether the data was represented faithfully, (3) whether data was used for its originally intended purpose, and (4) if data was used by an unauthorized third party. Wisniewski & Page (2022) used this scale to measure an individual's concern about organizational information privacy practices, as they considered information privacy one of the most important ethical concerns of the information age.

Adisa and Dadam (2023) observed that organizations across all industries are becoming more reliant on digital technology to get the job done. In this era of digital transformation, technologies such as the Internet of Things (IoT), social media, machine learning (ML) big data analytics, artificial intelligence (AI), and augmented reality exist to help organizations realize their strategic business objectives. Although digital transformation and the adoption of new technologies create a variety of illustrious new business opportunities, it also inherently introduces new forms of risk and challenges. This appears to be a lucrative market for cyber criminals to commit various crimes both on individuals and businesses.

Adisa and Dadam (2023) quoting a report by Surfshark, (a cybersecurity company), Nigeria recorded 82,000 data breaches in the first quarter of 2023 (January to March). Some other forms of attack ranged from concerted attacks by individuals who hack for personal gain or malice to poorly configured system security or careless disposal of used computer equipment or data storage media. These challenges according to Adisa and Dadam (2023), coupled with the risks, necessitated the enactment of some legislation in Nigeria for the protection of both individuals and businesses.

According Anthonia (2024) to cybercrime is a global problem. However it is rampant in Nigeria because of our economic and financial level. She observed that one of the problems Nigerians face as immigrants going abroad is that the country is affiliated as a country where cybercrime is the order of the day especially internet fraud. Anthonia (2024) noted that there has been efforts made towards curbing cybercrimes in Nigeria. However, it has not been effective because of lack of job opportunities for the working class and the poor living standard of the citizen. According to Anthonia (2024), Nigerian go into cybercrimes because of hunger and poverty, bad educational systems and because of their knowledge of the fact that the law regulating it is almost obsolete. Anthonia (2024) recommended that the government should try as much as possible to provide job opportunities for the working class and this can be done by helping infant companies grow. Nigerians should also be innovative by thinking of ways to develop businesses in a legal way and by the judiciary making sure the laws put in place for the prohibition of cybercrimes are effective.

Al-Emran & Deveci (2024) observed that the metaverse, often referred to as the next stage of the internet, is a virtual space that utilizes advanced technologies, such as augmented reality, virtual reality, and mixed reality, to enable real-time engagement and experiences beyond what can be achieved in reality. Al-Emran & Deveci (2024) maintained that cyber security behaviour in the metaverse refers to the actions taken by individuals and organizations to protect themselves and their information from various cyber threats in virtual reality environments by implementing various cyber security measures. Al-Emran and Deveci (2024) argued further that research on cyber security behaviour in the metaverse is still limited. Their study offers an overview of cyber security behaviour in the metaverse and identifies potential opportunities. Al-Emran and Deveci (2024) posit that their current and prospective challenges can be examined in future research about the metaverse. They contend that there is a need for a research agenda covering the security of the metaverse, influential factors, human behaviour in the metaverse, virtual identity and access management, privacy, legal and ethical issues, and cyber security education and awareness.

In their work, Malhotra et al. (2004) argue that the online world has led to internet users' information privacy concerns (IUIPC). IUIPC consists of three dimensions identified as the most pressing for online privacy concerns: collection, control, and awareness of privacy practices. Accordingly, a fine-grained version of IUIPC includes access/participation, information collection, information storage, information transfer, notice/awareness, and personalization, which are additional factors to consider. Malhotra el al (2024) studied information privacy online and developed their "information boundary theory" by studying privacy attitudes on information disclosure across e-commerce, finance, healthcare, and social networking websites. They found that privacy intrusion, risk, and control were all important factors related to privacy concerns in the context of social networking websites. This provided guidance on the common elements to be considered when studying information privacy across various online contexts.

Araujo, Machado & Passos (2024) opined that cyber resilience is a necessary tool to deal with the realities of cyber threats that the world is currently battling. Cyber resilience is a topic of extreme relevance to organizations in the most diverse segments of activity. The concept of resilience Araujo, Machado & Passos (2024) argues presents nuance in its different dimensions, in addition to the need to recognize and distinguish the different stages that characterize the state of cyber resilience. Araujo, Machado & Passos (2024) contends that if the various concepts of cyber resilience in its different contexts and dimensions are understood, it shall help in the development and deployment of the appropriate tools to deal with the threats of cyber insecurity. They postulated that to effectively deploy cyber resilience the main stages of resilience needs to be mapped, and an analysis to determine how these stages have evolved over the years is vital. They conclude that effective cyber resilience is an enterprise-wide risk-based strategy that involves governance, risk management, an understanding of data ownership and incident management. For any effective cyber resilience the right balance between three types of controls: preventative, detective and corrective must be found.

Theoretical Framework

The Social Strain Theory (SST) was adopted as the theoretical framework for this study. It was developed within the socio-structural context of the United States by Merton (1938). The major tenet of this theory lies in the postulation that when opportunities for achieving socially desirable goals are blocked, those affected may react in different ways to adapt to their situation. To him, there are five distinct ways through which people can adapt to social strain, including i) conformity, ii) innovation, iii) ritualism, iv) retreatism, and v) rebellion. Among these classifications, innovation is of major interest to drive the point with regards to the issue of cybercrime in this study. In this direction, innovation is developing new means of achieving socially desired ends. As such, innovators aim at fulfilling the goals of society, but instead of using legitimate channels, they find other means to reach their goals. In other words, when the legitimate channels of achieving socially desirable goals are perceived as being too stringent by some people, they become innovative in finding ways of meeting such goals using other means.

Cybercrime is one of the innovative means adopted by a number of youths in Nigeria to amass wealth, considering the view that other criminal acts such as armed robbery and kidnapping etc; are perceived as becoming more riskier for them due to improved security networks past few years. Thus, youths' involvement into cybercrime is a rational calculation that such crime within the Nigerian context is less risky and can attract wealth within one's private environment. This theory is also important for this study considering the fact it help to provide the reason why cybercrimes that is prevalent among youths in Nigeria.

METHODOLOGY

The research applied the secondary and primary source of data collection. Key Informant Interview (KII) from an unstructured interview with three (3) staff of the Economic and Finical Crimes Commission (EFCC) and one (1) staff of the Nigerian Data Protection Commission (NDPC). The observation method was deployed to collect primary data for the study. The researcher is a staff of the EFCC. The study gathered first-hand information about cyber insecurity and the perpetration of cybercrimes in Nigeria due to data protection failings. Information on data protection was also collected from (NDPC) and other relevant agencies. Government agencies also utilized reports on data protection, cybercrime, and data security. Information from reports from the internet, scholarly articles in journals, and information from websites and books were used in the paper.

Data Protection Frameworks in Nigeria

The basis for data protection in Nigeria are the laws that established institutions saddled with the responsibilities for this (Nigeria Data Protection Act" online at https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf). The stating point is the 1999 Constitution of the Federal Republic of Nigeria. Also we have the Criminal code (1990), the Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006, the Cybercrimes (Prohibition, Prevention) Act 2015, Nigeria Data Protection Regulation (NDPR) 2019 and ultimately the Nigeria Data Protection Act, 2023 (NDPA). NDPA is now the statutory provisions that defines and regulates data protection in Nigeria today.

According to Oyewole & Salami (2024) the Data Protection Act (2023) is enacted to safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria. Among other things, the objective of the Act include: the protection of personal information; establishing the Nigeria Data Protection Commission for the regulation of the processing of personal information; promoting data processing practices that safeguard the security of personal data and privacy of data subjects; protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights; and strengthening the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data etc. The Data Protection Act received Presidential assent on 13 June 2023 (Oyewole & Salami 2024:1).

Oyewole & Salami (2024:2) observed that four years after the adoption of the Nigeria Data Protection Regulation (NDPR), by the National Information Technology Development Agency (NITDA) on the 25 January 2019. Nigeria Data Protection Act, 2023 (NDPA) was passed into law in June 2023. NDPA led to the creation of the Nigerian Data Protection Commission (NDPC). The NDPC implements the NDPR.

The personal and territorial scope of the NDPR is defined by citizenship and physical presence. It applies to residents of Nigeria, as well as Nigerian citizens abroad. The NDPR provides legal safeguards for the processing of personal data. Under the NDPR, Personal Data must be processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject (One Trust Data Guidance, 2024). The Framework builds on the NDPR to ensure a tailored implementation of the data protection regime in Nigeria. It serves as a guide to data controllers and administrators/processors to understand the standards required for compliance within their organisations (One Trust Data Guidance, 2024). The Framework is to be read in conjunction with the NDPR and does not supersede the NDPR.

There are guidelines that applies to all public institutions (PIs) in Nigeria, including ministries, departments, agencies, institutions, public corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the Federal, State or Local levels, that process the personal data of a data subject. The Guidelines mandate all PIs to protect personal data in any incidence of processing of such data. Processing in this context retains the same meaning it has under the NDPR. All forms of personal data of a Nigerian citizen, resident or non-Nigerian individual that has interactions with PIs, or such PIs have access to the personal data in furtherance of a statutory or administrative purpose, are to be protected in accordance with the NDPR or any other law or regulation in force in Nigeria.

According to Osoro (2023) in addition to the principal legislation mentioned, the Constitution of the Federal Republic of Nigeria and various sector-specific laws make different provisions for privacy and data protection matters. Oyewole & Salami (2024:2-3) points out the key provisions in the laws covering data protection in Nigeria as are outlined thus:

1. **Constitution of the Federal Republic of Nigeria 1999 (As Amended)**: The Nigerian Constitution provides Nigerian citizens with a fundamental right to privacy. Section 37 of the Constitution guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. The Constitution does not define the scope of "privacy" or contain detailed privacy provisions.

2. **Child Rights Act 2003**: The Child Rights Act 2003 reiterates the constitutional right to privacy as relates to children. Section 8 of the Act guarantees a child's right to privacy subject to parent or guardian rights to supervise and control their child's conduct. Some Nigerian states have also enacted Child Rights Laws. Under the Act / Laws, age of a child is any person under the age of 18.

3. **Consumer Code of Practice Regulations 2007 (NCC Regulations)**: The Nigerian Communications Commission (NCC) issued the NCC Regulations which requires all licensees to take reasonable steps to protect customer information against improper or accidental disclosure, and ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information to any party except to the extent agreed with the customer, as permitted or required by the NCC or other applicable laws or regulations.

4. **National Identity Management Commission (NIMC) Act 2007**: The NIMC Act creates the National Identity Management Commission (NIMC) to establish and manage a National Identity Management System (NIMS). The NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers to qualified citizens and legal residents. Section 26 of the NIMC Act provides that no person or corporate body shall have access to data or information in the Database with respect to a registered individual without authorization from the NIMC. The NIMC is empowered to provide a third party with information recorded in an individual's Database entry without the individual's consent, provided it is in the interest of National Security.

5. **Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011**: Section 9 and 10 of the Nigerian Communications Commission Regulation provides confidentiality for telephone subscribers records maintained in the NCC's central database. The Regulation further provides telephone subscribers with a right to view and update personal information held in the NCC's central database of a telecommunication company in camera.

6. **Freedom of Information Act, 2011 (FOI Act)**: The FOI Act seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc.).

7. **National Health (NH) Act 2014**: The NH Act provides rights and obligations for health users and healthcare personnel. Under the NH Act, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NH Act further imposes restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NH Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

8. Cybercrimes (Prohibition, Prevention) Act 2015: The Cybercrimes (Prohibition, Prevention Etc) Act provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. The Act requires financial institutions to retain and protect data and criminalizes the interception of electronic communications.

9. Consumer Protection Framework 2016 (Framework): The Consumer Protection Framework 2016 was enacted pursuant to the Central Bank of Nigeria Act 2007. The Framework includes provisions that prohibit financial institutions from disclosing customers' personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

10. Credit Reporting Act 2017: The Credit Reporting Act establishes a legal and regulatory framework for credit reporting by Credit Bureaus. Section 5 of the Act requires Credit Bureaus to maintain credit information for at least 6 years from the date that such information is obtained, after which the information must be archived for a 10-year period prior to its destruction. Section 9 of the Act provides the rights of data subjects (i.e. persons whose credit data are held by a Credit Bureau) to privacy, confidentiality and protection of their credit information. Section 9 further prescribes conditions under which the credit information of the data subject may be disclosed ("Data Protection Act" https://www.dlapiperdataprotection.com/?t=law&c=NG).

Frameworks against Cybercrimes in Nigeria

Having good legislation in place is one of the major steps in curbing cybercrime. In 2004, the Nigerian government established the Nigerian Cybercrime Working Group, comprising representatives from the government and the private sector to develop legislation on cybercrime. Furthermore, in 2007, the government established the Directorate for Cyber Security (DfC), which is an agency responsible for responding to security issues associated with the growing usage of the Internet and other information and communication technologies (ICTs) in the country. It was provided with funding of N1.2 billion (approximately USD9.8 million using 2007 exchange rates) to carry out its mission (Viko, 2021 p. 154).

1. The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provides the legal framework for establishing the Commission. This Act repeals the Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2002 (Viko, 2021). Some of the significant responsibilities of the Commission, according to part 2 of the Act, include:

a. The investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;

b. The coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;

c. The examination and investigation of al1 reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;

d. The coordination of all investigating units for existing economic and financial crimes, in Nigeria;

e. The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud-Related Offences Act 1995; the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended; the Banks and other Financial Institutions Act 1991, as amended; and Miscellaneous Offences Act (EFCC, 2004) .

2. Advance Fee Fraud and Related Offences Act 2006

Section 23 of the Advance Fee Fraud Act (Laws of the Federation of Nigeria, 2006) defines false pretence as a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true. Section 383 sub-section 1 of the Nigerian Criminal Code states: “A person who fraudulently takes anything capable of being stolen, or converts to his use or to the use of any other person anything capable of being stolen, is said to steal that thing”. Advance Fee Fraud and Other Fraud Related Offences Act 2006 deals with internet crime issues; however, it only covers the regulation of internet service providers and cybercafés, and it does not deal with the broad spectrum of computer misuse and cybercrimes. The EFCC is responsible for implementing this Act. The EFCC has achieved quite a number of convictions via this Act (https://placng.org/lawsofnigeria/print.php?sn=18);

Table 1: EFCC Statistics on Cybercrime Investigation and Prosecutions

OFFENCES	2015	2016	2017	2018	2019	2020	2021	2022
Email Hacking (BEC)	24	46	12	21	13	147	90	49
Internet Fraud* (Computer Related Fraud)	33	112	56	120	26	302	-	-
Cybercrime (Other forms of Cybercrimes)			2	18	916	923	433	74
Internet Banking Fraud	12	25	59	1		5	-	-
Identity Theft							1057	865
Electronic Signature Theft							944	729
Credit Card Fraud							31	18
Theft of Electronic Device							133	
Fraudulent issuance of e-instruction							200	6

Source: **EFCC Records: Department of Planning, Policy Research and Statistics, 2023**

3. The Cybercrimes Act of 2015 in a Nutshell

All the above legislation has proven ineffective in curbing cybercrime as it is increasing. In a bid to put in place a stronger legal framework to curb cybercrime, the Government put forward a revision of the existing cybercrime legislation in September 2008. The bill titled “A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for Other Related Matters” passed a second reading in November 2012 at the Senate. In May 2015, the cybercrime bill was signed into law, properly defining the act as unlawful with penalties attached to any disobedience of the law—the Act, known as the Cybercrimes (Prohibition, Prevention, etc.) (Viko, 2021).

Act 2015 creates a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and other related matters. Particularly, the Act engenders a platform for cyber security and, in turn, ensures the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights, as well as preservation and protection of critical national information. The Cybercrimes Act 2015 is, thus, the first legislation in Nigeria that deals specifically with cybercrimes and cyber security. The Act, which was signed into law on May 15, 2015 stipulates that, any crime or injury on critical national information infrastructure, sales of preregistered SIM cards, unlawful access to computer systems, Cyber-Terrorism, among others, would be punishable under the new law.

The Act prescribes stringent penalties for offenders and perpetrators of cybercrime. The Cybercrimes Act is made up of 59 Sections, 8 Parts; and 2 Schedules. 1st Schedule lists the Cybercrime Advisory Council; 2nd Schedule lists businesses to be levied for the purpose of the Cyber security Fund under S.44(2)(a): GSM service providers and all telecom companies; Internet service providers; banks and other financial institutions; Insurance companies; and Nigerian Stock Exchange. Some of the provisions of the Act include:

a. It gives the president the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furtherance of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.

b. It prescribes the death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that result in the death of an individual (amongst other punishments for lesser crimes).

c. Hackers, if found guilty, of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

d. It makes provision for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment.

e. It specifically creates 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.

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

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

h. It forbids the 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 of 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.

i. 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.

j. It 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 a criminal investigation or proceedings (Cybercrimes Act, 2015).

DISCUSSION

Data Protection Framework and Cybercrimes in Nigeria

Nigeria Inter-Bank Settlement Systems (NIBSS) reports that electronic payment (e-Payment) transactions in Nigeria witnessed a remarkable surge in the first quarter (Q1) of 2024, hitting a total of N234 trillion, which was an 89.3% increase from the N123.8 trillion recorded in the corresponding period of 2023. The significant growth trajectory was unveiled in latest data released by the Nigeria Inter-Bank Settlement System (NIBSS), highlighting the expanding digital footprint within the country's financial ecosystem. Point of Sale (POS) transactions witnessed a 7.92% downturn in the review period, dropping from N2.84 trillion in Q1 2023 to N2.61 trillion in the first quarter of this year. A breakdown of the electronic payment landscape revealed that January witnessed transactions amounting to N72.11 trillion, indicating a substantial uptake in digital financial services. This trend continued into February 2024, with the total transaction value surging to N79.33 trillion, reflecting sustained momentum and increasing reliance on electronic payment platforms. As the quarter progressed, March saw a further increase in electronic transactions, reaching a noteworthy N83.05 trillion (NIBSS, April 2024).

The reports stated that the consistent growth witnessed month-on-month underscored the burgeoning prominence of e-payment solutions in Nigeria's financial landscape, signifying a shift towards greater digitalisation and efficiency in financial transactions. Comparing this to 2023, the first quarter breakdown of the analysis of electronic transactions value in Nigeria revealed that in January 2023, Nigerians engaged in electronic transactions amounting to N38.8 trillion on various platforms.in February 2024, the value of e-payments stood at N36.8 trillion, while in March 2023, the country witnessed a further increase in electronic transactions, reaching N48.3 trillion. Additionally, data on Bank Verification Number (BVN) enrolment revealed that as of April 2024, the total count was 61,605,261 individuals. This marked a noteworthy uptick of 1,449,901 registrations over the span of four months, compared to the figure of 60,115,360 people recorded at the close of 2023 (NIBSS, April 2024).

This data presents the increased utilization of online platforms in banking transactions in the country. This equally allows cybercriminals to seek vulnerable Nigerians that they can defraud. The Office of the National Security Adviser (ONSA) is charged with the responsibility of developing and implementing the National Cyber Security Policy and Strategy (NCPS), 2021. Likewise, the National Information Technology Development Agency (NITDA) has been at the forefront of addressing cybercrime and online security, as evidenced by the agency's role in developing Cybercrime (prohibition, prevention, etc.) Act 2015. This Act establishes a unified and comprehensive legal and regulatory framework for preventing, detecting, prosecuting and punishing cybercrimes in Nigeria.

Agencies like the EFCC are empowered by Section 46 of the EFCC act to investigate and prosecute cybercrimes leading to financial loss. As such the EFCC has been active in this regards. While the purview of cyber security in Nigeria is not within the mandate of the EFCC, the Commission has continued to play very important role in dealing with the threat of cybercrimes in Nigeria. According to investigation reports by the EFCC and the Nigerian Police, and other agencies that saddled with the responsibility of investigating cybercrimes such as the Department of State Security Service (DSS), data breaches are at the fore of cybercrimes in Nigeria.

The EFCC on the 7th of May 2024 accused bank official (compliance officers) of being complicit in the cybercrimes in the country. Acting Zonal Director of the Ibadan Zonal Command of the EFCC, during a stakeholders' meeting with Compliance

Officers of Banks in Oyo State said the Commission is aware that Compliance Officers of banks give information to their clients regarding 'letters of investigation activities' written to the banks from the EFCC. The Commission said this act usually jeopardises the investigation exercise of financial crimes and delays corruption cases from being filed before the law court. The Commission decried the unhealthy support fraudsters receive from the banking sector in Nigeria, stressing that it is posing considerable challenges and concerns to the Commission (www.efccng.gov.ng/news/ 7th may 2024).

A significant provision of the NDPA is that any organization that fails to comply with NDPA obligations on data breaches commits an infraction of the provisions of the NDPA, which attracts fines and possible criminal action against the defaulting data controller or processor. Under the NDPA, Data Controllers or Processors of Major Importance (DCPMI) that are found to have breached the provisions of the Act may be subject to the payment of a fine of whichever is greater between the sum of N10,000,000 or 2% of its annual gross revenue from the preceding financial year. Similarly, other data controllers or processors may be liable to pay a fine of whichever is greater than N2,000,000 or 2% of their annual gross revenue from the preceding financial year (NDPA, 2023). The enforcement of this provision has not been forthcoming. There is a need for a member of the public to be aware of this and use such organizations when their personal data is breach.

All government ministries, departments and agencies (MDAs) and private organizations and businesses in Nigeria, banks, insurance companies, manufacturing companies, etc., are obligated to keep the confidentiality of their clients' information. Many hospitals, telecommunication companies, etc., report receiving unsolicited messages, some of which are based on something very personal. For example it is not uncommon for a pregnant woman who visits the hospital to soon start receiving messages from companies who sell baby stuffs. This indicates that some hospital staff (in this case) give their information to the companies. Many people have had fraudsters give them information that can only be given by someone who has access to this information about themselves. Fraudsters are known to give people details of their date of birth, house address, and branch of bank and even call out their BVN numbers. All to convince the persons to send them the code sent to them by these fraudsters. One begin to wonder how this is possible without the active connivance of the bank officials for example.

The data protection regulations in Nigeria has put in place provisions for all companies in the country including MDAs to have a robust data protection infrastructure. NITDA makes it mandatory for all PIs in Nigeria to have a comprehensive cyber security framework which is to protect against unauthorized access. Failure on the part of any PIs to have this is in violation of extant laws and is liable for any data breach. A number of factors are responsible for data insecurity and the attendant increase in cybercrimes in the country. From the interview conducted in this work the following are some of the most cogent explanation:

i. Lack of knowledge on the part of most officers of the penalty for data breach allowed by them.

ii. Poor dissemination of the content of the NDPA.

iii. The poor economic condition of the country makes many officers to seek means of getting extra money, this also includes their volunteering information that they should not disclose in the first place.

iv. Workers in government and private institutions conniving with fraudsters to have access to information of people and give same to them.

v. Some PoS operators have been arrested and prosecuted for being fraudsters themselves. They operate the bossiness in order to have access to the personal information of people and steal their money after they patronise them.

CONCLUSION

The Office of the National Security Adviser (ONSA) which is charged with the responsibility of developing and implementing the National Cyber security Policy and Strategy (NCPS), 2021. ONSA must cooperate with NITDA, NDPC and law enforcement agencies like the EFCC, the Police, banks and all relevant stakeholders to take the message of data protection to the front burner. Though the purview of cyber security in Nigeria is not within the mandate of the EFCC, the Commission has continued to play very important role in dealing with the threat of cybercrimes in Nigeria. The EFCC leverage on legislations like the Cybercrime Act in the prosecution of cybercrimes that bothers on financial crimes. This because the Act establishes a unified and comprehensive legal and regulatory framework for preventing, detecting, prosecuting and punishing cybercrimes in Nigeria.

Cybercrimes has continued to be the highest convictions the EFCC have had over the years. This is so because of the penchant of the younger generation of Nigerians to engage in cybercrimes. A summation of our statistics shows that we have 12,394 convictions from inception till 31st December 2023. Over 80% of them are on cybercrime and related offences. The increasing sophistication deployed by cybercriminals to carry out this act is a cause for concern. Evidence abounds that cybercriminals get access to the private data of people. Investigation into some celebrated cases of cybercriminals like Obinwanne Okeke popularly known as Invictus Obi, Ismaila Mustapha (alias Mompha), and Ramon Olorunwa Abbas (alias Hushpuppy), etc. proves that there are institutional gaps that need to be addressed.

In spite of the efforts of the EFCC and other agencies in tackling cybercrimes in Nigeria, the failure of the data protection frameworks in the country in ensuring confidentiality, integrity and security of the data at their disposal is the reason for the spiralling of cybercrimes in the country. Without an effective data protection culture in the country, the issue of cybercrimes will continue to be on the increase. This portend grave danger to the nation in our quest for a digital economy.

Recommendations

Based on the findings in the work, it is recommended that, there is need for the establishing and enforcing of a robust cyber security strategy. Data protection is one of the major components of a good cyber security ecosystem. The Nigerian government must adopt the best practice policies and regulations, promoting awareness, and continuously updating cyber security practices which is germane to enhancing data protection in the country. All hands must be on deck for the purpose of dealing with the menace of data insecurity which is the bane of the evolution of a comprehensive cyber security strategy in order to enhance data protection and protect against cybercrimes in the country.

REFERENCES

1. Adeshina, S. O. (2017) “Cybercrime and Poverty in Nigeria” April 2017, 13(4):19-29 https://www.researchgate.net/publication/317139515
2. Advance Fee Fraud and Other Fraud Related Offences Act https://placng.org/lawsofnigeria/print.php?sn=18
3. Araujo, M.S.D., Machado, B.A.S., Passos, F.U. (2024) "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance" March 2024Applied Sciences 14(5):2116 DOI:10.3390/app14052116 https://www.researchgate.net/publication/378709279
4. Anthonia, O. (May 2, 2024) “A Literature Review on Emerging Cybercrime in Nigeria”. Available at SSRN: https://ssrn.com/abstract=4814920 or http://dx.doi.org/10.2139/ssrn.4814920 file:///C:/Users/aadebanjo/Downloads/SSRN-id4814920.pdf
5. Al-Emran, M. & Deveci, M. (2024) "Unlocking the potential of cybersecurity behaviour in the metaverse: Overview, opportunities, challenges, and future research agendas" March 2024, Technology in Society DOI:10.1016/j.techsoc.2024.102498 https://www.researchgate.net/publication/378607333
6. Abubakar, M.M., Umar, A.Z.. & Abubakar, M.

(2022) "Personal Data and Privacy Protection Regulations: State of compliance with Nigeria Data Protection Regulations (NDPR) in Ministries, Departments, and Agencies (MDAs)". Proceedings of the 5th International Conference on Information Technology for Education and Development: Changing the Narratives through Building a Secure Society with Disruptive Technologies, ITED 2022

7. Adisa, M. and Dadam D. (2023) "Cyber security and Data Protection Laws in Nigeria: Safeguarding Your Business" https://trustedadvisorslaw.com/cybersecurity-and-data-protection-laws-in-nigeria-safeguarding-your-business/

8. Anton, A. I., Julia B. Earp, and Jessica D. Young. (2010). How Internet users' privacy concerns have evolved since 2002. IEEE Security and Privacy 8 (1): 21–27.

9. Afifuddin, M. and Adriyanto, A (2023) "Challenges and Cybersecurity Threats in Digital Economic Transformation" International Journal of Humanities Education and Social Sciences (IJHESS) 2(6), June 2023, 2(6), DOI:10.55227/ijhess.v2i6.515

10. Blanchfield, D. (2023) "Data Security is the New Cybersecurity" https://elnion.com/2023/07/19/data-security-is-the-new-cybersecurity/

11. Cisco (2023) "What is Cyber security" https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#

12. Cybercrimes (Prohibition, Prevention) Act, 2015 downloaded from https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf

13. DLA Piper's Data Protection Laws of the World Handbook (2024) "Data Protection Laws in Nigeria" https://www.dlapiperdataprotection.com/index.html?

14. Economic and Financial Crimes Commission, Annual Reports, 2010 – 2023 from the Department of Planning, Policy, Research and Statistics

15. Egemonye, C., Adekunle, S. & Izuchukwu, A. (2023) "Better Late than Never – Nigeria Finally Passes the Data Protection Act" https://globallawexperts.com/better-late-than-never-nigeria-finally-passes-the-data-protection-act/

16. European Union's "General Data Protection Regulation (GDPR)" https://gdpr.eu/

17. "E-payment Transactions in Nigeria hit monthly all time High" https://nibss-plc.com.ng/e-payment-transactions-in-nigeria-hit-monthly-all-time-high-of-n33-2-trillion-in-august-2022/

18. Ec-Council Cyber Security Exchange (2022) "Understanding the Five Phases of the Penetration Testing Process" https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/#

19. Ellison, N.B., J. Vitak, C. Steinfield, R. Gray, and C. Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environments. In Privacy Online, ed. S. Trepte and L. Reinecke, 19–32. Berlin: Springer.

20. Gambo, A.Z. & Adebanjo, A. (2021) Developing the Security Conscious Mindset, Abuja: Accurate Press

21. Itgovernance (2023) "What is Cyber Security? Definition and Best Practices" ://www.itgovernance.co.uk/what-is-cybersecurity

22. International Telecommunication Union (ITU) (2023) "Definition of cyber security" https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

23. Jang, S.J. and Agnew, R. (2017) "Strain Theories and Crime" https://www.researchgate.net/publication/275271730_Strain_Theories_and_Crime

24. Kelley, K. (2024) "What is Cybersecurity and Why It is Important?" https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cybersecurity

25. Kumar J.B. (2024) "What is Ethical Hacking? A Comprehensive Guide" https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethicalhacking

26. Komminoth, L (2023) "Africa's Cybersecurity Threat" https://african.business/2023/02/technology-information/africas-cybersecurity-threat

27. Krasnova, Hanna, Natasha F. Veltri, and Oliver Günther. 2012. Self-disclosure and privacy calculus on social networking sites: The role of culture. Business & Information Systems Engineering 4 (3): 127–135.

28. Kramer, F.D.; Starr, S.H.; Wentz, L.K. (2009). "Cyberpower and National Security" National Defense University Press.

29. Merton, R.K., (1938). "Social Structure and Anomie". American Sociological Review, Vol. 3, No. 5. (Oct., 1938), pp. 672-682. Stable URL: http://links.jstor.org/sici?

30. Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research 15 (4): 336–355.

31. NBISS (2024) "Nigeria's e-Payment Transactions Soar To N234 Trillion In Q1 2024, Reflecting 89.3% Year-on-Year Growth" https://www.arise.tv/nigerias-e-payment-transactions-soar-to-n234-trillion-in-q1-2024-reflecting-89-3-year-on-year-growth/

32. Nigeria Data Protection Act online at https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf

33. Nigerian Communication Commission https://www.ncc.gov.ng/contactncc

34. Ngwu, S. (2023) "Data Protection Laws and Regulations" https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria an International Comparative Legal Guides (ICLG) Publication

35. Onadeko, O.A. & Afolayan, A.F. (2015) "A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria" Being a paper presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL) held at Halifax, Nova Scotia, Canada July 24 – 28, 2016 https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf

36. One Trust Data Guidiance (2024) "Nigeria: Data Protection Overview" https://www.dataguidance.com/notes/nigeria-data-protection-overview

37. Omoruyi, O. (2023) "Nigeria sees 64% increase in data breaches, recording an outstanding 82,000 episodes in Q1 2023", https://technext24.com/2023/05/23/nigeria-records-82000-data-breach-in-q1/

38. Oyewole, S, & Salami, A (2024) "Data Protection Act" https://www.dlapiperdataprotection.com/?t=law&c=NG

39. Osoro, P & Co (2023) "Overview of Data Protection in Nigeria" https://www.paulusoro.com/resources/overview-of-data-protection-in-nigeria/

40. Proshre (2020) "Cybercrime in Nigeria: Causes and Effects" https://proshare.co/articles/cybercrime-in-nigeria-causes-and-effects#

41. "Nigeria Data Protection Regulation (NDPR)" https://nitda.gov.ng/

42. "Nigeria Data Protection Act" https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf

43. Nigerian Data Protection Commission (NDPC) https://ndpc.gov.ng/

44. Sule, M., Zennaro, M. & Thomas, G (2021) "Cyber security through the lens of Digital Identity and Data Protection: Issues and Trend" Technology in Society, Vol. 67, November 2021:

45. Sharp, R. (2023) Introduction to Cyber Security: A Multidisciplinary Challenge, London: Springer Publishers

46. United Nations Office on Counter Terrorism

(2024) “Cyber security and New Technologies” https://www.un.org/counterterrorism/cyber security

47. Vitak, J. (2012) “The Impact of Context Collapse and Privacy on Social Network Site Disclosures”. Journal of Broadcasting & Electronic Media, 56 (4): 451–470.

48. Viko, I.J.L (2021) “Analysis of the Legal and Institutional Framework for Fighting Cybercrime in Nigeria” IJOCLLEP 3 (2) 2021, pp: 153 – 162 online at Nigerian Journals Online https://www.nigerianjournalsonline.com ›

49. Wang, V. Nnaji, H. & Jung, J. (2019) “Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability” https://pure.port.ac.uk/ws/portalfiles/portal/21217684/Manuscript_Internet_Banking_in_Nigeria.pdf

50. “What is Cybersecurity?” https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

51. "What is cyber resilience?" ://www.ibm.com/topics/cyber-resilience

52. “What is the social strain theory?” (2024) https://www.restonyc.com/what-is-the-social-strain-theory/

53. Wisniewski, J.P, & Page, X. (2022) “Privacy Theories and Frameworks,” First Online: 09 February 2022, online at https://link.springer.com/chapter/10.1007/978-3-030-82786-1_2

54. Wood, S., et al (2022) Review of Literature relevant to Data Protection harms plumconsulting.co.uk

Unstructured Interview

1. One Data Officer with NDPC 11th July 2024 Mrs. Aderonke Tali

2. 3 staff of the EFCC: Effa Okim, Zonal Director, Benin Directorate, Osodi Johnson Zonal Director, Uyo Directorate and Aisha Abubakar, Head of Investigation, Headquarters, Abuja