Procedure International Journal of Science and Technology

(International Open Access, Peer-reviewed & Refereed Journal)

(Multidisciplinary, Monthly, Multilanguage)

ISSN : 2584-2617 (Online)

Volume- 2, Issue- 1, January 2025

Website- www.pijst.com DOI- https://doi.org/10.62796/pijst.2025

Cyber security Challenges in Nigeria's Digital Economy

R.W. Urim

University of Agriculture, Makurdi, Nigeria

Abstract

Nigeria's digital economy, expanding at an estimated annual rate of 17%, holds the potential to reach $220 billion and generate millions of jobs by 2025. However, its rapid growth has been accompanied by rising cybersecurity threats that jeopardize data security, consumer trust, and sustainable digital transformation. This paper examines the major challenges facing Nigeria's digital economy in the context of cybercrime, including malware, phishing scams, ransomware, insider threats, and denial of service (DoS) attacks. It highlights the country's weak digital infrastructure, shortage of skilled cybersecurity professionals, and gaps in legal enforcement as critical vulnerabilities. Case studies demonstrate the economic and social impact of cyberattacks on banks, businesses, and consumers, underscoring the urgent need for robust defense mechanisms. The study also discusses Nigeria's regulatory frameworks such as the Cybercrime Act 2015, the National Cybersecurity Policy, and Data Protection Regulations, while emphasizing the importance of awareness campaigns, education, and international cooperation. Ultimately, the paper argues that securing Nigeria's digital economy requires strong government–private sector collaboration, investment in skilled manpower, effective regulatory enforcement, and the adoption of global best practices to ensure resilience, trust, and sustainable digital growth.

Keywords: Nigeria, digital economy, cybersecurity, cybercrime, malware, phishing, ransomware, insider threats, regulatory framework, data protection.

Introduction

The digital economy of Nigeria is currently growing at an estimated rate of 17% per annum, and evidence indicates that it could potentiality reach $220 billion and support over 25 million jobs by 2025. The digital economy consists of digital access, digital core, and digital value. Digital access covers availability of access to the internet at a named location such as home, the digital core includes the use of digital technologies in sectors such as agriculture and media, while the digital value covers digital financial services. Presently, Nigeria has 60.45 million active internet users from a total population of 214.1 million. The increasing scale, penetration, and usage of the digital economy emphasizes the vital importance to secure Nigeria's data and information, since the

digital economy has witnessed increased cyber attacks in recent years. Cyber security is a process of protecting systems, networks, and programs from digital attacks. Most cyber attacks are targeted at accessing, changing, or destroying sensitive information, or at extorting money from users via ransomware. Given the importance of data and information to the digital economy, cyber security has become a fundamental requirement to effectively run the operations of the digital economy, hence, there is a need to examine the challenges of cyber security in Nigeria's digital economy.

Overview of Nigeria's Digital Economy

Nigeria's digital economy remains expanding, supported by mobile technology and the internet. Since 2010, the digital-economy market size has increased steadily, reaching $13 billion in 2020, based on confirmed tech-sector deployment to mobile users. The contribution rests predominantly on mobile services, which assist in distributing commodities and services; their contactless nature is especially important during the COVID-19 pandemic for economic and social operations. Despite COVID-19's daunting impact on Nigeria, there are still great prospects for digital economy growth. A large proportion of the population is unbanked, yet more than half have a mobile phone, allowing more ready access to financial services. Digital-economy services have the potential to make an even larger positive impact during the expected economic recession, while at the same time enabling a more inclusive economy. Nigeria's digital hubs, where innovative digital-economy companies develop new solutions, are significant driving forces for the digital economy. The 102 hubs spread across Nigeria primarily focus on innovation; investment; and incubation, acceleration, and capacity building, thus providing the sector with digital skills training, mentoring, and early access to financial support (Abdullahi Saulawa & K. Abubakar, 2014). Digital platforms and services have become crucial components of the Nigerian economy, serving as channels for the supply of goods and services, financial transactions, payments, and transfers; the provision of entertainment; and the sharing of information and knowledge. Given their importance, effective implementation of cybersecurity remains a key issue in developing Nigeria's digital economy and society.

Importance of Cybersecurity

Cybersecurity represents the protection of information assets, including data, technological infrastructure, computers, networking equipment, and supply chains, from unauthorized access, modification, or destruction. The increasing number of individuals and organizations relying on digital platforms in the economy escalates vulnerability to cybercrime (Stella Adesina, 2017). The principal reasons for securing technological environments include safeguarding the confidentiality, availability, and integrity of information, as well as preserving the functioning of vital systems and services. Dominating the global digital economy are major internet companies, such as Google, Facebook, Apple, Amazon, PayPal, and eBay, which act as custodians for substantial information assets of organizations and individuals. Securing these assets is a prerequisite for ensuring privacy and building consumer trust, which in turn encourages economic and technological growth while deterring entrenched crime. Consequently, the emergence of a global digital economy and the need for sustained economic growth necessitate a globally coordinated cybersecurity effort to address related challenges.

Nigeria's capacity to engage in the digital economy substantially hinges on national cyber-readiness, which underpins the ability to deliver on national commitments. The digital economy's defining characteristic—the transformation of many business functions into digital services—amplifies the importance of national preparedness for digital technologies, especially in the contexts of location, investment, and business

processes. Despite its recent growth, Nigeria's telecommunications infrastructure lags behind that of other countries in the region, with prevailing uncertainties regarding the prospects of widespread deployment of next-generation mobile technologies. These technologies are the foundation of digital economies and rely on closed user groups to ensure national security. Financial transactions of companies, regulatory organizations, and national governments are swift and technologically advanced, rendering the security of the telecommunications infrastructure in Nigeria of paramount importance. Effective examination and consideration of cybersecurity challenges and opportunities in Nigeria are essential for informing national policy debates and business strategy decisions concerning future development.

Current Cybersecurity Landscape in Nigeria

The Nigerian government, aware of the threats posed by cyber threats such as hacking, fraud, identity theft and cyber terrorism, and the paucity of effective security measures, has put a legal framework in place to protect online system users and to punish offenders. Certain sections of this framework also offer guidelines to users on the kinds of information that are prohibited or vulnerable to being abused if publicly disclosed. Although the Nigerian cyber security and data protection environment is as yet underdeveloped, a number of active private sector initiatives exist alongside government oversight to address the key threats.

Cyber-attacks in Nigeria have extended beyond virtual scams to include tactics aimed at disrupting power supplies and other critical services, and a 2016 costing exercise by the global consultancy company Booz Allen Hamilton estimated that the agency responsible for the digital economy, the National Information Technology Development Agency (NITDA), lost US$11.1 billion as a result of cybercrime. Nigerian organisations therefore face a range of common threats. Banks and other financial services firms have been targeted by malware designed to steal data and commit fraud, there has been a rise in phishing attacks exploiting the lack of critical information infrastructure protection, and Denial of Service (DoS) attacks are regularly used by individuals or groups seeking to extort money from online service providers. Insiders are also a risk to firms, as employees either act maliciously or inadvertently create vulnerabilities that allow an attacker to gain access to internal systems (Abdullahi Saulawa & K. Abubakar, 2014). Cybercriminals target online institutions and platforms in banking, telecommunications, airlines and a number of sectors of the economy. Organisations seeking to operate in the digital realm consistently fall victim to break-ins and defacements (Oluwafemi Jemilohun & Ifedayo Akomolede, 2015). Over the past seven or eight years, hackers have gained access to data on millions of customers' credit cards, including information such as expiry dates and CVV numbers.

The government's response to these risks and the shape of the cybersecurity components needed to fully underpin the digital economy continue to be debated. Government departments such as the Ministry of Communications have offered positive statements and reassurances, and the minister for communications has also engaged with the National Assembly to ensure that the on-going debates concerning a draft version of the 2015 National Cybersecurity Policy and Strategy are expedited. However, policymakers and other stakeholders continue to make the case that a lack of easy and widespread access to the internet is the main constraint on Nigeria realising the full set of Digital Economy benefits. Indeed at present the value of the Nigerian digital economy is relatively small—around 3 per cent of GDP. Addressing the acute digital divide therefore remains the fundamental challenge; Nigerians busy obtaining power and other basic infrastructure in their locality continue to be some way from broad

digital access and the 'rebalancing' of the economy needed to significantly alter the country's development pathway.

Key Cyber Threats

Nigeria's economy has surged in recent decades with communication and information technology as prime movers. The rapid growth of the digital economy, driven virtually exclusively by the telecommunication sector, is recognised worldwide as the cornerstone of a knowledge-driven, high opportunity economy that engenders inclusive growth. Generating awareness of online risks and pursuing self-protection measures are essential for enhancing online privacy and trust and for encouraging participation in the digital economy. Despite the dynamic and advanced infrastructure that has attracted a host of global players, the local cyber environment is weak and exposed to rapidly growing cyberthreats. Adequate legislative framework, law enforcement as well as public and business awareness, all of which underpin an effective cybersecurity ecosystem, are seen by the government as critical for safeguarding the digital economy in Nigeria. (Stella Adesina, 2017) (Oluwafemi Jemilohun & Ifedayo Akomolede, 2015)

Malware attacks represent a common cyber threat in Nigeria. Attackers exploit weaknesses in networks, systems, and programs to access personal information such as credit card details, passwords, usernames, or to disrupt access to personal data. In extreme cases, they may threaten to withhold private information unless a ransom is paid. These attacks typically spread through email attachments or malicious websites. Unique variants of ransomware in Nigeria include: - Small ransom chain mail. - Fake advertiser ransomware. - PC browse-lock. - Ransom downloader. (Oyenike Fayomi et al., 2015)

Phishing scams work by sending emails to victims that request verification of personal information through a link to a seemingly trustworthy source, allowing hackers to access financial data and other confidential information. Rich narrative emails appeal to emotions and myths of windfall fortunes (Stella Adesina, 2017) (Longe & Osofisan, 2011). Cybercrime related to phishing has significantly harmed the Nigerian economy and reputation. Nigeria notably ranks among the top sources of spam and phishing emails worldwide. A surge in phishing emails occurred in 2015 following the Central Bank of Nigeria's deadline for Bank Verification Number compliance. Fraud on e-payment platforms increased by 183% between 2013 and 2014. Large numbers of Nigerians have been arrested for online fraud—primarily lottery, jobs, and matrimonial scams (Abdullahi Saulawa & K. Abubakar, 2014). Such activities have undermined international trade and investor confidence, prompting skepticism about Nigerian financial instruments and the blacklisting of Nigerian ISPs and email providers. The Nigerian government responded by establishing the Nigerian Cybercrime Working Group in 2004 and the Directorate for Cyber Security in 2007.

Discovered in 1989, the term ransomware denotes a form of malicious software that blocks access to the victim's data or computer, demands a ransom payment, and upon receipt is supposed to restore access. The demand for ransom can be presented during bootup in what is termed ransom-boot, overwriting the master boot record and thereby preventing the system booting into Windows. The ransom demands can also encrypt files on the system, leaving the user with the choice of paying to gain back access; this variant is known as crypto-ransomware (Beaman et al., 2021). Attacks are often delivered though email phishing campaigns from addresses disguised to represent reputable organizations. The ransom note can be presented using the well-known abbreviation "! ! ! READ_IT_ ! ! !", a text file, a popup window, or web page displayed by the victim's computer. Individuals seeking to deal with an infection are encouraged not to pay the

ransom but instead seek professional assistance, but close to half of small businesses (48%) have been reported as paying the ransom when presented with a ransomware incident in the Nigerian context, thereby fuelling the attacks.

According to Adesina (2017), insider threats are considered one of the leading causes of cybercrimes and the biggest cybersecurity challenge facing Nigeria. An insider threat is posed from within an organization, by anyone who has authorized access to a system or data (R. C. Nurse et al., 2014). The insider could be malicious or could be inadvertently negligent. In Nigeria, insiders cause the loss of sensitive information, especially in financial institutions, government, and to affiliated third parties, for example, agents, vendors, or contractors. Physical and information assets are damaged. IT sabotage is another form of insider threat that involves the introduction of malware, tampering with systems or data, or disruption or destruction of hardware. For example, a number of Nigerian banks had from 2015 onwards experienced frequent denial of service attacks from insiders, which led to the loss of vital information relating to customers. Insider threats are exacerbated by poor password and account management policies and practices, which allow unfettered access to systems and data through the negligence of insiders.

Capacity issues plague many governmental and private sector organizations. Many lack the human, financial, and technical resources needed to implement security controls that can effectively handle the scale of threats encountered. There are not enough skilled cybersecurity personnel to satisfy the demand for employees able to manage evolving threat actors and technical attack vectors. Without an adequate baseline of trustworthiness in digital systems, organizations encounter major obstacles when building new innovative digital services and new forms of online engagement with customers and partners. Capacity requirements for appropriately skilled personnel combined with Nigeria's existing network architecture, technological base, and organizational priorities present a complex challenge to escalating digital security measures. An agile, high-quality, technology-enabled, digitally-based system can help drive the digital economy and unlock opportunities that will benefit the nation at large (Oyenike Fayomi et al., 2015).

Cybersecurity Awareness and Education

Cybersecurity awareness and education have emerged as key strategies for addressing the escalating cybercrime challenges faced by Nigerian society. Efforts to enhance cyber-hygiene among internet users focus on imparting knowledge, skills, and values necessary for the responsible use of internet technologies. A study involving students and staff at the University of Nigeria found that only about half possessed good cyber hygiene knowledge and behaviours, underscoring the need for organized training programmes (Ugwu et al., 2021). In developing countries, educational initiatives including cyber safety frameworks for primary schools and tailored learning platforms for young rural populations have been proposed to promote diversity and inclusion (Quayyum & Naper Freberg, 2023). Research indicates that integrating cybersecurity awareness into both policy formulation and educational curricula can contribute to the creation of safer online environments, particularly for vulnerable groups such as children and youth. Given the pervasiveness of cybercrime—driven by factors such as economic hardship and corruption—and the consequent threats to financial health, customer trust, and national security (O. Uwadia et al., 2006) , awareness-building and education remain critical components of Nigeria's national cybersecurity strategy.

As the Nigerian digital economy grows, so too do cybersecurity risks and threats. Public awareness campaigns are therefore vital to shaping the knowledge and attitude

of participants. Such campaigns educate people about cybercrime and how to avoid falling victim to it (Stella Adesina, 2017). Cyber-attacks thrive on vulnerabilities caused by ignorance, for example, the inevitable weak passwords most Internet users choose, and an uninformed individual is more likely to become the victim of a social engineering attack or a phishing scam. Cybersecurity awareness campaigns encourage the adoption of safe practices when online. In addition, awareness campaigns promote a sense of responsibility for the protection of computer systems and digital services. Cybersecurity is not just the preserve of IT experts, rather, everyone associated with a digital platform is responsible for its security. Awareness campaigns help ensure that users understand this, and are able to make appropriate decisions either as consumers or vendors.

ICT literacy is introduced in schools at an early stage. Tertiary institutions, polytechnics and technical colleges take the programme a notch higher with the study of National Information Technology Development Agency (NITDA) curriculum in ICT, which includes software programming, web development, networking and internet security, and the basics of cybersecurity. Unisys launched a contest for senior and secondary school students, focusing on identifying and cultivating cybersecurity skills among Nigerian teenagers (Abah ABAH & Onwu Iji, 2019) (Onwu & Abah, 2019). Developing cybersecurity technology and know-how is not a task for the government alone. Educational institutions, especially the universities and research centres, are making efforts towards developing the right solution.

Role of Government in Cybersecurity

Impressive policy initiatives and capacity planning are yet to translate into policy execution (IMHONOPI & M. URIM, 2015). Despite Nigerian officials publicly subscribing to a cybersecurity strategy of convergence, implementation has not been forthcoming in either the government or private sector. This lack of execution has produced a vacuum through which cyber threats and cybercrime permeate the digital business environment. The Nigerian government implemented a number of steps in the direction of Cyber Security (CS), some of which are listed below: • Establishing a computer emergency response team (ngCERT) under the Office of the National Security Adviser to address cyber threats and promote security research and development. • Prioritizing the National Cybersecurity Policy and Strategy to establish a legal framework for national security, governance, and stability. • Developing a National Cybersecurity Strategy designed to provide policy directions for securing information infrastructure and reducing cybercrime vulnerabilities. • Refocusing the enforcement agency to intensify the fight against cybercrime and reviewing the national security architecture to establish a Cybersecurity Agency. • Drafting an Information and Communication Bill to establish legal and regulatory authorities for the ICT sector in Nigeria (Oluwafemi Jemilohun & Ifedayo Akomolede, 2015) (O. Uwadia et al., 2006). Private/public sector engagement in cyber security is recognised as an effective tool to address the threat and reduce the effects of cybercrime. According to the Nigerian Communications Commission (NCC), efficient collaboration with other agencies is imperative for Nigeria's ongoing fight against cybercrime.

Risk Management Strategies

Cybersecurity risk is inherent in any online activity, and all organisations must manage that risk. Many companies employ a Chief Information Security Officer (CISO) and maintain an information security function. Risk management strategies—employed by these organisations to assess cybersecurity risk and determine appropriate safeguards—must support the business strategy by aligning with available resources, risk appetite and the existing enterprise architecture. Whereas some organisations

favour sophisticated quantitative risk approaches, most security professionals tend to apply qualitative frameworks; the industry standard Critical Security Controls (CSC) from the Center for Internet Security (CIS) recommends a qualitative approach combined with detailed, task-specific surveys. A robust general framework can be implemented with adoption of the CSC, which guide users through incremental acquisition of technical and procedural safeguards for common risk scenarios (Stella Adesina, 2017) (O. Uwadia et al., 2006). Organisations that face a growing cyber threat environment but lack detailed insider knowledge can implement sound, cost-effective risk management through application of the first ten CSC. They can then use the remaining controls to bolster resistance to targeted attacks, depending on the assessed adversary capability and intent. Effective risk management requires a clear understanding of how safeguards protect assets, and has the following features: • Priority-based selection of controls and safeguards. • Practical advice on how to carry out specific risk management tasks. • Facilitation of prioritisation within the organisation. • Alignment with the organisation's risk appetite. Risk management must be integrated; the interrelation between information and other organisational assets means that it cannot be a stand-alone activity. It must accommodate the changing nature of threats and be sensitive to fluctuating priorities and resources. Critical information infrastructure is defined by the United States Department of Homeland Security as systems and assets so vital that their destruction or damage would have a debilitating impact on security, ransom, the economy and public welfare. The Cross Sector Cyber Security Working Group (CSCSWG) has identified the six following domains: •Chemical sector. •Commercial facilities sector. •Communications sector. •Critical manufacturing sector. •Dams sector. •Defence industrial base. A risk assessment can be conducted with little or no detailed knowledge of the potential adversaries. A risk survey approach—which specifies the general adversary model, potential attack vectors, and an assessment of impact—can provide a quantitative or qualitative report highlighting controls and safeguards relevant to the organisation's risk appetite, the criticality of each asset, and the threats to which these assets are exposed. Guidance is also available under the ISO 31000 standards—that provide general principles and guidelines on risk management; legible, adaptable and reusable frameworks that respect the existing external contexts under which organisations operate; and tools that embed existing best practices, decrypt jargon, and yield intuitive results that are negotiable and auditable.

Future Trends in Cybersecurity

Nigeria's digital economy is at risk from cybercrime and activities such as illegal online shaming and identity theft, which increase all swelling losses. Diverse actors exploit vulnerabilities in commerce and finance to perpetuate cybercrime and undermine Nigeria's economic vitality (Stella Adesina, 2017). Reform and innovation in cybersecurity policy development and enforcement are critical. Nigeria must acknowledge that cybercrime, backed by foreign and organized crime syndicates, poses a significant continuing threat to its digital economy. Malicious programs have the potential to inflict lasting damage upon critical infrastructure, stunting growth and preventing the country from realizing the full benefits of its digital economy initiatives.

Emerging information technologies—from mobile money to the Internet of Things, artificial intelligence, robotics, and blockchain—will provide semi-automated tools that not only facilitate commerce and enhance security but also lower the bar for automation in cybercrime and other malicious activities. Nigerian Internet users, including home networks, banks, government servers, and industrial control and critical infrastructure facilities, are all vulnerable to attack, and all data on these systems are vulnerable to

deletion, alteration, or compromise.

Information systems and telecommunications have undergone significant transformation owing to the emergence of disruptive technologies such as artificial intelligence, cloud computing, data analytics, blockchain, big data, and cyber-physical systems. Within the Nigerian socio-economic context, such developments provide an opportunity for businesses to either transform or retrench. Businesses also stand the chance of establishing a strong presence locally and internationally. Recent studies reveal that 46% of African countries have established cybercrime units at the national police level, with a significant proportion of such units reporting either pre-established or ad hoc public-private partnerships at the national level (O. Uwadia et al., 2006). Many emerging technologies provide a new business frontier for Nigerian business enterprises. However, the rapid adoption of such technologies must be handled with care and due diligence (Stella Adesina, 2017).

Nigeria faces a wide range of cyber threats amid its growing digital economy; predicted threats remain loosely defined according to a wide spectrum of risk perceptions rather than actual instances or a clear sense of Nigeria's unique landscape. Ongoing exposure and adjacent international risks continue to deliver growing uncertainties as the country's digital ecosystem develops. Nigeria requires tailored, practical responses that help foster confidence and resilience, with room to evolve as new technology induces new disturbance (Stella Adesina, 2017).

International Cooperation in Cybersecurity

International cooperation is critical in combating cybercrime, as tools and targets ignore national boundaries; domestic measures alone are insufficient (Stella Adesina, 2017). Global political will and operational resolve are essential to stem the flow of attacks and prevailing gaps in legislation. International coordination has become even more critical because cyber criminals constantly change course to meet new enforcement policies, develop new tools and tactics, and use new opportunities within the legal framework to conduct their illicit operations. International partnerships enable the development of specialized information and intelligence sharing arrangements between nations and their law enforcement communities to allow timely and effective responses to international cyber incidents. Despite the Paris cybercrime convention having been ratified by almost every nation, including regional agreements at international levels, many countries still use national sovereignty as a justification to ignore reporting, referrals, and information exchanges. International cooperation will require the proper registration of agencies involved in cybersecurity and the proper use of existing surveillance hardware. Communications between law enforcement agencies and the intelligence community, the private sector, and international partners are necessary to ensure that information reaches the appropriate authority in time to take action to prevent or mitigate the effects of cyber attacks.

International cooperation occupies an increasingly prominent place in many official eGovernment policies and services around the world today. Given the absence of a global police force, cooperation of authorities concerned with cyber security across national borders cannot be overstated. Simply because borders are more porous in cyberspace and/or at least well respected should not serve interference. Cooperation can take place at different levels ranging from data exchanges to shared procurements, international multilateral law enforcement agreements, and bilateral government-to-government agreements and at many international organizations that are available in this field. Information sharing and knowledge exchange play a central role in this cooperation and the exchange of best practices. Policy cooperation between officials from different

governments is another area where countries can benefit from pooling efforts and sharing information (Stella Adesina, 2017).

Cybersecurity information-sharing governance structures constitute an ecosystem of diversity, trust, and tradeoffs. Policymakers regard cybersecurity information sharing as a solution but ascribe widely varying scopes to it. From 2009 to 2015, the United States debate centered on increasing private sector sharing, with laws such as the Cybersecurity Information Sharing Act addressing liability concerns. Historically, efforts like the U.S. Secret Service's Electronic Crimes Task Force (established 1995) and entities such as US-CERT established multiple information-sharing systems across federal agencies. Alongside these initiatives, private-sector sharing arrangements multiplied, creating a complex ecosystem of exchanges, platforms, and groups responsive to responsible disclosure, emerging threats, coordinated defense, and mutual aid. These developments unfolded through a process of negotiation, policy adoption, and cooperative modelling, propelled by government and industry. Whereas the Cybersecurity Information Sharing Act sought to enhance private-sector and government-private-sector sharing, it was enacted without a comprehensive mapping of the existing ecosystem. Legal liability issues, especially concerning privacy laws, figured prominently as barriers to information exchange. Nevertheless, the act's efficacy in improving information sharing remains indeterminate: analyses suggest limited effects (M. Sedenberg & X. Dempsey, 2018).

Conclusion

Nigeria's emerging digital economy offers enormous potential, but without proportional investment in strategies for protection, the nation remains vulnerable to cyber-threats (Abdullahi Saulawa & K. Abubakar, 2014). Security challenges adversely affect individual and organizational wellbeing, unleashing a cascade of economic consequences across all sectors. Substantial safeguards are imperative to protect assets and ensure safe, trustworthy, and transparent digital platforms. To overcome these obstacles, the government must collaborate closely with the private sector to review and enhance the existing cybersecurity framework, cultivate human and institutional capacity, and equip the growing digital economy with holistic security measures that enhance prevention, detection, response, and management of cybercrimes (Stella Adesina, 2017). Continuous reform of the regulatory framework is essential to sustain a conducive environment for the digital economy. Efforts to build awareness, bridge the capability gap, and provide relevant educational and training opportunities will play an important role in strengthening the cybersecurity posture of Nigeria's digital economy.

Author's Declaration:

The views and contents expressed in this research article are solely those of the author(s). The publisher, editors, and reviewers shall not be held responsible for any errors, ethical misconduct, copyright infringement, defamation, or any legal consequences arising from the content. All legal and moral responsibilities lie solely with the author(s)

References:

1. Abdullahi Saulawa, M. & K. Abubakar, M. (2014). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. https://core.ac.uk/download/234650033.pdf
2. Stella Adesina, O. (2017). Cybercrime and Poverty in Nigeria. https://core.ac.uk/download/236295899.pdf
3. Oluwafemi Jemilohun, B. & Ifedayo Akomolede, T. (2015). Legislating for Cyberspace: Challenges for the Nigerian Legislature. https://core.ac.uk/download/234650179.pdf

4. Oyenike Fayomi, O., Nelson Ndubisi, O., K. Ayo, C., Chidozie, F., & A. Ajayi, L. (2015). Cyber-Attack as a Menace to Effective Governance in Nigeria.
5. Longe, O. & Osofisan, A. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. https://core.ac.uk/download/231820776.pdf
6. Beaman, C., Barkworth, A., David Akande, T., Hakak, S., & Khurram Khan, M. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. ncbi.nlm.nih.gov
7. R. C. Nurse, J., A. Legg, P., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., & Creese, S. (2014). A critical reflection on the threat from human insiders - its nature, industry perceptions, and detection approaches. https://core.ac.uk/download/189720787.pdf
8. Jerome Orji, U. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. https://core.ac.uk/download/201167572.pdf
9. Akindele, R. (2017). Data protection in Nigeria: Addressing the multifarious challenges of a deficient legal system. https://core.ac.uk/download/160477225.pdf
10. Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., Atanda, A., & Ukwandu, E. (2021). Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene. https://arxiv.org/pdf/2103.06621
11. Quayyum, F. & Naper Freberg, G. (2023). Designing Cybersecurity Awareness Solutions for the Young People in Rural Developing Countries: The Need for Diversity and Inclusion. https://arxiv.org/pdf/2312.12073
12. O. Uwadia, C., O. Omogbadegun, Z., & P. Fasina, E. (2006). Cybercrime Pervasiveness, Consequences, and Sustainable Counter Strategies. [PDF]
13. Abah ABAH, J. & Onwu Iji, C. (2019). Internet Skills as a Measure of Digital Inclusion among Mathematics Education Students: Implications for Sustainable Human Capital Development in Nigeria. https://core.ac.uk/download/187537074.pdf
14. Onwu, C. & Abah, J. (2019). Internet Skills as a Measure of Digital Inclusion among Mathematics Education Students: Implications for Sustainable Human Capital Development in Nigeria. https://core.ac.uk/reader/217903910
15. IMHONOPI, D. & M. URIM, U. (2015). INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) AND GOVERNANCE IN NIGERIA: CHALLENGES AND PROSPECT. https://core.ac.uk/download/233940787.pdf
16. H. Mohammed, K., D. Mohammed, Y., & A. Solanke, A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. https://core.ac.uk/download/215437646.pdf
17. Liu, X., Fayaz Ahmad, S., Khalid Anser, M., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. ncbi.nlm.nih.gov
18. M. Sedenberg, E. & X. Dempsey, J. (2018). Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs. https://arxiv.org/pdf/1805.12266

Cite this Article-

"R.W. Urim", "Cyber security Challenges in Nigeria's Digital Economy", Procedure International Journal of Science and Technology (PIJST), ISSN: 2584-2617 (Online), Volume:2, Issue:1, January 2025.

Journal URL- https://www.pijst.com/

DOI- https://doi.org/10.62796/pijst.

Published Date- 06/01/2025