

STRENGTHENING CYBERSECURITY IN NIGERIA: A HOLISTIC APPROACH

Adekunle Emmanuel Makanjuola¹, Mary Mojirade Ayantunji²

¹Department of Social Studies, Federal College of Education

²Department of Arts & Social sciences Education, Lead City University

ABSTRACT: Given Nigeria's growing reliance on technology, it is imperative that the country take a comprehensive approach in order to strengthen its cybersecurity posture. This article provides an analysis of the current vulnerabilities, focusing on the limitations of the regulatory frameworks that are now in place, the degrees of public awareness, and the protection from vital infrastructure. As a result, it is recommended that a multi-pronged plan be proposed in order to solve these difficulties. The establishment of a comprehensive cybersecurity law, the implementation of national awareness campaigns and the incorporation of cybersecurity education into curriculums, the execution of vulnerability assessments and the enforcement of stricter protocols for critical infrastructure sectors, the investment in capacity building programmes to develop a skilled cybersecurity workforce, and the promotion of international cooperation to share best practices and threat intelligence are all included. Through the implementation of these interrelated measures, Nigeria is able to considerably boost its cybersecurity defences and develop a digital environment that is safer for its residents and enterprises.

KEYWORDS: *Cybersecurity, Holistic Approach, Nigeria, Digital Security, Capacity Building*

1. INTRODUCTION

Nigeria is currently experiencing a widespread and significant transformation in the digital realm. The 2024 Global System for Mobile Communications report reveals that mobile phone usage has reached remarkable levels, with more and more people using their handsets to browse the internet and carry out financial transactions [1]. Jumia's financial statement is evident that this spike has contributed to the growth of e-commerce, with online marketplaces making purchasing and commercial transactions easier [2]. The fintech innovation study revealed the incorporation of technology into everyday life, as seen by the emergence of start-ups providing mobile banking and digital payment services [3]. Nevertheless, this increasing reliance on technology is accompanied with negative consequences. The Nigerian Data Protection Commission (NDPC) report showed that Nigeria is confronted with a substantial predicament posed by cybercriminals that employ phishing, scams, identity theft, and financial fraud [4]. Ransomware attacks present an escalating danger to vital infrastructure and enterprises, with the potential to result in substantial financial damages [5]. Insufficient data security measures worsen the problem, making personal information susceptible to breaches and misuse [6]. The cyber dangers provide a genuine peril to Nigeria's economic progress, national security, and the confidence that residents place in digital platforms.

Nigeria's digital ecosystem is thriving, since there has been a significant increase in the adoption of mobile phones [1]. However, this reliance on digital technology exposes individuals, organisations, and essential infrastructure to a perilous network of cyber assaults. Cyber assaults can have severe repercussions. Individuals are highly vulnerable to cybercriminals who engage in phishing scams, identity theft, and financial fraud [4]. Envision a scenario where a teacher is deceived by a cunningly camouflaged email that seems to originate from their financial institution, leading them to unwittingly provide their login credentials. Subsequently, these pilfered login details can be employed to deplete their diligently accumulated funds, resulting in significant economic distress. Businesses are also susceptible.

Ransomware assaults, in which malevolent individuals encrypt a company's data and want a payment in exchange for its decryption, are becoming more prevalent [5]. An act of cyber intrusion targeting a prominent retailer has the potential to severely impair its functioning, resulting in financial losses, harm to its reputation, and potentially even workforce reductions. The most concerning dangers are associated with essential infrastructure. Power grids, transportation systems, and communication networks are susceptible to cyber attacks. A case study conducted in 2022, revealed that a power grid can be effectively targeted, resulting in the complete loss of electricity in entire cities [7]. This would lead to the disruption of crucial services and trigger widespread fear. The repercussions of these cascading impacts can severely undermine a nation's security and stability. The potential ramifications of cyber strikes in Nigeria are severe. To ensure the security of its inhabitants, enterprises, and key infrastructure, the nation must comprehend these risks and adopt strong cybersecurity measures, thereby promoting a safer digital future. The digital ecosystem in Nigeria is experiencing significant growth, but it is also plagued by numerous cyber risks. In order to properly address these hazards, a disjointed strategy will not be adequate. The adoption of a comprehensive approach to cybersecurity is thereby advocated [8]. This method surpasses mere technical solutions, incorporating a network of procedures that tackle weaknesses at several levels. Envision a meticulously maintained residence. A solid base guard against structural problems, while a robust roof provides protection from the weather. However, a house lacking locks renders it susceptible to trespassers. Adopting a holistic approach to cybersecurity is similar to strengthening the overall system. The statement recognises the interdependence of vulnerabilities: inadequate legal structures empower cybercriminals, while insufficient public information renders individuals susceptible to phishing assaults [9]. Simultaneously tackling these vulnerabilities, a holistic strategy enhances the entire cybersecurity posture. Moreover, cybersecurity does not rely solely on one individual. Collaboration among legislators, corporations, law enforcement agencies, and ordinary individuals is essential [10]. An all-encompassing approach promotes this collaboration, guaranteeing that each individual plays a crucial part in establishing a secure digital environment. Essentially, a holistic approach surpasses temporary solutions and constructs a resilient cybersecurity defence system, protecting Nigeria's digital realm for individuals, businesses, and the nation as a whole.

2. CURRENT STATE OF CYBERSECURITY IN NIGERIA

The digital revolution in Nigeria has both positive and negative consequences. As mobile phone usage increases rapidly [1], it creates opportunities for e-commerce and financial inclusion. However, it also exposes the country to an expanding network of cyber dangers. Regrettably, the present condition of cybersecurity in Nigeria exposes notable weaknesses. A significant issue arises from the legal structure. Although there are existing cybersecurity laws, scholars therefore, contend that these laws are fragmented and lack the necessary strength to effectively discourage cybercrime [11, 12]. This provides a secure refuge for malevolent individuals who take advantage of vulnerabilities to initiate phishing schemes, pilfer identities, and perpetrate financial deception [6]. Public awareness is also a challenging aspect. Research indicated a worrisome deficiency in cybersecurity literacy among a significant portion of the Nigerian population [13]. Their lack of awareness renders them more vulnerable to becoming targets of online scams and social engineering strategies. Envision receiving an email that appears to be authentic, requesting your banking information - lacking sufficient knowledge, it is simple to become a victim of such deceit.

Ultimately, Nigeria's crucial infrastructure, which serves as the foundation of the digital economy, is exposed to substantial weaknesses. The presence of outdated systems and inadequate security processes renders them very vulnerable to ransomware assaults, as emphasised in a recent case study [7]. An effective assault on a power grid, for instance, has the potential to incapacitate whole urban areas, resulting in significant economic turmoil and social upheaval. These vulnerabilities reveal a worrisome depiction of Nigeria's present state of cybersecurity. Nevertheless, by recognising these vulnerabilities

and embracing a comprehensive strategy, Nigeria may construct a more robust digital future for its populace and enterprises [11, 12].

3. CHALLENGES IN NIGERIAN CYBERSECURITY

The digital growth in Nigeria has both positive and negative consequences. Although it promotes economic expansion and involvement in the financial system, it also makes the country vulnerable to an increasing network of cyber risks. Regrettably, Nigeria has numerous significant obstacles that impede its capacity to adequately protect itself in the realm of cyberspace.

1. A Patchwork of Laws, Not a Cybersecurity Shield

The legislative framework for cybersecurity in Nigeria is currently fragmented and contains numerous vulnerabilities. Scholars have stated that, the existing sectoral regulations lack consistency and fail to effectively handle emerging and growing cyber dangers [9]. These weaknesses provide a secure environment for cybercriminals to exploit and carry out activities such as launching phishing scams, stealing identities, and committing financial fraud [6]. Implementing comprehensive cybersecurity legislation with explicit directives and more severe punishments will discourage cybercriminal activities and provide law enforcement with enhanced capabilities to investigate and bring legal action against cyber attacks with more efficiency [14].

2. When Knowledge is Power, Lack of Awareness Makes Nigerians Vulnerable

Studies indicate a worrisome deficiency in cybersecurity knowledge among a significant number of individuals in Nigeria [13]. The presence of this digital literacy gap increases their vulnerability to online scams and social engineering approaches. Envision receiving an email that appears to be authentic, requesting your banking information - lacking sufficient knowledge, it is simple to become a victim of such deceit. The poor awareness, as emphasised by scholars is worsened by the restricted availability of education and digital resources in rural populations [15]. Implementing public awareness programmes that specifically target different groups is essential in order to close the knowledge gap and enable Nigerians to securely traverse the digital world.

3. A Skill Gap Threatens Nigeria's Cybersecurity Defences

Nigeria is experiencing a severe scarcity of cybersecurity personnel that possess the requisite expertise to effectively counter advanced cyber attacks. Therefore, it is evident, that this deficiency in skills obstructs the country's capacity to enforce strong cybersecurity measures and adequately counter cyber threats [16]. Tertiary institutions and training institutes frequently do not have the capability to provide extensive cybersecurity programmes. This is imperative to enhance investment in this domain [16]. Developing a proficient workforce is crucial in order to acquire the necessary competence to meet the cybersecurity requirements of the nation.

4. Critical Infrastructure: A Fragile Lifeline in Need of Protection

Nigeria's crucial infrastructure, which serves as the foundation of the digital economy, is exposed to substantial vulnerabilities. For instance, electrical grids and financial institutions frequently depend on outdated technologies that have inherent vulnerabilities [17]. Obsolete technologies are highly vulnerable to cyber attacks, which greatly jeopardise both national security and economic stability. Moreover, the problem is worsened by the absence of strong security standards and regular updates to these systems. Failure to perform adequate maintenance and keep software up to date leaves critical infrastructure susceptible to exploitation [17].

4. HOLISTIC APPROACH TO STRENGTHENING CYBERSECURITY

The digital environment in Nigeria is experiencing significant expansion, however, this progress is accompanied by an increase in cyber risks. Conventional, incremental solutions are no longer sufficient.

To establish a strong cybersecurity defensive system, it is necessary to adopt a comprehensive approach, as suggested by experts such as [8]. This method extends beyond technology alone and includes a network of safeguards that target weaknesses at various levels.

1. Legal & Regulatory Framework: Building a Strong Foundation

A comprehensive legal framework is the foundation of a holistic strategy. Studies have emphasised that the existing fragmented legislation creates opportunities for cybercriminals to exploit [9]. An all-encompassing legislation on cybersecurity, as advocated would create explicit directives; discourage cybercrime by imposing more severe punishments, and enable law enforcement to efficiently counter cyber threats [18]. This legislative framework serves as the basis upon which other measures can be constructed.

2. Public Awareness & Education: Empowering Citizens

Cybersecurity is not solely a technological obstacle; it necessitates a collaborative endeavour that indicates a notable deficiency in cybersecurity knowledge among a substantial number of individuals in Nigeria [13]. The presence of this digital literacy gap renders people vulnerable to online scams and social engineering approaches. Envision receiving an email that appears to be authentic - lacking sufficient knowledge, it is simple to become a target of such deceit. Public awareness efforts play a vital role in closing this gap in knowledge [15]. Through the dissemination of knowledge on secure online habits and potential dangers, we enable individuals to actively contribute to the establishment of a protected digital environment.

3. Critical Infrastructure Protection: Shielding the Backbone

Nigeria's crucial infrastructure, which is the essential foundation of the digital economy, is exposed to substantial vulnerabilities. Obsolete systems and inadequate security measures make them vulnerable to cyber attacks, posing a threat to national security and economic stability [17]. A comprehensive approach gives top priority to the safeguarding of essential infrastructure. This entails doing vulnerability assessments, adopting strong security measures, and ensuring frequent system updates are enforced.

4. Capacity Building & Skills Development: Investing in the Workforce

The field of cybersecurity is a continuous struggle, and proficient experts are important in safeguarding against constantly changing dangers. The severe scarcity of cybersecurity experts in Nigeria is a pointer that lack of these talents impedes the country's capacity to enforce comprehensive security measures and successfully counter cyber threats [16]. It is therefore, essential to invest in capacity building programmes, for efficiency. Enhancing cybersecurity education at colleges and providing specialised training programmes are crucial measures to cultivate a proficient workforce capable of protecting the nation's digital future.

5. Technological Solutions: Equipping the Defenders

Technology is essential in every cybersecurity plan. Nevertheless, technology by itself is not a panacea. Efficient remedies must be executed inside the structure formed by the remaining foundations. This involves implementing firewalls, intrusion detection systems, and other security measures to actively monitor and safeguard against cyber threats.

6. International Cooperation: Sharing Intelligence, Building Alliances

The frontiers of cyber risks surpass geographical bounds and therefore necessitated the importance of international cooperation in sharing optimal methods, threat intelligence, and synchronised reactions to cyber threats [19]. Nigeria's cybersecurity posture is enhanced by collaboration with international organisations and other governments, contributing to a worldwide endeavour to address this persistent concern.

5. STRATEGIES AND INITIATIVES TO STRENGTHENING NIGERIA'S CYBERSECURITY

Nigeria's digital environment requires a strong and effective cybersecurity protection. An all-encompassing approach, incorporating multiple pillars, is essential for ensuring effective protection. Let us examine these fundamental principles and particular tactics and programmes that can be put into practice:

1. Legal & Regulatory Framework: Building a Strong Foundation

Create an all-encompassing legislation on cybersecurity that will precisely delineate cybercrimes, delineate investigation protocols, and institute more stringent sanctions for cyber offences [9]. Create a specialised cybercrime investigation division within law enforcement organisations to handle cybercrimes and enhance expertise in digital forensics. Adopt and approve pertinent global agreements on cybercrime and cooperate with international law enforcement organisations to locate and apprehend cybercriminals who operate in several countries.

2. Public Awareness & Education: Empowering Citizens

Implement a focused nationwide cybersecurity awareness initiative using diverse media channels to instruct individuals on best practices for online safety, methods to identify phishing frauds, and strategies to counter social engineering tactics. Integrate a cybersecurity component into the national curriculum across various educational levels, providing younger generations with essential digital literacy skills. Collaborate with non-governmental organisations (NGOs) and community leaders to coordinate workshops and seminars focused on promoting cybersecurity awareness in rural regions.

3. Critical Infrastructure Protection: Shielding the Backbone

Perform an extensive evaluation of the susceptibility of crucial infrastructure sectors such as power grids and banking institutions at a national level. Establish and implement rules tailored to critical infrastructure sectors, requiring strong security mechanisms and frequent system updates. Promote cooperation between governmental entities and commercial enterprises that possess and manage essential infrastructure to exchange optimal methods and allocate resources towards collaborative cybersecurity endeavours.

4. Capacity Building & Skills Development: Investing in the Workforce

Enhance cybersecurity education at higher education institutions by providing dedicated undergraduate and graduate programmes focused on cybersecurity. Deliver focused training programmes for IT personnel regarding evolving cyber risks, incident response, and security best practices. Facilitate collaborations between educational institutions and industry leaders to provide training programmes that are in line with the latest industry requirements.

5. Technological Solutions: Equipping the Defenders

Deploy firewalls, intrusion detection and prevention systems (IDS/IPS), and data encryption solutions to actively monitor and safeguard networks against cyber threats. Deploy vulnerability management systems to detect and rectify security vulnerabilities in systems and applications. Conduct thorough investigation and examination of the capabilities of technologies such as blockchain for safeguarding data storage and artificial intelligence for identifying and reducing risks.

6. International Cooperation: Sharing Intelligence, Building Alliances

Collaborate with regional cybersecurity organisations such as the African Union's African Cybersecurity and Information Assurance Agency (CAIAA) to exchange optimal methods and information regarding potential risks. Formulate bilateral or multilateral agreements with foreign nations to streamline the exchange of information regarding cyber risks and enable prompt communication and coordinated actions in response. Enhance the expertise of cybersecurity professionals by participating in international training programmes provided by organisations such as the International Telecommunication Union (ITU).

6. BENEFITS OF A HOLISTIC APPROACH

The digital landscape in Nigeria is both advantageous and disadvantageous. Although it facilitates economic expansion and promotes financial access, it also exposes the country to an increasing network of cyber risks. Conventional, incremental solutions are no longer sufficient. An all-encompassing cybersecurity strategy, akin to a heavily walled castle, necessitates robust defences on various fronts. By targeting weaknesses at several levels, this method has the potential to greatly enhance Nigeria's digital security position.

An effective defence against cybercrime begins with a robust legal framework. Stringent cybersecurity legislation with severe sanctions discourages offenders and enables law enforcement to efficiently investigate and punish cyber assaults. This fosters confidence in the digital realm, instilling a sense of security among individuals when engaging in online transactions. Public awareness campaigns hold equal significance. By providing citizens with knowledge and skills to recognise and prevent online dangers, they are empowered to actively protect the digital realm. Citizens, no longer susceptible to phishing scams, have formed a formidable barrier against cybercrime. Firewalls and intrusion detection systems are essential components of advanced security measures. These solutions actively oversee and safeguard networks, promoting a more secure environment for businesses to function and carry out online transactions. This resilient defence mechanism establishes the basis for a flourishing digital economy.

Investing in cybersecurity education and training programmes enhances the internal resilience of the system. An adept labour force can actively detect and resolve weaknesses in vital infrastructure, such as electricity networks and financial establishments. These specialists serve as the protectors of the fundamental infrastructure of the digital economy, ensuring that vital services continue to function and defending the security and stability of the nation's economy. Ultimately, international collaboration is crucial. Nigeria can enhance its defences and provide a more secure digital environment for everyone by collaborating with other nations and organisations to exchange best practices and threat intelligence. This worldwide endeavour guarantees a more secure and affluent future for all individuals.

7. CONCLUSION

Nigeria's digital revolution is a double-edged sword. While it unlocks doors to economic growth and financial inclusion, it also exposes the nation to a growing web of cyber threats. Imagine trying to defend a grand castle with just a single, rickety gate – that's the vulnerability of a piecemeal approach to cybersecurity. A holistic approach, however, is like fortifying the entire castle. This comprehensive strategy strengthens Nigeria's defences on multiple fronts, building a secure digital environment for all. These include: strong legal walls, public awareness Ramparts, technological bulwarks, skilled workforce watchtowers and an international alliances.

Therefore, the benefits of this holistic approach are far-reaching. Clear laws and an empowered citizenry breed trust in online transactions, fostering a thriving digital economy. Secured critical infrastructure ensures a stable national security and economic climate. With increased confidence in the digital space, businesses and citizens can operate and flourish. Building this secure digital castle requires a collective effort from policymakers, businesses, individuals, and educational institutions. By working together, we can transform Nigeria's digital landscape into a secure and prosperous space for all.

RECOMMENDATIONS

1. Assume a leadership role by implementing comprehensive cybersecurity legislation, allocating resources towards public awareness initiatives to educate the population, and promoting international cooperation to address cyber threats at a worldwide level.

2. Employ strong security policies to safeguard their digital assets, educate staff on optimal cybersecurity practices, and collaborate with necessary authorities to exchange threat intelligence and enhance the defensive network.
3. Employ appropriate online hygiene practices such as utilising robust passwords, regularly updating software, and exercising caution when encountering dubious emails and links. Notify the authorities of any suspected cybercrime in order to aid them in tracing and capturing the culprits.
4. Incorporate cybersecurity modules into the curriculum at every educational level, providing future generations with the necessary information and abilities to properly navigate the digital realm.
5. Conduct workshops and seminars in rural regions to address the digital knowledge gap and empower communities to enhance their online security.
6. Facilitate cooperation among educational institutions, corporations, and government organisations. This collaboration has the potential to facilitate the creation of specialised training programmes and the sharing of optimal methods, ultimately enhancing cybersecurity for all.

REFERENCES

- [1]. GSMA (2024). *The Mobile Economy Sub-Saharan Africa 2024*. <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf>
- [2]. Jumia 2023. *Jumia Group Financial Statements 2023*. [https://www.google.com/search?q=Jumia+\(2023\)+Jumia+Group+Financial+Statements+2023+%5BFinancial+Statement%5D&oq=Jumia+\(2023\)+Jumia+Group+Financial+Statements+2023+%5BFinancial+Statement%5D&aqs=chrome..69i57.6692870j0j15&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=Jumia+(2023)+Jumia+Group+Financial+Statements+2023+%5BFinancial+Statement%5D&oq=Jumia+(2023)+Jumia+Group+Financial+Statements+2023+%5BFinancial+Statement%5D&aqs=chrome..69i57.6692870j0j15&sourceid=chrome&ie=UTF-8)
- [3]. Pricewaterhouse Coopers Nigeria (PwC Nigeria) 2023. *Nigeria Fintech Report 2023*. <https://www.pwc.com/ng/en/assets/pdf/fintech-banking-sector-nigeria.pdf>
- [4]. Nigerian Data Protection Commission (NDPC) (2023) *Nigerian Cybersecurity Report 2023*. <https://ndpc.gov.ng/Files/AnnualReport2023.pdf>
- [5]. Cyber Security Experts of Nigeria (CSEAN) 2024. *National Cyber Threat Forecast 2024*. <https://csean.org.ng/national-cyber-threat-forecast-2024/>
- [6]. Nigeria Data Protection Bureau (NDPB) 2022. *Annual Report 2022*. <https://csean.org.ng/national-cyber-threat-forecast-2024/>
- [7]. Atlantic Council 2022. *Securing the Energy Transition against Cyber Threats: Report of the Atlantic Council Task Force on Cybersecurity and the Energy Transition*. <https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Securing-the-Energy-Transition-against-Cyber-Threats.pdf>
- [8]. Chernov, D., & Sornette, D. 2020. *Critical risks of different economic sectors. Based on the Analysis of More Than, 500*. Switzerland: Springer Cham
- [9]. Sibe, R. T., & Kaunert, C. 2024. *Cyber Crime in Nigeria - Reviewing the Problems*. In *Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria* (pp. 19-55). Cham: Springer Nature Switzerland.

- [10]. Hu, M. 2024. National Security and Federalizing Data Privacy Infrastructure for AI Governance. *William & Mary Law School Research Paper*, (09-488).
- [11]. Akongburo, R. A., Boshe, P., Dei-Tutu, S. A., & Hennemann, M. (Eds.). 2024. *African Data Protection Laws: Regulation, Policy, and Practice* (Vol. 3). Walter de Gruyter GmbH & Co KG.
- [12]. Katagiri, N. 2024. Why Soft Measures Are Too Soft: International Law and Norms. In *How Liberal Democracies Defend Their Cyber Networks from Hackers: Strategies of Deterrence* (pp. 77-94). Cham: Springer Nature Switzerland.
- [13]. Essien, E. S., & Edun, E. E. 2024. Digitalizing cyber security for data management in higher education: Implication for Educational Management in Nigeria. *International Journal of Education and National Development*, 2(1), 70-78.
- [14]. Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. 2024. A Comprehensive Analytical Review on Cybercrime in West Africa. *arXiv preprint arXiv:2402.01649*. <https://www.arxiv.org/pdf/2402.01649>
- [15]. Kuteesa, K. N., Akpuokwe, C. U., & Udeh, C. A. 2024. Theoretical perspectives on digital divide and ICT access: comparative study of rural communities in Africa and the United States. *Computer Science & IT Research Journal*, 5(4), 839-849.
- [16]. Aliyu, A. A. 2024. A Multi-Pronged Framework for a Cyber-Secure Nigeria. *Scientific and Practical Cyber Security Journal (SPCSJ)* 8(1): 69 – 75 ISSN 2587-4667
- [17]. Usama, M., Ullah, U., & Sajid, A. 2024. Cyber Attacks against Intelligent Transportation Systems. In *Cyber Security for Next-Generation Computing Technologies* (pp. 190-230). CRC Press.
- [18]. Hiller, J., Kisska-Schulze, K., & Shackelford, S. 2024. Cybersecurity carrots and sticks. *American Business Law Journal*, 61(1), 5-29.
- [19]. Rasel, M. 2024. Synergizing Cyber Threat Intelligence Sharing and Risk Assessment for Enhanced Government Cybersecurity: A Holistic Approach. *Journal Environmental Sciences and Technology*, 3(1), 649-673.