*e-ISSN: 3027-0650*
*Vol. 2, Issue 1, pp182-195, November 6 -9, 2024*

# CYBER SECURITY AWARENESS IN DEVELOPING COUNTRIES IN AFRICA: LESSONS FROM NIGERIA

**Oni Damilola**

Department of Informatics & Computer Engineering International School Vietnam National University - Hanoi, Vietnam
**E-mail**: igbagbooluwadamilola@gmail.com

## ABSTRACT

This research investigates the dynamics of cyber security awareness in the African context, drawing insightful lessons from Nigeria's experience. With the escalating digital landscape across Africa, understanding the role of cyber security awareness becomes crucial. This study delves into the multifaceted dimensions of cyber security awareness programs, exploring their design, implementation, and impact. It sheds light on Nigeria's unique position as a prominent player in the African technological landscape and examines how its initiatives have contributed to enhancing cyber security awareness. By dissecting Nigeria's strategies, challenges, and successes, this research abstract identifies key lessons that can be extrapolated to other African nations. Through a meticulous analysis of Nigeria's cyber security awareness initiatives, this research uncovers strategies that have effectively engaged various sectors of society, including government, private industry, and civil society. Furthermore, the research delves into the challenges encountered, such as the digital divide and evolving cyber threats, which provide insights into tailoring awareness campaigns to address region-specific concerns. The work also shed-light on how Nigeria's experiences highlight the importance of collaboration between national and international stakeholders in bolstering cyber security resilience. By extrapolating these lessons, this research underscores the potential for other African countries to adopt similar strategies, thus fortifying their cyber security landscapes.

**KEYWORDS:** Cybersecurity, Africa, Nigeria, Digital.

## 1 INTRODUCTION

### INTERNET IN NIGERIA

The internet, an interconnected global network of information and communication, has become an indispensable part of modern life. Its journey from inception to ubiquity has been nothing short of innovation, as it has also transformed the way we perceive the world: "The electromagnetic discoveries have recreated the simultaneous 'field' in all human affairs, so that the human family now exists under conditions of a 'global village,'' stated Marshal McLuhan[1].

McLuhan's concept of the global village refers to the entire world coming together under the tent of technology, with diverse locations across the globe having the potential to connect. Studies reveal that the evolution of the internet is not a one-time engulfing phenomenon; many parts of the world joined the train as the digital tide surged. Nigeria, once dominated by traditional forms of communication, witnessed the pioneering introduction of the internet in the early 1990s.

Spearheaded by the Nigerian government, in 1991, the country’s first Internet Service Provider (ISP), named The National Center for Communication Technologies (NCCT), and was founded. This dawn of the modern internet age paved the way for a digital revolution. More ISPs like Nitel, Interswitch, and Vee Network came into the picture in the mid-1990s, with increasing investments in technological infrastructure to establish reliable internet connectivity[2].

[1] Georgiadou, “McLuhan’s Global Village and the Internet.”
[2] “Detailed History of Internet in Nigeria - History of Nigeria.”

6th Despite the limited online representation of Nigerians in 1999, internet accessibility in Nigeria underwent swift expansion during the early 2000s. On August, 2001, the mobile system was introduced to the Nigerian market and society, marking the third year of former President Olusegun Obasanjo's initial term[3].

The introduction of GSM technology to the nation led to a sudden or gradual cessation of the troublesome and extensively criticized offerings of the Nigerian Telecommunications Limited (NITEL), which previously held a monopoly on telecommunications and data services in Nigeria. Right from the beginning, it was evident that the emerging era of wireless communications held superior services, prospects, and commitments for Nigerians.

ECONET Wireless is credited with placing the first live GSM call in the country on June 8, 2001[4], making it the inaugural network provider to do so. MTN quickly followed suit, being established on May 16, 2001, but its operations commenced in August of the same year. Initially, the Nigerian government granted licenses to only three companies: Econet Wireless, MTN, and MTEL. GSM services were initially introduced in Lagos, followed by Abuja, and then Port Harcourt. The new calling services were launched within the 900 and 1800 MHz spectrum, with charges set at N50 per minute due to the absence of a per-second billing system. This system persisted until Mike Adenuga's Globacom Nigeria Limited (Glo) entered the market in 2003, introducing per-second billing.

A report from the International Telecommunications Union focused on telecommunications development across nations from 1996 to 2009. Updated in July 16, 2010, the data regarding Nigeria revealed that internet usage among every 100 individuals surveyed in 1996 was at 0% and remained consistent for four years. Only by the close of the year 2000 did this figure rise, albeit insignificantly, to a surprising 0.3%. From 2002 to 2004, the percentage climbed to 1.5%. As stated by Adomi in 2005, Nigeria had a total of 750,000 internet users, representing 0.5 percent of the population by late 2003. Four years later, in 2007, this percentage escalated to 7%, and rapidly ascended further in 2008, reaching a peak of 15.9%[5].

Since then, there has been consistent exponential growth in the sector, with about 100-120 million Nigerians connected to the internet as of 2019 (NOIPolls, 2019; Russon, 2020). This growth in the number of internet users in 2019 was much expected after the 28 million internet users recorded in 2012 jumped impressively to 103 million users in May 2018. This figure suggests that only 55% of the Nigerian population is connected to the internet.

In 2020, the Nigerian government projected to increase broadband accessibility and have 70% of the population connected to broadband by 2025. This can be linked to the surge in internet subscriptions witnessed in the country, as the Nigerian Communications Commission recorded that the first quarter of 2023 saw the number of internet users grow by 1.7%, with over 2.7 million new internet users, making the total number 157.5 million as of March 2023, added to the 154.8 million recorded in December 2022[6].

However, challenges emerged alongside progress. Cyber security and privacy concerns underscored the need for robust online protection measures, as cybercrime is a growing trend with the internet's continued penetration into every sector of society and the expanding digital landscape. In November 2022, Business Day, a national newspaper, reported that Nigeria recorded a 174% increase in cybercrime in six months, solidifying its 16th position in the world cybercrime ranking.

Nigeria, like many other countries, faces specific challenges when it comes to cybercrime. Factors such as limited cyber security awareness, weak legislation and law enforcement, and socio-economic conditions contribute to the prevalence of cybercriminal activities. It is imperative for individuals in Nigeria to be vigilant and take proactive measures to protect themselves from cyber threats, particularly on social media platforms. Oni Damilola et al "Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention 2023[7]"

[3] Ubabudu, "The Effectiveness of Global System Mobile Providers' Services on Communication in Nigeria."
[4] "Econet Founder Reveals Story behind Company's Downfall in Nigeria."
[5] "Study on International Internet Connectivity in Sub-Saharan Africa."
[6] Jaiyeola, "$461m Investment Gap Slows Nigeria's Internet Coverage."
[7] International School Vietnam National University - Hanoi, Vietnam et al., "Cybercrime On Social Media In Nigeria."

Given the intricate nature of cyber security, it's evident that a crucial approach to mitigating its impact involves the formulation of stronger regulations and the steadfast enforcement of these laws. With the ongoing expansion of the digital landscape and the increasing sophistication of cyber threats, fostering an innovative culture requires an unwavering commitment to sustained support and robust infrastructure. This research initiative is poised to thoroughly explore the multifaceted domain of cyber security, shedding light on the path towards a future for Nigeria that is digitally secure and empowered.

## 2 THE POLITICAL ECONOMY OF CYBERSECURITY IN NIGERIA

Cybersecurity in Nigeria is shaped by a complex interplay of various actors, each with their roles, interests, and influence. The political economy of cybersecurity encompasses the following key players:

1. **GOVERNMENT INSTITUTIONS:** The government, through various agencies, plays a central role in shaping the cybersecurity landscape. It is responsible for creating the legal and regulatory framework, enforcing laws, and fostering an environment conducive to cybersecurity innovation. Key institutions include:

- **National Information Technology Development Agency (NITDA):** They Oversees IT development and cybersecurity policies, including the Digital Literacy and Capacity Development (DLCD) program[8].

- **NIGERIAN COMMUNICATIONS COMMISSION (NCC):** Regulates the telecommunications sector, which is critical for cybersecurity, especially concerning data protection and privacy.
- **Economic and Financial Crimes Commission (EFCC):** They  Focuses on investigating and prosecuting cybercrime.[9]
- **NIGERIA COMPUTER EMERGENCY RESPONSE TEAM (NGCERT):** Coordinates responses to cybersecurity threats and incidents.[10]

2. **CIVIL SOCIETY ORGANIZATIONS (CSOS):** They play an important role in raising public awareness about cybersecurity issues, advocating for stronger protections, and providing education and resources to vulnerable populations. They often fill gaps left by the government, especially in rural areas where access to technology and cybersecurity education is limited.

3. **ACADEMIA:** Academic institutions contribute to the cybersecurity ecosystem by conducting research, developing new technologies, and training the next generation of cybersecurity professionals. Universities and research institutes are also key players in advancing theoretical and practical knowledge in cybersecurity, although Nigerian academic institutions often face funding constraints, which limit their capacity to conduct cutting-edge research and develop new technologies. Additionally, there is a gap between academic research and its practical application in the cybersecurity industry.

## 3 ROLES OF CYBERSECURITY AWARENESS IN DEVELOPING NIGERIA

The integration of the internet has become increasingly intertwined with our daily lives, encompassing not only individuals but also small businesses, large corporations, and even countries. Its remarkable evolution over recent decades

[8] "Cyber Security – NITDA."
[9] "Economic and Financial Crimes Commission - EFCC - EFCC Reaffirms Commitment to Fight against Cyber Crimes."
[10] "ngCERT | Security Quality Management."

has had a profound impact. Undoubtedly, the internet has significantly and positively influenced communication, opened up new business avenues, and provided countries with opportunities and capabilities for electronic governance. Virtually every aspect of human endeavor now relies on the internet, permeating our existence. With a diverse array of smart devices, advanced technologies, wireless connectivity, and the Internet of Things (IoT), accessing the internet has remarkably simplified both life and work, achievable with just a click or tap, as data seamlessly traverses the expansive realm known as cyberspace.

Cyberspace is characterized as an electronic medium or a virtual computer realm that interconnects various networks. The connections between these networks collectively create a multifaceted global network of computers, facilitating online communication among cyber users. The integration of the internet into everyday activities is so pervasive that many users unknowingly navigate between the physical world and the cyberspace. As data exchanges, encompassing activities like socializing, education, entertainment, and business, traverse cyberspace, there is a latent risk of malicious activities occurring. These malevolent acts, collectively termed as cyber crimes, pose a potential threat to cyber users, leading to damages that are often substantial and challenging to reverse.

As a computer-oriented crime, cybercrime revolves around criminal activities involving a network, a computer, or networked devices. Generally, a computer, a computer network or a networked device is used to commit the crime or may even be the target of the criminal act [11]. Typically directed at compromising the security, privacy, and financial well-being of individuals, organizations, or countries, cyber crimes often result in reputational damage and financial losses. The targets of these criminal activities face significant threats that extend beyond digital breaches, impacting their overall integrity and economic stability. Ibrahim (2016), identified three primary factors contributing to cyber crimes in Nigeria: socioeconomic, psychosocial, and geopolitical. These factors, according to the author, present challenges to the statistical data used to analyze cybercrime incidents across the country[12].

The emergence of cybercrime has given rise to contemporary concepts, notably cybersecurity. Cybersecurity is essentially the practice of safeguarding computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. However, the effectiveness of cybersecurity relies heavily on the awareness and consciousness of cyber users. Consequently, awareness and education constitute the primary defense against cybercrimes. Oforji et al (2017), conducted a study on cybersecurity and its associated challenges in Nigeria, providing recommendations to address the growing threat of cybercrime. Similarly, in the work by Uwadia and Eti, (2018), the authors emphasized that the escalating unemployment rates contribute to the increasing incidents of cybercrime in Nigeria. Despite these challenges, the legislative branch has taken a step by passing a bill to address issues related to cybercrime.

In a separate study, Osho et al (2015) presented a qualitative analysis of the cybersecurity policy and strategy in Nigeria. The authors examined the Nigerian National Cyber Security Policy and Strategy by employing selected harmonized strategy developmental frameworks and conducted a comparative evaluation with similar documents from other chosen nations. The findings revealed that, while the document largely met expectations in terms of content, it overlooked certain critical aspects affecting cyber security across various sectors of the Nigerian economy. Dambo et al (2017), in their exploration of cyberspace technology, underscored that cyber security has evolved into a matter of national concern in Nigeria due to the significant threat posed by cybercrime activities. Despite the incorporation of built-in firewall security software in modern computers and mobile phones, the authors argued that these technologies are not entirely foolproof, leaving users' information vulnerable. Hassan et al (2012), identified urbanization, unemployment, and ineffective enforcement of cybercrime legislation as causative factors for cyber crimes in Nigeria. The authors recommended that individuals or corporate entities take proactive measures to safeguard their IT infrastructure, emphasizing the necessity for the government to rigorously enforce cybercrime laws.

According to Oni et al (2023), Nigeria, a country with a population of over 200 million had over 31.6 million active social media users. With most popular social media platforms with WhatsApp having over (95%) users, Facebook having

[11] "What Is Cybercrime?"

[12] "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals - ScienceDirect."

over (88.8%), Facebook Messenger having over (69.9%), Instagram having over (69.4%) and Twitter having over (61.2%). With a high number of users this social media platform is the most popular social media platform used by cybercriminals in Nigeria. These platforms are popular because they allow cybercriminals to reach a large number of people and to build trust with their victims.[13]

Considering Nigeria's expanding population of cyber users (Nigerian Bureau of Statistics, 2020), there is an anticipation of increased information exchange within the cyberspace, making it susceptible to exploitation. Safeguarding this information has become crucial for cyber user security and economic stability. Hence, the role of cybersecurity awareness among users becomes pivotal in thwarting cyber-attacks by online predators and ensuring overall cybersecurity. It underscores the importance of proactive measures and education in fortifying the digital landscape.[14]

## 4. COMBATING CYBERCRIME AND MALICIOUS COMPUTER ACTIVITIES IN NIGERIA

Cybercrime, which refers to illegal activities conducted using computers and the internet, including hacking, phishing, online fraud, identity theft, and more, exploits digital technology to steal, deceive, disrupt, or harm individuals, organizations, or society, posing significant risks to data security, privacy, and financial well-being. The term "cybercrime" can be used to describe any criminal activity involving computers or the internet network (Okeshola, 2013)[15].

According to Maitanmi (2013), cybercrime is a complex phenomenon. He describes it as more than just defrauding individuals; it involves criminals utilizing computers as tools and the internet as a means to achieve various objectives. These objectives can include illegal downloading of music files and films, piracy, spam mailing, and similar activities. Cybercrime often arises from the misuse or abuse of internet services[16].

As our world becomes increasingly interconnected, these developments allow for enormous gains in productivity, efficiency, and communication. However, they also create vulnerabilities that can potentially devastate a country. The threat of cybercrime has grown exponentially, posing substantial challenges to nations worldwide. This pervasive global issue has firmly established its presence within the borders of Nigeria.

The concept of cybercrime has a historical background. It was found that the first published report of cybercrime dates back to the 1960s, occurring on mainframe computers (Maitanmi, 2013)[17]. At that time, these computers were not connected to the internet or other systems, and the perpetrators were often employees within the company. Therefore, it was referred to as computer crime rather than cybercrime.

In Nigeria, cybercrime has emerged as a primary avenue for embezzling money and conducting business espionage. According to the Nigerian Deposit Insurance Company's report, Nigeria incurred losses of 15.15 billion Naira (approximately $43 million in 2019) due to fraud in the banking sector alone in 2018. This amount marked a staggering increase of 539% compared to the 2.37 billion Naira recorded in 2017, with cybercrime being the predominant contributor. The victims of cybercrime span across the financial sector, other institutions, and individuals in various jurisdictions. Internet fraud is primarily motivated by financial gain[18].

Internet fraud can be traced back to Advanced Fee Fraud, a fraudulent scheme believed to have originated in West Africa[19]. This scheme has gained global recognition, particularly being associated with Nigeria, which has led to its nickname "Yahoo-Yahoo," with the "419" code referring to Nigeria's criminal code for fraud. In addition to having one of the highest average losses per victim, Nigerians are also reported to engage in the second most reported cyber crimes. According to Symantec Corporation and the African Union, a significant portion of online scammers use Nigerian Internet Protocol (IP) addresses, with 46% of the email addresses associated with these scams originating from Nigeria.

[13] International School Vietnam National University - Hanoi, Vietnam et al., “Cybercrime On Social Media In Nigeria.”

[14] “Cybersecurity and Cybercrime Combatting Culture for African Police Services | SpringerLink.”

[15] Galle, “A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development.”

[16] Ahmad, “CYBER CRIME AND THE SOCIOLOGICAL IMPLICATION IN THE NIGERIA’S TERTIARY EDUCATION SYSTEM.”

[17] Galle, “A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development.”

[18] Tade, “Electronic Banking Fraud in Nigeria.”

[19] “Scams and Fraudulent Investment Schemes That Misuse Our Name.”

According to Check Point, a global cybersecurity vendor, as of 2016, Nigeria was ranked as the 16th highest country in terms of vulnerabilities to cyberattacks in Africa (Ewepu, 2016). This prevalence of cybercrime not only compromises the nation's efforts to uphold national security but also fosters negative perceptions that leave a lasting mark on the country's global reputation. A significant factor contributing to the widespread growth of cybercrime in Nigeria is the prevalent issue of unemployment and poverty. The country faces an unemployment rate of 23.1%, with youth unemployment accounting for a substantial 55.4% of that figure. Nationally, a staggering 40.1% (approximately 82.9 million people) of Nigerians are living below the poverty line. Furthermore, four out of every ten individuals in Nigeria have per capita expenditures that fall below N137,430 (equivalent to $355) annually[20].

The number of Nigerians apprehended for fraudulent activities conducted through broadcasting stations is notably higher compared to citizens of other countries. To gauge the severity of cybercrime in Nigeria, it is essential to analyze past convictions of individuals engaged in such activities. For instance, in 2019, a notorious Nigerian cybercriminal, Ramon Olorunwa Abbas, widely known as "Hushpuppi," was arrested and subsequently convicted for his participation in a global cyber fraud scheme. His case attracted international attention, highlighting the scale and audacity of cybercriminal operations originating from Nigeria. Likewise, in 2020, a Nigerian man named Obinwanne Okeke, commonly known as "Invictus Obi," faced conviction in the United States for masterminding a multi-million-dollar online fraud scheme. These prominent cases not only illustrate the international reach of Nigerian cybercriminals but also underscore the urgency of implementing comprehensive cybersecurity measures within the country.

Nigeria has implemented various preventive measures to combat cybercrime. These measures include the establishment of organizations such as the Nigerian Communications Commission (NCC) and the Nigeria Computer Emergency Response Team (ngCERT) to oversee cybersecurity and respond to cyber threats. The Economic and Financial Crimes Commission (EFCC) primarily focuses on investigation, while the Nigerian Police Force maintains a dedicated cybercrime unit tasked with cracking down on internet fraud. Furthermore, the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 provides a legal framework to address various forms of cybercrime.

In recent years, Nigeria has also emphasized cybersecurity awareness and education to help citizens protect themselves from online threats. While progress has been made, the fight against cybercrime remains an ongoing challenge, given the evolving nature of digital threats. Continued efforts in legislation, technology infrastructure, and international collaboration are essential to curb cybercrime in Nigeria effectively.

## 5 LESSONS LEARNED IN CYBERSECURITY AWARENESS FOR NIGERIA

Nigeria's rapid digital transformation presents both exciting opportunities and significant challenges. As the nation embraces the power of the internet and mobile technology, ensuring the safety and security of its citizens online becomes paramount. Here, we delve into key lessons learned from Nigeria's journey in raising cybersecurity awareness, highlighting both successes and areas for improvement.

### 1. EARLY AND CONTINUOUS EDUCATION: BUILDING A GENERATION OF CYBERSECURITY AWARE CITIZENS

At the heart of a robust cybersecurity posture lies a well-informed citizenry. Nigeria has recognized this crucial element, and efforts to integrate cybersecurity education into the national curriculum at all levels are a positive step towards building a generation of cybersecurity aware citizens.

**Laying the Foundation:**

- **Starting Young:** Integrating cyber security lessons into the primary school curriculum equips young Nigerians with a fundamental understanding of online safety from a young age. These lessons can focus on basic concepts like strong password creation, identifying suspicious emails, and responsible online behavior.
- **Age-Appropriate Progression:** As students' progress through secondary and higher education, the complexity of cyber security education should increase. This could involve topics like cyber bullying, social engineering tactics, data privacy principles, and secure browsing habits.

[20] Tredger, "Mobile-First Status a Chink in Africa's Security Armour?"

- **Interactive Learning:** Traditional classroom lectures can be complemented with interactive learning methods. Gamified simulations, ethical hacking scenarios, and online quizzes can make learning engaging and ensure students retain key concepts.

**Initiatives and Role Models:**

- **The National Information Technology Development Agency's (NITDA) "Digital Literacy and Capacity Development" (DLCD)** serves as a model for equipping young Nigerians with the foundation for safe online practices. The DLCD provides resources and training programs for educators, ensuring they can effectively deliver cyber security awareness lessons.

**Beyond the Classroom:**

- **Parental Involvement:** Educating parents and guardians is crucial. Workshops on online safety for parents can equip them to guide their children's online activities and reinforce cyber security best practices learned at school.
- **Community Outreach Programs:** civil society organization and non-profit organizations can play a vital role in raising cyber security awareness through community outreach programs. These programs can target specific demographics, such as rural communities with limited access to technology, and provide training in local languages.

**The Benefits of Early Education:**

By integrating cyber security education into the national curriculum at all levels, Nigeria can reap several benefits:

- **Empowered Citizens:** A populace equipped with cyber security knowledge can make informed decisions online, reducing their vulnerability to cyberattacks.
- **Reduced Cybercrime:** A decrease in cybercrime incidents translates to less financial loss and a safer digital environment for all Nigerians.
- **Future-Proofing the Workforce:** By fostering a culture of cyber security awareness from a young age, Nigeria can create a future workforce equipped to handle the ever-evolving cyber threat landscape.

**Challenges and Considerations:**

- **Teacher Training:** Ensuring educators have the necessary skills and knowledge to deliver effective cyber security lessons is crucial.
- **Resource Constraints:** Limited resources can hinder the implementation of comprehensive cyber security education programs. Public-private partnerships and international collaborations can address this challenge.
- **Digital Divide:** Not all schools have equal access to technology. Bridging the digital divide is essential for inclusive cyber security education.

## 2. BUILDING A CYBERSECURITY SHIELD: COLLABORATION IMPORTANT PARAMETER

Nigeria faces a complex cyber security landscape. No single entity can effectively address these challenges. Collaboration between government agencies, educational institutions, private companies, and civil society organizations (CSOs) is key to building a comprehensive cyber security strategy.

**Fostering Synergy:**

- **National Cyber security Council:** Establish a central National Cyber security Council composed of representatives from all stakeholder groups. This council can set national priorities, coordinate efforts, and ensure all voices are heard.
- **Information Sharing Platform:** Create a secure information sharing platform where stakeholders can share threat intelligence, best practices, and incident response protocols. This fosters faster detection and coordinated responses to cyber threats.

**Government and Education Partnership:**

- **Cybersecurity Curriculum Integration:** Collaborate with educational institutions to integrate cyber security education into the national curriculum at all levels. Equip students with the knowledge and skills to navigate the digital world safely.
- **Cybersecurity Scholarships and Training:** Offer government-sponsored scholarships and training programs for cyber security professionals. This can address the current skills shortage and build a robust cyber security workforce.

**Public-Private Partnerships:**

- **Joint Awareness Campaigns:** Develop joint public awareness campaigns with private companies to educate citizens of all ages about cyber security best practices. This can leverage the reach of private companies' communication channels to amplify the message.
- **Research and Development Collaborations:** Encourage collaboration between government agencies, universities, and private companies on cyber security research and development. This can lead to the creation of innovative solutions tailored to address local cyber security challenges.

**The Role of Civil Society:**

- **Grassroots Mobilization:** Civil society organizations can play a crucial role in mobilizing communities and raising awareness about cyber security in rural areas. This can bridge the digital divide and ensure everyone benefits from a secure digital environment.
- **Advocacy and Oversight:** Civil society organizations can advocate for stronger cyber security regulations and hold government and private companies accountable for data protection. This promotes transparency and builds trust in the digital ecosystem.

**Challenges and Opportunities:**

**Building Trust:** Building trust between different stakeholder groups can be challenging. Fostering open communication and mutual respect is crucial for successful collaboration.

- **Resource Constraints:** Some stakeholders may have limited resources to participate in collaborative initiatives. Explore funding opportunities from international partners and encourage knowledge sharing to bridge this gap.

**Benefits of Collaboration:**

- **Unified Approach:** Collaboration fosters a unified approach to cyber security, ensuring all stakeholders are working towards a common goal – a safer digital environment for all Nigerians.
- **Leveraging Expertise:** Collaboration allows each stakeholder to contribute their unique strengths and expertise, leading to a more comprehensive and effective cyber security strategy.
- **Sustainability:** A collaborative strategy has a higher chance of long-term sustainability. By working together, stakeholders can ensure the continuous improvement of Nigeria's cyber security posture.

By fostering collaboration between all sectors, Nigeria can build a robust cyber security shield, protecting its citizens, businesses, and critical infrastructure from evolving cyber threats.

### 3. Fostering a Culture of Security in Nigerian Organizations

Nigeria faces a unique challenge in cyber security awareness. While technical solutions are crucial, building a culture of security within organizations is equally important. This means creating an environment where Nigerian employees feel empowered to make security-conscious decisions, report suspicious activity, and learn from mistakes.

**Leveraging Nigeria's Strengths:**

- **Community Focus:** Nigeria has a strong sense of community. Use this to build a collaborative security culture where employees feel a shared responsibility for protecting the organization.
- **Open Communication:** Nigerians are known for their direct communication style. Encourage open communication about security concerns and incidents, fostering trust and transparency.

**Strategies for Nigerian Organizations:**

- **Security Champions as Mentors:** Appoint respected and tech-savvy employees as Security Champions. These champions can provide culturally relevant guidance and answer questions in a familiar way.
- **Leverage Informal Communication Channels:** Many Nigerians rely on informal communication channels like WhatsApp groups. Consider using these platforms for security reminders and quick polls to gauge employee understanding.
- **Gamification with a Nigerian Twist:** Develop gamified security awareness programs that incorporate local references, humor, or even traditional proverbs to make learning engaging and memorable.

**Addressing Challenges:**

- **Fear of Retribution:** Some Nigerian employees may fear being blamed for security incidents. Address this by emphasizing a focus on learning and improvement, not punishment.
- **Limited Resources:** Many Nigerian organizations have limited resources. Look for cost-effective solutions, such as online training modules or peer-to-peer learning initiatives.

By implementing these strategies, Nigerian organizations can foster a culture of security that is both effective and culturally relevant. This will empower employees to become active participants in cyber security, ultimately leading to a more secure digital environment for businesses and individuals across Nigeria.

## 4. STRENGTHENING CYBERSECURITY REGULATIONS IN NIGERIA

Nigeria has made strides in addressing cyber security challenges, but gaps remain. Here's how strengthening regulations can create a safer digital environment:

**A National Cyber security Framework:**

- **Develop a comprehensive framework:** Nigeria needs a robust national cyber security framework that outlines clear standards and best practices for all stakeholders, including government agencies, businesses of all sizes, and critical infrastructure providers.
- **Sector-Specific Regulations:** In addition to the national framework, consider developing sector-specific regulations for critical industries like finance, telecommunications, and healthcare. These regulations should address the unique risks faced by each sector.

**Focus on Data Protection:**

- **Data Protection Law Enforcement:** Nigeria's Data Protection Regulation (NDPR) is a positive step. However, enforcement mechanisms need to be strengthened to ensure businesses comply with data security requirements. This can involve establishing a dedicated data protection authority and imposing fines for non-compliance.
- **Consumer Awareness:** Public awareness campaigns are crucial to educate Nigerians about their data privacy rights and how to protect their personal information online.

**3. Collaboration between Regulators:**

- **Cyber security Coordination:** Establish a central coordinating body to oversee cyber security efforts across different government agencies. This body can facilitate collaboration, information sharing, and a unified approach to cyber threats.
- **Public-Private Partnerships:** Foster public-private partnerships between government regulators and the private sector. This collaboration allows for knowledge sharing, joint capacity building initiatives, and the development of effective cyber security solutions.

**Challenges and Opportunities:**

- **Limited Resources:** The present government might face resource constraints in implementing and enforcing robust cyber security regulations, therefore it is advisable to explore international partnerships and capacity-building programs to address this gap.
- **Adapting to Evolving Threats:** Cyber threats are constantly evolving. Regulations need to be flexible and adaptable to address new and emerging risks.

**Benefits of Strong Regulations:**

- **Improved Security Posture:** Robust regulations set clear expectations and hold organizations accountable for cyber security. This strengthens the overall security posture of the Nigerian digital ecosystem.
- **Increased Investor Confidence:** Stronger cyber security regulations can demonstrate Nigeria's commitment to protecting sensitive data and critical infrastructure, potentially attracting foreign investment.
- **Empowering Consumers:** Data protection regulations empower Nigerian citizens by giving them control over their personal information.

By strengthening cyber security regulations and fostering collaboration between stakeholders, Nigeria can create a safer digital environment for businesses, individuals, and the nation as a whole.

## 5. Building a Culture of Security: Empowering Employees through Security Champions

A strong cyber security posture goes beyond technical solutions. Creating a culture of security within organizations is crucial, and Security Champions play a vital role in fostering this culture.

**The Power of Peers:**

- **Accessibility and Trust:** Employees often feel more comfortable approaching colleagues with questions or concerns than IT security teams. Security Champions act as trusted peers who can provide readily available guidance and support.
- **Promoting Best Practices:** Security Champions can lead by example, demonstrating best practices like strong password hygiene and secure browsing habits. This peer-to-peer influence can have a significant positive impact on overall organizational security posture.
- **Building Awareness:** Security Champions can organize awareness campaigns, distribute security tips, and conduct internal training sessions within their teams. This continuous reinforcement of cyber security practices keeps security top-of-mind for all employees.

**The Role of Security Champions:**

- **Answering Questions:** Security Champions can act as a first point of contact for colleagues with cyber security-related questions. This reduces the burden on IT security teams and allows for more immediate resolution of basic concerns.
- **Identifying Vulnerabilities:** By being embedded within teams, Security Champions can observe and identify potential security vulnerabilities in daily workflows. They can then report these vulnerabilities to the IT security team for mitigation.
- **Building a Sense of Shared Responsibility:** Security Champions play a crucial role in fostering a sense of shared responsibility for cyber security within organizations. By actively promoting secure practices and encouraging open communication, they create an environment where everyone feels accountable for protecting the organization's digital assets.

**Developing Your Champion Team:**

- **Selection Criteria:** Identify employees who demonstrate strong cyber security awareness, possess good communication skills, and are respected by their peers.
- **Training and Development:** Provide Security Champions with comprehensive training on relevant cyber security topics, communication skills, and best practices for championing a culture of security within their teams. Organizations like the **Cyber Security Experts Association of Nigeria (CSEAN)** can play a valuable role in training and empowering potential Security Champions by offering specialized workshops and certification programs.

**Benefits of a Security Champion Program:**

- **Increased Employee Engagement:** Employees feel empowered and valued when they actively contribute to organizational security. This fosters a more engaged and security-conscious workforce.
- **Improved Incident Detection and Response:** Security Champions can help identify suspicious activity and encourage colleagues to report potential security incidents promptly. This allows for faster detection and response to cyber threats.
- **Enhanced Overall Security Posture:** By creating a culture of open communication and shared responsibility for cyber security, organizations can significantly improve their overall security posture.

Building a successful Security Champion program requires ongoing support and investment. By empowering employees through Security Champions, organizations in Nigeria can create a more secure digital environment for everyone.

## 6. Prioritizing Mobile Security in Africa: The Nigerian Case

Developing countries in Africa are witnessing a mobile revolution, with smartphone adoption on the increased. However, this increased reliance on mobile devices presents unique cyber security challenges. Here's how Nigeria can address these challenges by dedicating resources to mobile security:

**Understanding the Threats:**

- **Phishing on Mobile:** Nigerians are susceptible to phishing scams delivered via SMS or messaging apps. A very strong awareness campaign highlighting red flags of mobile phishing attempts should be carried out in all the nooks and crannies of the country.

- **Unsecured Public Wi-Fi:** Public Wi-Fi networks are popular in Nigeria, but often lack proper security. Users should be educated on the risks of using public Wi-Fi and promote the use of VPNs for added protection.
- **Malicious Apps:** Third-party app stores can harbor malware-infected applications. Encourage downloading apps only from official stores and educate users on reviewing app permissions before installation.
- **SIM Swapping Scams:** SIM swapping, where fraudsters take over a victim's phone number, is a growing threat in Nigeria. Advocate for stronger SIM registration processes and two-factor authentication for mobile financial transactions.

**Resource Allocation Strategies:**

- **Mobile-Specific Training Programs:** Design training programs specifically focused on mobile security best practices. These programs can be delivered through mobile learning apps, SMS alerts, or community workshops.
- **Public-Private Partnerships:** Partner with mobile network operators to develop and implement mobile security solutions. Mobile network operators can offer SMS-based security tips, promote secure mobile banking practices, and collaborate on public awareness campaigns.
- **Capacity Building for Law Enforcement:** Train all law enforcement agencies to investigate mobile cybercrime effectively. This includes training on forensics for mobile devices and international cooperation to track down cybercriminals operating across borders.
- **Incentivize Secure Mobile Development:** Offer grants or tax breaks to encourage developers to create secure mobile applications. This can promote the adoption of secure coding practices and secure payment gateways.

**Leveraging Nigeria's Strengths:**

- **Mobile Penetration:** Nigeria's high mobile penetration rate allows for widespread dissemination of security awareness messages through SMS campaigns or mobile apps.
- **Tech-Savvy Youth:** Nigeria's young population is tech-savvy and can be mobilized as advocates for mobile security. Partner with youth organizations to develop innovative mobile security awareness campaigns.

**Challenges and Opportunities:**

- **Digital Literacy Gap:** Not all Nigerians possess the necessary digital literacy skills to stay safe online. Address this by creating training programs in local languages and focusing on user-friendly security solutions.
- **Limited Resources:** Resource constraints may hinder the implementation of comprehensive mobile security initiatives. Explore public-private partnerships and international aid to bridge the funding gap.

By dedicating resources to mobile security and leveraging its unique strengths, Nigeria can create a safer mobile environment for its citizens. This will not only protect individuals but also foster a thriving mobile economy where trust and security are paramount.

## 7. Staying Ahead of the Curve: Continuous Improvement in Cybersecurity Awareness

The digital threat landscape is constantly evolving. Cybercriminals develop new tactics, and technology advancements introduce new vulnerabilities every day. Nigeria's cyber security awareness programs must adapt to remain effective. Here's how to ensure continuous improvement:

**Staying Informed:**

- **Threat Intelligence Gathering:** Establish mechanisms for gathering and analyzing threat intelligence. This could involve collaborating with international cyber security organizations or subscribing to threat feeds.
- **Regular Vulnerability Assessments:** Conduct regular vulnerability assessments for critical infrastructure and government systems. This proactive approach helps identify and address weaknesses before they can be exploited.

**Program Evaluation and Updates:**

- **Track Training Effectiveness:** Evaluate the effectiveness of cyber security awareness training programs through surveys, knowledge assessments, and phishing simulations. This helps identify areas where improvement is needed.
- **Update Content Regularly:** Refresh training content to reflect the latest threats and best practices. Include real-world examples relevant to the Nigerian context to keep learners engaged.
- **Adapt Delivery Methods:** Explore new and innovative ways to deliver cyber security awareness training. This could involve using gamified learning platforms, interactive simulations, or micro-learning modules delivered through mobile apps.

**Building a Culture of Learning:**

- **Promote Continuous Learning:** Encourage a culture of continuous learning within organizations. This could involve establishing cyber security newsletters, lunch-and-learn sessions, or internal knowledge-sharing platforms.
- **Employee Feedback Mechanisms:** Create feedback mechanisms for employees to provide input on cyber security awareness programs. This allows you to tailor programs to address employees' specific needs and concerns.

**Leveraging Technology:**

- **Automated Phishing Simulations:** Utilize automated phishing simulations to test employees' ability to identify and avoid phishing attempts. This helps employees stay sharp and adapt to evolving phishing tactics.
- **Security Awareness Platforms:** Consider implementing security awareness platforms that provide employees with on-demand access to training materials, security updates, and best practices.

**Benefits of Continuous Improvement:**

- **Enhanced Protection:** By staying informed and updating programs, Nigeria can ensure its citizens and organizations are equipped to address the latest cyber threats.
- **Increased Engagement:** Fresh and relevant content keeps employees engaged with cyber security awareness, leading to more effective behavior changes.
- **Adaptability:** A culture of continuous improvement allows Nigeria's cyber security awareness programs to adapt to the ever-changing digital landscape.

By prioritizing continuous improvement, Nigeria can create a culture of cyber security awareness that empowers its citizens and organizations to stay ahead of the curve and navigate the digital world with confidence.

## 6 CONCLUSION

Nigeria's journey towards a robust cyber security ecosystem necessitates a multifaceted approach. This research paper has explored key strategies for raising cyber security awareness, fostering a culture of security within organizations, and building a collaborative national effort. By acknowledging valuable lessons learned and addressing existing challenges, Nigeria can create a safer digital environment for its citizens and businesses.

**Key Takeaways:**

- **Early and continuous cyber security education** is fundamental, equipping young Nigerians with the foundation for safe online practices.
- **Targeted awareness campaigns** addressing the knowledge gap and utilizing diverse communication channels are essential.
- **Collaboration between government, educational institutions, private companies, and CSOs** is crucial for a unified national approach.
- **Building a culture of security within organizations** through Security Champions and open communication empowers employees and strengthens overall security posture.
- **Continuous improvement and adaptation** to evolving threats and technologies are necessary for sustained effectiveness.

**Moving Forward:**

- **Increase Investment:** Nigeria needs to prioritize investment in cyber security initiatives. Public-private partnerships and international aid can bridge the resource gap.
- **Capacity Building:** Continuous training and capacity building programs for IT professionals, educators, and Security Champions are essential.
- **Leverage Technology:** Utilizing innovative technologies like gamified learning platforms and mobile applications can enhance awareness programs and reach wider audiences.
- **Data-Driven Approach:** Collecting and analyzing data on cyber threats can help tailor awareness campaigns and resource allocation for maximum impact.
- **International Collaboration:** Nigeria can benefit from knowledge sharing and collaboration with international organizations and developed nations with established cyber security frameworks.

Building a secure digital future for Nigeria requires a collective effort. By implementing the strategies outlined in this research paper, fostering collaboration across sectors, and prioritizing continuous learning, the citizens can be empower, safeguard its critical infrastructure, and thrive in the ever-evolving digital landscape.

**Looking Ahead:**

This work provides a foundation for understanding the importance of cyber security awareness in Nigeria. Further work can be carried out on areas like:

- Developing a national cyber security strategy framework.
- The economic impact of cybercrime in developing countries in Africa.
- The role of artificial intelligence and machine learning in enhancing cyber security defense in Africa.

By building upon these efforts, Nigeria can navigate the complex digital landscape with greater confidence and create a future where digital opportunities flourish alongside robust cyber security.

## REFERENCES

[1] Okeshola F.B. and Adeta A.K, (2013) The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria American International Journal of Contemporary Research, vol. 3(9), 98-114.

[2] Ewepu G, (2016) Nigeria loses N127bn annually to cyber-crime — NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses- n127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

[3] Maitanmi, O. Ogunlere, S. andAyinde S. (2013), Impact of Cyber Crimes on Nigerian Economy, The International Journal of Engineering and Science (IJES, vol. vol 2(4), 45–51.

[4] "Cybercrime Top 10 Countries Where Attacks Originate", (2015b), online:<https://www.bba.org.uk/wp-

[5] Kaspersky Lab (2020). What is Cybersecurity? Kaspersky Resource Centre. Internet: https://www.kaspersky.com/resource-center/definitions/what-is-cyber- security.( Sourced 07/01/2024).

[6] J. C. Oforji, E. J. Udensi, and K. C. Ibegbu (2017). Cybersecurity Challenges in Nigeria: The Way Forward. SosPoly Journal of Science and Agriculture, Vol. 2, 1-5

[7] F. Uwadia and F. I. Eti (2018). Cyber Security in Nigeria: Issues, Challenges and Way Forward. International Research Journal of Advanced Engineering and Science, Volume 3, Issue 2, pp. 351-354.

[8] Oni Damilola, Arshad Emmanuel & Pham Bich Ngoc (2023): Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria.

[9] O. Osho, and A. D. Onoja (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology, Vol. 9, No. 1, 120–143.

[10] Nigerian Bureau of Statistics (NBS) (2020). Telecoms Data Q1 2020. https://nigerianstat.gov.ng/resource/Q1%202020%20Telecoms%20data.xlsx. (Sourced 07/01/2024)

[11] Daniel Eluwah (2021), Cyber Awareness and Education in Nigeria: An Assessment, National Identity Management Commission, Nigeria

[12] Dambo, O. A. Ezimora and M. Nwanyanwu (2017). Cyber Space Technology: Cyber Crime, Cyber Security and Models of Cyber Solution, A Case Study of Nigeria. International Journal of Computer Science and Mobile Computing, Vol. 6, No. 11, 94-113

[13] S. Ibrahim (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice, 47, 44-57.

[14] Ahmad, A. Suleiman. "CYBER CRIME AND THE SOCIOLOGICAL IMPLICATION IN THE NIGERIA'S TERTIARY EDUCATION SYSTEM." *FUDMA JOURNAL OF SCIENCES* 3, no. 1 (2019): 249–57.

[15] "Cyber Security – NITDA." Accessed September 2, 2024. https://nitda.gov.ng/department/cyber-security/.

[16] "Cybersecurity and Cybercrime Combatting Culture for African Police Services | SpringerLink." Accessed September 2, 2024. https://link.springer.com/chapter/10.1007/978-3-030-62803-1_20.

[17] "Econet Founder Reveals Story behind Company's Downfall in Nigeria." Accessed April 26, 2024. https://techpoint.africa/2015/10/06/econet-founder-reveals-story- behind-companys-downfall-in-nigeria/.

[18] "Economic and Financial Crimes Commission - EFCC - EFCC Reaffirms Commitment to Fight against Cyber Crimes." Accessed September 2, 2024. https://www.efcc.gov.ng/efcc/news-and-information/news-release/10020-efcc- reaffirms-commitment-to-fight-against-cyber-crimes.

[19] Galle, Salihu Abdullahi. "A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development," n.d.

[20] Georgiadou, Elissavet. "McLuhan's Global Village and the Internet," 2002. International School Vietnam National University - Hanoi, Vietnam,

[21] Damilola Oni, Emmanuel Arshad, and Bich Ngoc Pham. "Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention." *Advances in Multidisciplinary and Scientific Research Journal Publication* 2, no. 1 (July 30, 2023): 143–50. https://doi.org/10.22624/AIMS/CSEAN-SMART2023P17.

[22] Jaiyeola, Temitayo. "$461m Investment Gap Slows Nigeria's Internet Coverage." Businessday NG, April 15, 2024. https://businessday.ng/technology/article/461m- investment-gap-slows-nigerias-internet-coverage/.

[23] NextGen Innovative Digital Solutions. "Detailed History of Internet in Nigeria - History of Nigeria," December 30, 2022. https://innovative.ng/detailed-history-of- internet-in-nigeria/.

[24] "ngCERT | Security Quality Management." Accessed September 2, 2024. https://cert.gov.ng/security-services.

[25] "Scams and Fraudulent Investment Schemes That Misuse Our Name." Accessed April 26, 2024. https://www.worldbank.org/en/about/legal/scams.

[26] "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals - ScienceDirect." Accessed April 26, 2024. https://www.sciencedirect.com/science/article/pii/S1756061616300787.

[27] "Study on International Internet Connectivity in Sub-Saharan Africa," n.d. Tade, Oludayo. "Electronic Banking Fraud in Nigeria: How It's Done, and What Can Be Done to Stop It." The Conversation, June 23, 2020. http://theconversation.com/electronic-banking-fraud-in-nigeria-how-its-done-and- what-can-be-done-to-stop-it-141141.

[28] Tredger, Christopher. "Mobile-First Status a Chink in Africa's Security Armour?" ITWeb Africa, June 3, 2016. https://itweb.africa/content/8OKdWMDYXgaqbznQ.

[29] Ubabudu, Mary Chinelo. "The Effectiveness of Global System Mobile Providers' Services on Communication in Nigeria." *International Journal of Business and Public Administration* 10, no. 2 (September 22, 2013): 58–80.