**CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURE IN NIGERIA**

**Introduction**

In the realm of financial markets infrastructure, safeguarding against potential disruptions and ensuring the stability and integrity of the financial system are paramount. The utmost importance lies in the cyber resilience of financial market infrastructure in Nigeria or any country, aiming to protect against potential cyber threats and guarantee the stability and security of the financial system. As the financial sector increasingly relies on technology and digital platforms, it has become crucial to implement effective measures that safeguard against cyber attacks and ensure the uninterrupted continuity of financial services**.**

## Importance Cyber Resilience

Financial markets represent a significant focal point for potential cyber threats, owing to the substantial value of transactions and the sensitive nature of the involved data. Cybersecurity breaches have the potential to result in financial losses and the disruption of essential services.

Preserving public trust and mitigating potential threats to the overall stability of the financial system are critical considerations. In the context of Nigeria's financial market infrastructure, the significance of cyber resilience cannot be overstated. The growing interconnectivity and technological sophistication within the financial sector elevate the risk of cyber threats and attacks. Cyber resilience, therefore, assumes paramount importance in fortifying the capacity of financial market infrastructure to withstand and recover from such

adversities. This involves implementing a spectrum of strategies and practices, encompassing risk management, incident response, and security controls, all collaboratively reinforcing the overall resilience of the financial system against cyber threats.

**Overview of Financial Markets Infrastructure in Nigeria**

Financial market infrastructures encompass diverse elements, including payment systems, securities settlement systems, and central securities depositories. Serving as the backbone of the financial system, these entities are intricately interconnected, rendering them susceptible to cyber threats that pose substantial risks to the stability of the financial sector.

The Nigerian digital financial ecosystem has experienced noteworthy expansion in recent years. Currently, the country hosts over 254 fintech organizations, exclusive of fintech solutions provided by banks and mobile network operators. The emergence of new service providers spans mobile money operators, payment service providers, fintech firms, and various other financial services entities. This trend underscores the escalating imperative to prioritize consumer security and trust.

Ensuring the cyber resilience of this intricate financial infrastructure is indispensable. This imperative is underscored by the need to uphold trust, confidence, and stability in Nigeria's financial markets, particularly in the face of the expanding and evolving landscape of digital financial services.

## Threat Landscape in Nigeria

Nigeria's digital financial landscape is characterized by a diverse array of digital financial products, services, and service providers, reflecting a dynamic and rapidly evolving sector. The ecosystem includes a comprehensive range of financial institutions, such as 32 deposit money banks, 6 merchant banks, 3 Payment Services banks, and 4 Non-interest banks. Additionally, there are more than 254 fintech firms contributing to the innovation and growth of the sector. In parallel, the financial landscape features over 916 microfinance banks, further diversifying the financial services available.

Beyond the formal financial institutions, Nigeria's digital financial space accommodates numerous other financial entities, fostering a rich and competitive environment. This diverse array of financial players caters to the multifaceted needs of the economy, ranging from traditional banking services to innovative fintech solutions.

Notably, the digital financial landscape in Nigeria extends its reach to the non-formal sector, providing essential services to the unbanked segment of the economy. This sector plays a pivotal role in financial inclusion, addressing the needs of individuals and businesses that might otherwise lack access to conventional banking services. The presence of a robust non-formal sector underscores the broader commitment to inclusivity and accessibility in Nigeria's evolving financial ecosystem.

## Regulatory Framework for  Cyber Resilience in Nigeria

Nigeria has been actively working on developing and enhancing its regulatory framework for cybersecurity and cyber resilience. General overview of the regulatory framework for cyber resilience in Nigeria:

### 1. National Cybersecurity Policy and Strategy.

Nigeria has a National Cybersecurity Policy and Strategy that provides a comprehensive framework for addressing cyber threats and enhancing cyber resilience. This policy outlines the government's approach to ensuring the security of cyberspace, protecting critical infrastructure, and fostering a secure digital environment.

### 2.  National Information Technology Development Agency (NITDA)

NITDA is a key regulatory body in Nigeria overseeing the development and regulation of information technology, including cybersecurity. NITDA plays a crucial role in formulating policies and guidelines to enhance the country's cyber resilience.

### 3. Central Bank of Nigeria (CBN)

The Central Bank of Nigeria is actively involved in regulating the financial sector's cybersecurity. It issues guidelines to financial institutions to ensure the security and resilience of their systems against cyber threats. This includes measures to protect customer data, financial transactions, and the overall stability of the financial system.

The Central Bank of Nigeria (CBN) plays a pivotal role in fortifying the cyber resilience of financial institutions, including those within the financial market infrastructure, by issuing comprehensive guidelines and directives. These directives encompass crucial areas such as risk management, information security, and incident response, thereby establishing a robust framework for cyber resilience enhancement.

Under the ambit of supervision and examination, the CBN conducts regular assessments of financial institutions to ensure strict adherence to cybersecurity regulations. This involves scrutinizing the efficacy of their cybersecurity measures, evaluating incident response plans, and assessing overall resilience against cyber threats.

Facilitating collaboration and information sharing is another cornerstone of the CBN's strategy. By fostering a collaborative environment among financial institutions, government agencies, and stakeholders, the CBN aims to strengthen collective cyber resilience. This approach entails sharing threat intelligence and best practices to effectively address emerging cyber threats.

In tandem with these efforts, the CBN engages in capacity-building initiatives targeted at enhancing the cybersecurity prowess of financial institutions. This may involve structured training programs aimed at equipping personnel with the necessary skills and knowledge.

Recognizing the escalating number and sophistication of threats targeting deposit money banks, payment service providers, and financial institutions, the CBN introduced the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. Effective from January 1, 2019, these guidelines delineate minimum requirements to bolster the cybersecurity posture of banks and payment service providers, emphasizing proactive measures to secure critical information assets and online customer information. The framework mandates the integration of cybersecurity into business functions and overarching risk management processes. Deposit money banks and payment service providers are directed to conduct regular risk assessments, vulnerability assessments, and threat analyses to detect and evaluate risks to their information assets.

In an ongoing commitment to fortify cybersecurity across the financial sector, the CBN released a draft version of the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions on August 13, 2021, seeking public input. This framework aims to prevent and combat cybercrimes within the Other Financial Institutions (OFI) subsector, promote the adoption of cybersecurity best practices, create a secure cybersecurity environment for OFI operations, and uphold public trust in the OFI subsector.

Furthermore, the Nigerian Payments System Risk and Information Security Management Framework addresses information security risks, directing payment service providers and operators to implement information security policies in line with ISO 27001 standards. The framework emphasizes ensuring the

confidentiality, integrity, and availability of critical information, systems, and networks vital for operational success.

**4.Data Protection Regulation:**

Nigeria has introduced data protection regulations, such as the Nigeria Data Protection Regulation (NDPR), which focuses on ensuring the privacy and security of personal data. Effective data protection is a crucial component of any cyber resilience framework.

**5. Collaboration with International Organizations:**

Nigeria collaborates with international organizations and adopts best practices from global cybersecurity frameworks. This collaboration helps align its cybersecurity efforts with international standards and strengthens the country's ability to respond to evolving cyber threats.

**6. Cybersecurity Incident Response Team (CIRT):**

Nigeria has established a national Computer Security Incident Response Team (CSIRT) to facilitate the detection, response, and mitigation of cybersecurity incidents. This team plays a vital role in coordinating responses to cyber threats across different sectors.

**7. Legislation and Cybercrime Laws:**

Nigeria has enacted laws to address cybercrime, such as the Cybercrime (Prohibition, Prevention, etc.) Act. These laws provide a legal framework for prosecuting cybercriminals and serve as a deterrent to potential offenders.

**8. Capacity Building and Awareness Programs:**

The government, in collaboration with various agencies, conducts capacity building and awareness programs to educate individuals and organizations about cybersecurity best practices. This includes training initiatives to enhance the skills of cybersecurity professionals.

.

## Conclusion

In conclusion, the imperative of cyber resilience for financial market infrastructure in Nigeria cannot be overstated. As the digital landscape expands and evolves, safeguarding against potential disruptions and ensuring the stability of the financial system remains paramount. The interconnected nature of financial market infrastructures amplifies the risks posed by cyber threats, necessitating a robust cyber resilience framework.

The significance of cyber resilience is underscored by the pivotal role of financial markets in the economy. Not only do they handle high-value transactions, but they also manage sensitive data critical to public trust and confidence. The potential consequences of cyberattacks, including financial losses and service disruptions, emphasize the urgency of proactive measures.

Nigeria's financial sector, comprising a diverse ecosystem of formal and non-formal entities, faces an evolving threat landscape. With over 254 fintech organizations, deposit money banks, payment service providers, and other financial institutions, the need for a comprehensive regulatory framework is evident. The government, through entities like the National Cybersecurity Policy and Strategy and the Central Bank of Nigeria (CBN), has been actively shaping and implementing measures to enhance cyber resilience.

The CBN, in particular, has played a pivotal role in formulating guidelines, conducting supervisory assessments, and fostering collaboration among financial institutions. The Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, introduced in response to the escalating threats, exemplify a forward-looking approach. The ongoing efforts to extend this framework to other financial institutions and the emphasis on international collaboration highlight a commitment to staying ahead of emerging challenges.

Legislation, such as the Cybercrime (Prohibition, Prevention, etc.) Act, reinforces the regulatory landscape, providing a legal basis for prosecuting cybercriminals. Collaborative initiatives, capacity-building programs, and the establishment of a Cybersecurity Incident Response Team (CSIRT) further contribute to Nigeria's multifaceted approach in addressing cyber threats.

As Nigeria continues to align with global cybersecurity standards and adapt to emerging threats, the regulatory framework is positioned to evolve. Data protection regulations, collaboration with international organizations, and a focus on capacity building underscore a comprehensive strategy. By integrating cybersecurity into business functions, conducting regular risk assessments, and fostering a culture of awareness, Nigeria is actively working towards a resilient and secure financial ecosystem.

In essence, the pursuit of cyber resilience is an ongoing commitment, crucial for maintaining trust, confidence, and stability in Nigeria's financial markets amidst the transformative landscape of digital financial services.