ÆLEX

THE EVOLUTION OF CYBER SECURITY IN THE NIGERIAN BANKING SECTOR

Nigeria moved from a country with zero legislation on cyber security to a country with an extensive law with the enactment of the Cybercrime (Prohibition, Prevention, Etc.) Act ("the Act") in 2015.

The Act prescribes punishment for specific actions such as cybersquatting, cyberstalking, identity theft, unlawful access to a computer (popularly called hacking), cyber terrorism, racism and xenophobic crimes.[1] The Act also establishes the Cybercrime Advisory Council which is constituted by representatives of almost all the law enforcement agencies in Nigeria.[2]

The Cybercrime Advisory Council is responsible for policy formulation,while the Office of the National Security Adviser (ONSA) is responsible for the enforcement of the Act.[3]

The promulgation of the Act was lauded by the public as it codified illegal activities conducted in the cyberspace. However, it has not been able to assist organisations with required information on how to structure their businesses to prevent cybercrime. Consequently, it is being argued in some quarters that the Act has failed to provide a standard by which organisations would prevent and mitigate cybercrime.

For instance, in 2018, in spite of the existence of the Act, it was reported that 60% of Nigerian businesses experienced cyber-attacks[4] and that Nigeria loses N127,000,000,000 (one hundred and twenty- seven billion Naira) annually through cybercrime. [5]

Introduction of the Risk-Based Cybersecurity Framework and Guidelines
In furtherance of the cashless policy mandate of the federal government, the banking sector began employing the use of information technology to expedite the flow of funds.

This includes the use of Automated Teller Machines (ATM), mobile banking applications and Unstructured Supplementary Service Data (USSD) platforms. In the light of the perceived gaps in the cybersecurity legislation in Nigeria and pursuant to the powers of the Central Bank of Nigeria ("CBN") to regulate banking activities in Nigeria,[6] it became imperative for the CBN to issue a guideline to regulate the use of information technology in the banking sector.

Further to this, the CBN issued the Risk-Based Cybersecurity Framework and Guidelines ("the guidelines") which became effective on 1st January 2019.

[1] Part III of the Cybercrimes (Prohibition, Prevention, etc) Act, 2015.
[2] For example, the Nigerian Police Force, the Economic and Financial Crimes Commission, Independent Corrupt Practices Commission, Nigerian Security Civil Defence Corps.
[3] Section 42 of the Cybercrimes (Prohibition, Prevention, etc) Act, 2015.
[4] Osagwu P. (2019, March 8), Cyber Attack: 60% of Nigerian Businesses attached in 2018, Vanguard, retrieved from https://www.vanguardngr.com/2019/03/cyber-attack-60-of-nigerian-businesses-attacked-in-2018/
[5] Iroegbu S. (2016, April 19), Nigeria Loses over N127bn annually through cybercrime, ThisDay, retrieved from https://www.thisdaylive.com/index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime/
[6] Section 1 of the guidelines.

The guidelines apply to all Deposit Money Banks (DMBs) and Payment Service Providers (PSPs).

PSPs include platforms such as GTpay, eTranzact, Simple Pay, quickteller, jumia pay and other third-party service providers who use their infrastructure to store, process or transmit DMBs' customer information.

The guidelines prescribe the following standards to be upheld by DMBs and PSPs[7]:

1. Board Oversight and Responsibility: Ensure that the Board of Directors of the companies have oversight and overall responsibility for the cybersecurity programme and governance documents (e.g. the strategy, framework and policies)

2. Cybersecurity budget: Allocate a cybersecurity budget.

3. Chief Information Security Officer: The mandated position must be occupied by qualified personnel.[8]

4. Information security steering committee: set up this steering committee which will be responsible for the governance of the cybersecurity programme.

5. Independent Internal Audit: Ensure that the audit team reviews the cybersecurity programme.

6. Risk Management System: Employ a risk management system to reduce the incidence of significant adverse impact on an organisation.

7. Cybersecurity Resilience Assessment: Evaluate the organisation's defence posture and readiness to cybersecurity risks.

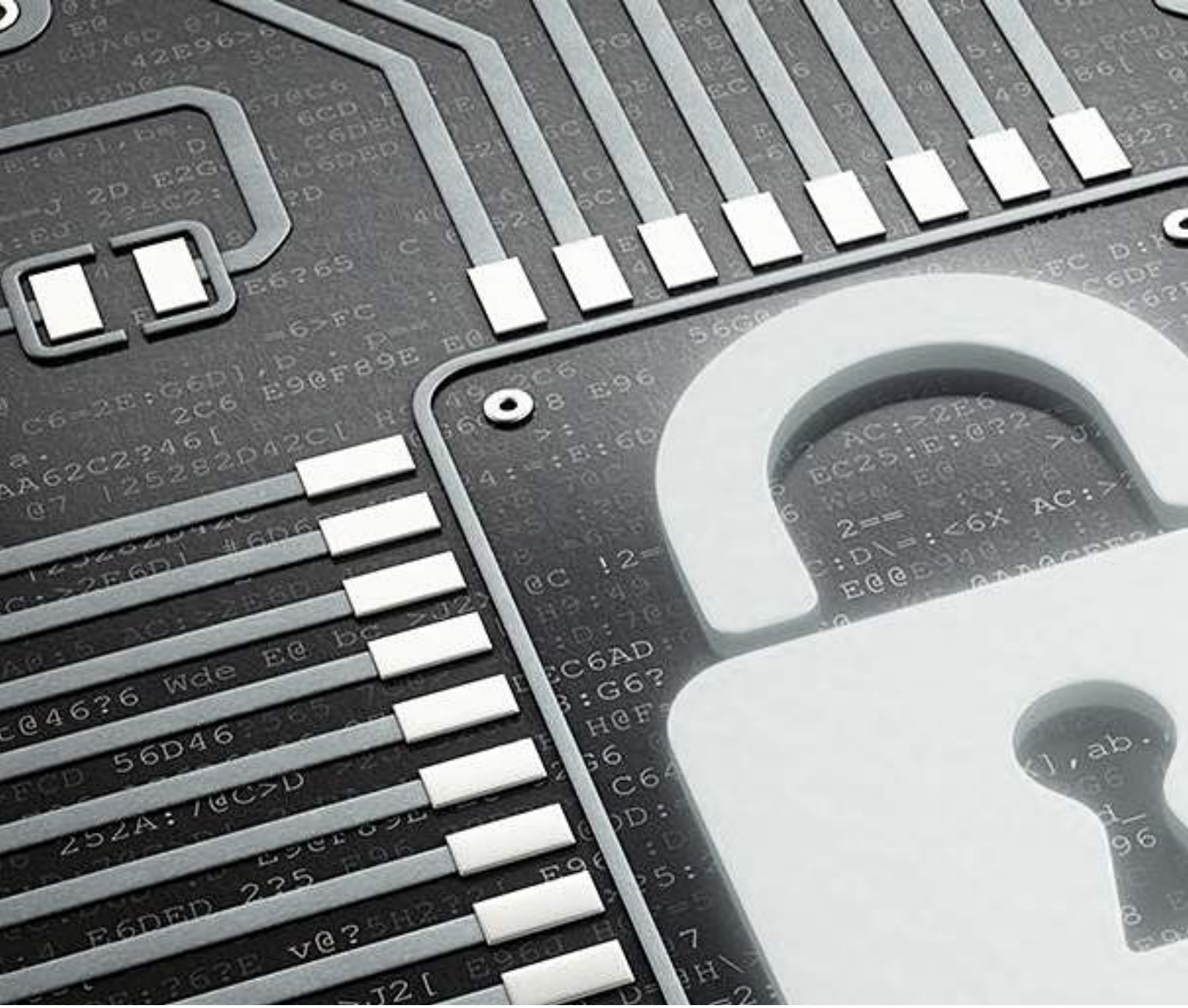
8. Cybersecurity Self-Assessment: Submit to the CBN, an annual report of the procedure/tools/framework used to conduct the self-assessment..

9. Cybersecurity Operational Resilience: Strengthen cyber defence by 'know your environment' (which means to devise mechanisms to maintain an up to date inventory of authorised software); and by having a cyber threat intelligence.

10. Metrics, Monitoring and Reporting: Ensure compliance by putting in place metrics, monitoring and reporting.

11. Cyber Incidence Report: In the event that a DMB/PSP experiences a cyber-incident,[9] it must report the breach within 24 hours of the incidence to CBN. Failure of which, the CBN would take appropriate sanctions.

[7] Sections 2-5 of the guidelines.
[8] He must have relevant experience with any of the following certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Chief Information Security Officer (CISO).
[9] an incident that results in a loss that exceeds 0.01% of shareholders' funds unimpaired by losses.



CYBER SECURITY IN THE NIGERIAN BANKING SECTOR

Cybersecurity in the United Kingdom and the United States of America

In the United Kingdom, the National Information Security Regulation which was adopted from the European Union Directive (EU) 2016/1148, is the overarching cyber security law. It requires various ministries of the relevant sectors to publish a national strategy on network and information systems.[10]

It therefore permits the relevant sectors to determine their cyber policy. In addition, operators of essential services[11] are mandated to take appropriate and proportionate technical and organisation measures to manage risks posed to the security of the network and information systems and prevent and minimise the incidents affecting security of networks.[12]

The United States in its effort to fight cyber threat, mandates its private entities to share their cyber threat indicators or defensive measures with certain government entities.[13] The objective is for knowledge sharing in the fight against cybercrime.

CONCLUSION

In prescribing the guidelines, the CBN appears to have recognised the evolving nature of cybercrime and the ingenuity in every attack.

In prescribing the guidelines, the CBN appears to have recognised the evolving nature of cybercrime and the ingenuity in every attack.

The CBN has therefore tried to curb cybercrime by prescribing measures that should be carried out by the DMBs and the PSPs to prevent and mitigate the use of cybercrime techniques, such as viruses, worms, Trojan horses, ransomware, rootkit, keyloggers and grayware on their information technology platforms.

This approach by CBN gives the DMBs and the PSPs, the liberty to prescribe their cybersecurity governance and resolve cyber threats, while remaining accountable to CBN. It enables the DMBs and PSPs to utilise current and effective measures in managing cyber threats.

This approach is in tangent with the approach taken by the European Union and the United States. CBN as the primary regulator in the Banking sector has by the provisions of the guidelines, provided a framework to ensure cyber safety. It has been reported that Africa's mobile economy will generate more than 7.9% of its GDP and that about 300 million people are expected to make up the mobile economy by 2025.[14]

It therefore means that it is imperative that adequate regulation of the cyber space be carried out for other sectors of the economy as has been done in the Nigerian banking sector.

[10] Section 2 of the National Information Security Regulations, 2018.
[11] Schedule 2 of the National Information Security Regulations, 2018- Essential Services includes the electricity, oil, gas, air, water, rail, road, health, drinking water supply and distribution and digital infrastructure subsectors.
[12] Section 10 of the National Information Security Regulations, 2018.
[13] Section 104 (C)(1) the Cybersecurity Information Security Act (CISA).
[1] Chike Onwuegbuchi, (2019 March, 29), Africa: CWG Boss At Africa CEO Forum, Harps On Building Viable Digital Economy, AllAfrica, retrieved from https://allafrica.com/stories/201903290075.html

ÆLEX

AUTHOR
FLORENCE BOLA-BALOGUN

fbola-balogun@aelex.com

Florence is an Associate in the firm's Corporate/Commercial, Banking and Finance, Tax and Company Secretarial practice groups.

CONTACT

DAVIDSON OTURU

Partner IP/TMT and Corporate/Commercial
doturu@aelex.com

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana.

Contact us at:

4th Floor, Marble House,
1 Kingsway Road, Falomo Ikoyi,
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

E-mail: lagos@aelex.com

Click here www.aelex.com

to follow our social media handles click below

@aelexpartners

@aelexpartners

@aelexpartners