PIN Policy Brief No. 3

PARADIGM INITIATIVE NIGERIA

CyberSecurity in Nigeria: Need For A Paradigm Shift

Introduction

Nigeria has the largest Internet population in Africa, estimated at about 56 million by Freedom House in its 2013 Freedom on the Net report. 57.9% of the Internet traffic being via mobile phones and the latter is largely accountable for the surge in its penetration rate from 27% in 2011 to 33% in 2013. This buttresses the increasingly important role of the Internet across societal sectors. This represents both an opportunity and a drawback - for example the African continent accounts for only 2% of global GDP, yet it accounts for 10 per cent of global cybercrime incidents.

In 2013, the Paradigm Initiative Nigeria (PIN) publication on "Economic Cost of Cybercrime in Nigeria" provided quantitative data for measuring the extent of cybercrime in Nigeria and proposed recommendations for combating its influence in the country. This is one of the first major studies dedicated entirely toward quantitatively measuring the costs of cybercrime in Nigeria.

With the high cost of cybercrime, and accompanying security risks, there is an ever-increasing need to create awareness about cyber security - a responsibility of all concerned. It is in view of this that the Nigerian government in partnership with civil society and private sector organizations launched a series of initiatives to combat cybercrime in Nigeria.

Regulatory Framework for Cyber Security in Nigeria

Cybercrime involves using computers and Internet by individuals to commit crime. Cyber terrorism, identity theft and spam are identified as types of cybercrimes.

Cyber Security is a fast-growing field of Information and Communication Technology concerned with reducing organizations' risk of hack or data breach.

Under Nigeria's current democratic dispensation, the function of lawmaking lies with the National Assembly. Although, there are no current laws that specifically target cyber security, government agencies such as the Economic and Financial Crimes Commission have been given the directives to prevent financial crimes within the country, including cases of online fraud.

In February 2013, the House of Representatives put forth a proposal to amend the 2004 Criminal and Penal Codes to place strict penalties on cybercrime, prescribing fines ranging from 5 to 25 million naira for offenders and jail terms of between 2 and 15 years. The Ministry of Justice resisted the proposed amendments, advising that a "comprehensive executive bill on cybercrimes" would be a better approach than amending the criminal and penal codes. Meanwhile, broader conversations on issues of cyber security have also focused on how to protect Internet freedom, especially as more citizens and civil society organizations take interest in the constitutionally guaranteed right. There has been a renewed focus by the Nigerian government on cyber security post revelations of surveillance globally in 2013. In the last year, there has been an emergence or renewal of debates on a number of bills before the National Assembly that refers to or is directly about cybercrime. These include:

1. Electronic Transaction Bill, 2011 (HB 03)
2. Cybercrime Bill, 2014 (SB 438)
3. Electronic Fraud and Electronic Transfer of Funds (Prohibition and Punishment) Bill, 2011 (SB 69)
4. Electronic Transfer of Funds Crime Bill 2011 (SB 35)
5. Nigeria Communications Act (Amendment) Bill 2013 (HB 561)

Despite an acknowledgement by law makers of the critical nature of the issues these bills are developed to address, none has so far been passed into law. This is as a result of internal politics and dynamics within and between the Senate and the House of Assembly, very long (tending towards excessive) recesses taken by members of the National Assembly, and the economic pressures brought to bear to ensure non-passage as it affects corrupt businesses.

Government Initiatives to Combat Cyber Crime

Two agencies of the Federal Ministry of Communications Technology have announced government initiatives to combat cybercrime. The National Information Technology Development Agency (NITDA) with the goal of "being a trusted intermediary organization dedicated to provide support in responding to computer network and related cyber security incidents" commissioned and funded the Computer Emergency Readiness Response Team (CERRT.ng) in April 2014. This is an anti-cybercrime forensic laboratory that seeks to assist public institutions, private bodies and individuals in responding to computer, network and related cyber security challenges or threats. The forensic laboratory, described by promoters as the first of its kind in the West African region, is expected to analyse and resolve cyber security incidents as needed, "in Nigeria, by Nigerians and for Nigerians". In December 2013, the National Information Technology Development Agency (NITDA) adopted the COBIT 5 framework, which is

expected by implementation to help "provide a holistic approach by including all the minimum requirements for a policy framework and thus lead to a better cyber security atmosphere in Nigeria".

The Nigeria Communications Commission (NCC), the regulatory body for the telecommunications sector, has also established a Media and Information Security department to explore ways to protect corporate and individual citizens from the challenges, providing awareness and information to help those vulnerable to these cybercrimes to curb the menace of cybercrimes in the country. Also, the National Identity Management Commission (NIMC) has taken security measures to protect its database from cybercrimes.

Private Companies' Efforts to Reduce Threats

In an attempt to reduce the level of threat and cyber attack, *Cyber Security, Fire Protection and Safety Suppliers* gathered in Lagos on March 18-19, 2014, at the Securex West African trade show, to discuss initiatives, challenges and emerging technologies. They also evaluated existing counter-terrorism policies and sought better understanding of new domain threats posed by regionally active militant organisations. Also, in the financial sector, Computer Warehouse Group (CWG) PLC, in partnership with MAG Tech, a specialized information security and intelligence company, recently organized an Information Security session in Lagos. The session with the theme, "Security Operations Centre (SOC) - Financial Services in the Cyber Attack Era" created an avenue for stakeholders to extensively discuss and understand the new concept, Security Operations Centre (SOC), as the ultimate major information security platform required to drastically minimize cyber attacks and threats encountered by financial institutions.

Cyber Security Bill

In November 2011, the office of the National Security Advisor and the Attorney General completed work on a Cyber Security Bill for Nigeria, having revised the earlier *Cyber Security and Information Protection Agency Bill,* which had provisions that could restrict users' rights to free expression and privacy, by allowing security officials to apprehend and prosecute users based on suspicion and without a court order. Taking into account feedback from citizens and stakeholders in the Nigerian ICT sector, the revised bill reduced the powers granted to security officers by requiring a court order for the seizure of any equipment and for arrests based on suspicion. The draft bill passed a second reading in the House of Representatives in November 2012. Meanwhile, many fear that the draft 2010 Lawful Interception of Information Bill, which was still being deliberated in the National Assembly as of May 2013, may include provisions that could allow voice and data monitoring.

Conclusion

In response to growing instances of cybercrime in Nigeria, the government has increased its measures to crackdown against criminal activity online. A 2011 Ernst & Young report found that the country's unchecked cybercrime imposes costs on the Nigerian economy to the tune of $200 million per year from cyber attacks alone.

Cyber Crime Bill, 2014, and other bills mentioned in this brief, face similar problems such as the need to pass fair versions of the bill into law by the National Assembly and the fact that though there is input from government agencies, there is no sufficient input from industry players, civil society and other stakeholders that these bills would affect directly. In some instances where industry players were consulted, their opinion was overruled by regulators who seek to impose control and therefore threaten to choke the market of real growth if the bills get passed in law, as they currently exist.

While the need for an effective cyber security environment is needed, the efforts must ensure legal compliance, technical competence, other required organizational measures, capacity building and cooperation, for it to be effective. It is only when this is done that proper growth can be achieved, and citizen rights not threatened.

Prepared by **Abikoye Oluwafemi** and **Yusuf Salihu** for **Paradigm Initiative Nigeria**. July 3, 2014

For further information, contact Paradigm Initiative Nigeria:
info@pinigeria.org | **www.pinigeria.org** | **@pinigeria**