Opportunity Spotting:

Telescoping Potentials for Cyber Insurance in Nigeria

Thought Leadership | by Gabriel Fatokunbo *(Originally published in BDLegal Business, 17th January, 2018, p.17)*

g.fatokunbo@lelawlegal.com

Introduction

Recent developments, such as: the rise of insurance aggregators, disruptive technologies (e.g internet of things (IoTs)) in business, improvement in Nigeria's ranking in *World Bank's Ease of Doing Business 2018*, recent inclusion of e-commerce services on the Pioneer List (conferring eligibility for 'pioneer status' tax holiday), increased emergence and leverage of technology driven businesses (like electronic identification, online registration and business negotiation etc.) are good indices for improved insurance penetration in Nigeria. These underscore the potentials that lie ahead for the industry's positive evolution and growth.

However, with this growing success lies the impending challenges of cybercrimes, 'yahoo plus', ponzi schemes, data breach, intellectual property thefts, etc.; contributing to enterprises' major business risks. Considering Nigeria's notoriety in cybercrimes - according to the Nigeria Communication Commission, she ranked third globally behind UK and US in 2017- is Nigeria's insurance industry prepared to manage the risks that will surely arise from cyber activities? And is it positioned to benefit from the dynamics of the present realities of cyber frauds by providing cyber insurance products? These questions and the writer's humble attempt to answer them, underpins this article.

Cybercrime Realities in Nigeria

The Minister of Technology, Adebayo Shittu, during a Cybersecurity Conference in 2017 said: *"Nigeria loses N127 Billion annually to cybercrime."* Similarly, the *Global Threat Impact Index 2017* listed Nigeria (and four other African countries) amongst the world's highest risk countries for cyberattacks. The Federal Government (FG) had its fair share of cybercrimes when in 2011, Niger Cyber Hacktivists hacked the websites of National Poverty Eradication Programme and the Niger Delta Development Commission; the website of Economic and Financial Crimes Commission's was also attacked in 2013. Knowing that several strategic public and private sector entities and projects can be targeted by cyber hacktivists, how can stakeholders (underwriters, brokerage firms, the potential targets/ insureds) rise to the occasion in a proactive and optimal manner?

Also, the CBN's *Economic Report* for H1 2013, recorded 2,478 fraud and forgery cases in Nigerian banks at over N20 billion whilst the 2014 and 2015 Report recorded 11,447 and 5,917 fraud cases valued at N25.81 billion and N11.99 billion respectively. Incidentally, a 2017 KPMG publication, '*Seizing the Cyber Insurance Opportunity: Rethinking the Insurers' Structures and Strategies in the Digital Age*' asserted that 60% of Fortune 500 companies lacks protection due to lack of insurance cover for many types of cyber risks. Leading insurance companies in Nigeria, do not appear to offer any or significant cyber-insurance products. Information on their websites seems to corroborate this position, and obviously, there is huge prospect in this untapped area.

BusinessDay (25 October 2017), reported on Leadway Assurance's proposed collaboration with Chubb, a global insurance leader, to provide cyber-insurance products for the Nigerian market. The earlier insurers begin to leverage on the cyber opportunities, the better it will be for the industry especially in providing financial security required for enterprises to continue to run their businesses in the event of occurrence of cyber-insured events.

Regulatory Snippets on Cyber-insurance In Nigeria

Regulatory oversight on cybercrimes has assumed increased fillip, following the enactment of ***Cybercrimes (Prohibition and Prevention etc.) Act 2015 (CPPA); Economic and Financial Crimes Commission Act, Cap E1 LFN 2004; Money Laundering (Prohibition) Act Cap. M18, LFN 2004; Advance Fee Fraud and other Fraud-Related Offences (Amendment) Act Cap. A6, LFN 2004; and Bank and Other Financial Institution Act Cap. B3, LFN 2004*** etc. For instance, ***section 6(3)(4)CPPA*** provides for fines of up to N7 million or imprisonment for not less than three (3) years or both on convictions for crimes involving computer related fraud, identity theft and impersonation.

Apparently, there currently exists no cyber-insurance policy that could mitigate such incidence when they arise in Nigeria. Initiatives envisaged by the draft ***National Insurance Commission (NAICOM)'s Insurance WEB Aggregators Operational Guidelines,*** and ***Statement of Regulatory Priorities for 2017*** (published January 2017), could be welcome development in this regard. The (latter) NAICOM publication states (at page 3) that "*the Commission is currently consulting on the membership of an Information Technology Working Group (ITWG) that will develop a framework for balanced adoption of technology driven innovation in the industry...opportunities in InsurTech, RegTech and strategies for cost effective deployment of Information Technology.*"

This deficit requires prompt stakeholder and regulatory actions to provide cyber-insurance products and engender facilitative regulatory framework to grow such operations in Nigeria. According to Fitch Rating, cyber-insurance global worth is estimated to increase to US$20 billion before 2020; the USA, the world's largest cyber-insurance market, generated US$1 billion premium in 2015. Nigerian industry players need to be well-positioned to tap these opportunities as cyberattacks will continue to target both local and international personalities and corporate entities' data around the globe. Regulators and stakeholders need to be proactive in their approach to cyber-insurance as the reality of cyberattacks and attendant business opportunities and risks are unassailable. Insurance brokers can also take a cue from Stanbic IBTC Brokers that provide advisory support on Cyber liability insurance product as part of its services.

Cyber-Insurance and Its Huge Opportunities for Stakeholders

Cyber insurance is yet to find its footing in Nigeria. Apparently, lack of awareness and underwriting experience, dearth of industry data on cybercrime and related losses, cyber risks unpredictability, and high correlation of one type of cyber risk with another could be some of the debilitating factors. Surprisingly, no individual nor corporate organization is immune from cyber risks in as much as they use phones containing important data, send and receive emails, operate internet transactions (e-banking, e-payment, e-registration etc), publish electronic content, engage the services of third service providers for storage, processing or sharing of confidential information etc. amongst others. This serves as a huge market for insurers as digital eruption is gradually taking over manual services in every sectors including government parastatals in the country. In the *Nigeria Electronic Fraud Forum Annual Report 2016*, documenting 19,531 fraud cases in Nigerian banks, the traditional channels recorded the lowest number: cheques (12), across the counter (325), kiosk(3); compared to ATM (9522), e-commerce(520), internet banking (698), mobile(3832), POS(1658), Web(2677) and other channels(284).

Cyber insurance related work could also be a goldmine for professional service providers to the insurance industry. For example, legal and regulatory advisory service opportunities to clients on insurance policy interpretation, product development, risk management, regulatory compliance, and drafting/reviewing various agreements such as cyber risk agreements and reinsurance contracts. Some key clauses that would interest lawyers include: indemnity provisions especially on scope, liability limitations, governing law (in multi-jurisdictional party), and dispute resolutions etc. These must be negotiated/advised on with the aim of meeting local compliance requirement and international best practices.

Nigerian insurers could leverage on these opportunities by partnering with foreign insurance firms with vast experience in cyber-insurance to provide various products, covering - business income loss, funds transfer fraud, telecommunication theft, business interruption and additional expenses, legal and forensic services, computer fraud, third party defence and liability expenses, data security breaches, defence and liability judgement payment, proprietary breach actions, cyber extortion, physical assets damage, etc.

Conclusion

Cyber insurance is still novel in Nigeria's insurance landscape but its increasing relevance is inevitable, given technology developments and consequent business realities and risks. Insurers need to develop a healthy cyber-insurance portfolio through market research and data, out-of-the-box thinking to cover future risks, and improve home grown cyber-insurance products development. A look at some other African markets reveals that cyber insurance is still evolving; nonetheless Nigeria can be monitoring developments and leverage learning points. For instance, South Africa (SA) tabled revisions to her *Cybercrimes & Cybersecurity Bill* in February 2017. These include "new structures to fight cybercrime" and international collaboration towards meeting up with industry challenges and ensuring effective cross-border law enforcement; challenges which are also tasking developed markets like the USA and Western Europe. The SA legislation has, (as at December 2017), not yet been enacted, albeit the original draft was published for comments in August 2015. All Nigerian stakeholders: underwriters, regulators (NAICOM, NCC, NITDA, etc), brokers, professional service providers (actuaries, loss adjusters, technology developers and consultants, lawyers, etc) all have a role to play. Cyber insurance could represent a new horizon of opportunity because almost every business enterprise is a potential insurance client.