Deloitte.

Nigeria Cyber Alert
June 2015

‘Cyberharam’: can Nigeria prepare for the next generation of terrorists?

Bombs here, bombs there. This was the case in Nigeria a short while ago. Many could not believe that such a thing could happen in a nation where everyone appeared to be peace-loving and hospitable. It was unheard of that a Nigerian will wrap himself or herself with a bomb and commit suicide in an attempt to kill other people. The worst we imagined at that time was economic instability as a result of corruption or clashes based on religious doctrines. Even the Nigerian President Goodluck Ebele Jonathan, in July 2014 admitted that the intensity of the Boko Haram crisis in the North East caught the government and the security agencies unaware. The unfortunate reality is that there is a new type of terror that is brewing and evolving at an alarming speed all around the world; this threat is more sophisticated and can cause exponentially more damage than Boko Haram. This new generation of terrorism may not be in close combat but will be in cyber space. A director of the Federal Bureau of Investigation (FBI) in 2013 said he expects cyber threats to surpass the terrorism threat that nations will face in the years to come.

The capacity to inflict serious damage from cyber space is not just a marketing gimmick used by security vendors to promote their business, but has now become a well-established trend with occurrences making headlines across the globe. Of worthy mention is the attack that destroyed centrifuges at an Iranian nuclear facility; we can also recall the Sony Pictures Entertainment hack late last year. Even in Nigeria, it was reported that the website of the Independent National Electoral Commission (INEC)

was hacked on the day of the 2015 presidential election. These forms of attacks in cyber space, which may be termed “cyber war”, range from simple probes, website defacement, denial of service and espionage, to wide-scale terrorism.

We are seeing significant interest by terrorist organizations in leveraging cyber capabilities to further their cause. For example, the Boko Haram sect gets media attention by leveraging social media. In 2013, the Syrian Electronic Army (SEA) hacked the Twitter account of a news agency and falsely claimed the White House had been bombed and President Barack Obama was injured.

Cyber security has now become a key topic amongst government policy makers worldwide and from all indications, it will be a key topic till the end of time.

This led to a US$136.5 billion dip on the S&P 500 index that same day. If terrorists are choosing to dedicate so much resources into advancing their knowledge of cyber security, why then should our law-enforcement agents be caught unawares and keep playing catch up?

The same way many never saw Boko Haram coming 15 years ago, we may also be blindsided to the concept of cyber-terrorism on the Nigerian infrastructure. Many mistakes of the past have been laced with statements assuming that such problems can only happen in the western world. For instance, I recently facilitated a cyber-security forum for c-level executives in West Africa where we discussed the report of the possibility to hack into a plane’s control system via the in-flight Wi-Fi system. After much deliberation, one of the participants remarked, “thank God we don’t yet have Wi-Fi in our domestic planes.” I think the emerging threats should not be easily dismissed with such statements. Cyber terrorism knows no borders. The internet, although very good, may be used as a recruitment tool for terrorists worldwide as has been alleged of ISIS and an evolving weapon in the global distribution of chaos.

Cyber security has now become a key topic amongst government policy makers worldwide and from all indications, it will be a key topic till the end of time. The advent of cyber as a weapon of warfare is rapidly gaining momentum and Nigeria is not immune to such threats. It is only a matter of time before it becomes full blown. In 2012, it was reported that there was a 60% increase in the attacks on Nigerian government websites. We cannot control when the threat will occur but we can control our response to it. We have ample time now to invest massively in cyber-capacity development and embark on deliberate media strategies.

We are relatively in a time of national Cyber-Peace now and as I recall from an old adage, ‘a soldier prepares for war in time of peace’. Peace should not be a factor to cost us our strength; peace is a time when development and massive investment in cyber security and cyber related matters should become paramount issues. As of today, it is unbelievable that only one tertiary institution in Nigeria currently administers cyber security as a course of study. A large proportion of Nigerian PhD holders in Computer Science related courses are not Cyber Security experts. The expertise is lacking and hence a defence strategy cannot work with the status-quo.

It is only a vision of cyber-war and cyber-peace that will make the United States embark on a Cambridge Vs. Cambridge cyber challenge; a new competition geared at improving cyber security initiatives between MIT in Cambridge, Massachusetts and Cambridge University in England.

Also a cyber-security fellowship was initiated to aid knowledge transfer

between the United States (US) and the United Kingdom (UK). The US Government is pitching $14Billion in cyber security spending for fiscal year 2016 across all its agencies. This budget keeps increasing year after year.

Investment strides like this can only be done because of a high probability of an impending global catastrophe that can come as a result of cyber-terrorism. Nigeria has to take charge and make significant investments in cyber security capability so as to adequately defend the nation against cyber-attacks.

In this war, the possibility for success is still a moving target as both heroes and villains are learning and seeking out new ways to defend and attack respectively. Today's defence or better said; this second's defence is the next second's weakness. How can we play in such a field where the weapons and the yardstick of success change on a per second basis? How do we fight a war that will not be limited to a section of the country but has the potential to undermine even the high and mighty in every nook and cranny?

A next step could then be inculcation of cyber security as a discipline of study in Nigerian Universities. We need to win the future and that can only be achieved by educating the present.

My experience with performing ethical hacking and cyber security related assignments across 16 countries has put me in a better position to appreciate the words of the former FBI director, Robert Mueller, who said, "There are only two types of companies: Those that have been hacked, and those that will be." I desire that all organisations in Nigeria wake up to this new reality. I was speaking at a cyber-security conference in Washington DC recently and did not hesitate to tell the bankers that they appear to focus more on credit risk, market risk, and liquidity risk without appropriately considering cyber risk.

Whilst the traditional risk management portfolio is great, cyber-risk has the immense power to wipe out an organisation's shareholder value faster than the combination of these other risks. The role of governments cannot be overemphasized in tackling cyber threats,

It should no longer be a backburner idea which should be handled only by the Ministry of Science and Technology or the office of the National Security Adviser. It is a frontline issue that could result in cascading economic catastrophes.

In tackling the challenges posed by cyber threats, one top consideration is to identify our critical infrastructure and assess the risks to these systems so as to identify threats and vulnerabilities. Examples of our critical infrastructure include those supporting our financial and telecommunication systems, systems hosting classified national security information amongst others. On conclusion of the assessment, a long term roadmap that will guide investments in securing our infrastructure should be prepared.

As a nation, we need to invest massively in cyber-capacity development with emphasis on law enforcement agencies, policy framework developers, the judiciary and both the state and federal legislative arms of government. All routes to cyber capacity must be taken. Other training initiatives could include wide-scale Federal Government and private sector backed scholarships for students with interest in cyber security. A next step could then be inculcation of cyber security as a discipline of study in Nigerian Universities. We need to win the future and that can only be achieved by educating the present. The enactment into law of the Cybercrime bill is a step in the right direction and the Nigerian government has to be lauded for that

achievement. The incoming National Assembly and President should work together for a flexible and evolving budget that caters to the demands of cyber security. Research and development in cyber security must become fluid and must provide for the future cyber threats.

The establishment of a joint task force for cyber security and building of a National Cyber Command Centre that will be the go-to centre for cyber security in Nigeria and will facilitate Cyber intelligence integration for all governmental parastatals and other institutions in Nigeria. Collaboration among stakeholders and cyber-intelligence sharing is key to having a united front against cyber terrorism. During our counter strikes against Boko Haram, it was reported that at our time of need, countries were not willing to sell weapons to cater for our needs. It makes no sense for us to allow such to repeat itself. We have to be prepared and Nigerians can do it.

It is difficult to estimate the level of damage a catastrophic event such as a successful cyber-attack could inflict on the future of Nigeria but I am not ready to find out and I hope Nigerians are not eager to find that out either. This is why it makes logical sense to be prepared beyond Sambisa and Shekau, and look forward to successfully defending our national infrastructure from cyber-terrorism. In conclusion, I would like to answer the question posed by the title of this article. Is Nigeria prepared for the next generation of terrorism? No we are not, but YES WE CAN BE.

Tope S. Aladenusi *is a Partner at Deloitte Nigeria and the President of ISACA Lagos Nigeria, the largest association of IT audit, IT risk, IT governance and Cyber Security professionals in Nigeria.*

Contacts

For more information, please contact:

Tope S. Aladenusi
Partner
Telephone: +234 1 904 1730
Email: taladenusi@deloitte.com