CYBER SECURITY AND LATEST DEVELOPMENT: TOWARDS EFFECTIVE GLOBAL REGULATION AND GOVERNANCE IN CYBERSPACE*

Abstract

Cyber security attacks are constantly evolving and becoming increasingly damaging. Cyber security is a complex transnational issue that requires global cooperation for ensuring safe internet. Cybercrime is the greatest threat to every individual and or company in the world. As cybercrime become more lucrative and cybercriminals become smarter, cyber security too will have to be intelligence driven, enabling a swift response to the advance attacks. This paper is aimed at performing a critical scrutiny of the purpose of cyber security regulation in Nigeria and globally. This paper focuses on the main challenge in managing cyber security and undertakes a comparative study of the legal framework of cyber security in some other selected jurisdictions. The paper aims at analysing the efficacy or otherwise of the extant Nigerian statutory framework in relation to those of other jurisdictions. The paper makes a case for an effective and comprehensive body of legislation to deal with the precarious position of cyber security in Nigeria.

Keywords: Cyber security, cyber crimes, data protection, information security, cyber threats

1. Introduction

Cyber crime is one of the fastest growing crimes across the globe, and its increasing in number, sophistication and cost daily. In August 2016, it was predicted that cyber crime will cost the world $ 6 trillion annually by 2021, up from $ 3 trillion in 2015[1]. Cyber crimes are a seemingly impossible challenge. By their nature, are fast-changing, borderless, asymmetric and difficult to predict. The World Economic Forum placed cyber security near the top of its latest list of global risks[2]. Cyber crime costs include damage and destruction of data, stolen money , lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post- attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. It is indeed worrisome that the rate of internet connection and use is outpacing our ability to properly manage and secure it. The most common cyber threat we encounter daily is credential theft; every day we use credentials for access to websites, computers, smart devices and other sources to complete business or personal transactions. Furthermore, with the ever – growing pervasiveness of computers, mobile devices, servers and smart devices, the aggregate threat exposure grows each day. Multiple cyber – attacks and compromise of personal information of millions of people globally show that the complexity and intensity of cyber security attacks are on the rise, and it could have broader political and economic ramifications. It is pertinent to state that irrespective of the size of a company, a successful cyber attack has enormous financial and reputational implications[3]. It is important to note that conventional crimes can be addressed by way of physical measures involving detection, investigation, apprehension and prosecution, however, cyber crimes are committed in the space and are digitized which makes it difficult to detect or find its perpetrators.

Globally, the growth in information technology and E-commerce sector, has given rise to cyber crimes, causing a huge loss to nation states and its people. Many countries and international organizations are overwhelmed by the activities of cyber crime perpetrators hence reflecting the issue of cyber security as a national and international issue[4]. Data breeches have gained more attention due to the impact of digitization on financial, healthcare, SME's and other industries. Cyber security laws are needed to prevent economic harm to companies and individuals. On aggregate, cyber security incidents take a significant economic toll. If companies are to successfully defend themselves from these attacks, they must and should as a matter of priority have the right laws, policies and procedures in place[5]. Companies must adopt both proactive and reactive security solutions. They must and should wake up to the realities of data breeches, their vulnerable state, and ways of mitigating the risks as well as putting in

*By **Ngozi Chisom UZOKA**, **PhD,** Lecturer, Department of International Law and Jurisprudence, Nnamdi Azikiwe University Awka, Anambra State. Nigeria. Phone No: 08063212174 E-mail: chisongozi@yahoo.com , nc.uzoka@unizik.edu.ng.

[1]S Morgan: 2019 Official Annual Cybercrime Report available at http://www.

[2]World Economic Forum: The Global Risks Report 2019. 14th edn. Available at htpp://www.weforum.org accessed on 15th day of November, 2019.

[3]Cyber Security and Risk Management 2019: Financier Worldwide Magazine, November, 2019 available at http://www.financierworldwide.com accessed on 12 November, 2019.

[4]O Osho & AOnoja, National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis, 2015 *International Journal of Cyber Criminology*, Vol 9(1)120-143.

[5]Emerging Trends in Cyber Security: Financier Worldwide Magazine, November, 2019 available at http://www.financierworldwide.com accessed on 12 November, 2019.

place additional resources into their cyber defences. Cyber security law should attempt to reduce these negative impacts both in individuals, companies and the economy as a whole. The key overall trend is the growing willingness of regulators to get involved in setting out ever more prescriptive requirements, and to apply sanctions to those who they do not think comply.

2. Definition of Cyber Security

Cyber security is a very critical topic. There are several critical questions that must be answered in relation to cyber security to ensure the protection and integrity of I.T systems and data. The definition of cyber security is crucial; however there are no globally harmonized definitions of cyber security. Almost every country has provided its own definition in the strategy. Cyber security can be defined as the protection of cyberspace itself, the electronic information, the ICT's that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace[6]. Cyber security has also been defined as combating every cyber threat within the cyber space[7]. Cyber security is the 'organization and collection of resources, processes, and structures used to protect cyberspace and cyber-enabled systems from occurrences that misalign de jure from de facto property rights'[8].There is an ill defined enemy behind the emerging trend of cyber attacks. The enemy could vary, and understanding their evolving capabilities and organizational limits is crucial to fending off cyber attacks orchestrated by a range of possible foes, such as state-sponsored attackers, hackers, anarchists, and criminal gangs.

3. The Nature and Need for Cyber Security

a. **Innovative Products:** As new products emerge, tactics change and new attack methods are constantly being developed by malicious actors. It accords with common sense that for cyber security controls to remain effective, it should also embrace innovative solutions if they provide a good fit and true value.
b. **Cyber Threats have Come to Stay:** Threats to cyber security no matter how well equipped a company is, cannot be evaded but the exposure rate can be minimized. Data security and privacy have been a burning issue for the past few years[9]. As maturity in these areas continues to evolve, it is imperative to keep up with the regulatory requirements. Proper documentation of compliance initiatives is vital to securing organization's data.
c. **Information and Communication Technology:** The need for cyber security is becoming increasingly important due to our large dependence on information and communication technology. Cyber security is important for individuals, public and private organizations, and government agencies. However, guaranteeing security often proves to be difficult. The issue of security of the cyber space is not limited to the above, it is also relevant to service providers, administrative organizations, NGO's, sporting organisations and political parties, all of which are target of breaches and the stealing of information[10].

4. Cyber crimes in Jurisdictions

Nigeria

Nigeria is not left out by the activities of cyber crime incidences. Nigeria's cyber crime statistics is high and climbing[11]. Cyber security is considered in Nigeria as well as a national security threat. Issues pertaining to cyber security are handled by the Office of the National Security Adviser. In Nigeria, steps have been taken to help combat the cyber security threats in our cyberspace. In June 2014, the National Cyber Security Policy and Strategy drafts were officially presented at a symposium in Lagos, Nigeria[12]. In 2015, the Cyber Crimes (Prohibition) Prevention, etc Act was enacted in response to the prohibition, prevention, detection and investigation and prosecution of

[6]R Von Solms &J Van Niekerk, 'From Information Security to Cyber Security', *Computers & Security* 38(2013), 97-102.
[7]N Shafqat&AMasood, 'Comparative Analysis of Various National Cyber Security Strategies', *International Journal of Computer Science and Information Technology*. Vol. 14, No 1, 2016. P. 129
[8]D Craigen, N Diakun-Thibault & R Purse, 'Defining Cybersecurity', 2014 *Technology Innovation Management Review*. 4 (10).
[9]K Nakata, Global Threat Intelligence Report. Available on http://www.nttsecurity.com, accesed on 15th, November, 2019.
[10]Hans de Bruijn & M Janssen, Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies, Government Information Quarterly, Vol. 34, Issue 1, 2017 Available at http:www.sciencedirect,com accessed on 16th, November, 2019.
[11]O Osho & A Onoja, National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis, 2015 *International Journal of Cyber Criminology*, Vol 9 (1)120-143.
[12]*Ibid*.

cybercrimes. The Act provides a legal framework for the implementation and evaluation of response and preventive measures in the fight against Cyber Crimes as well as other related in line with international best practices.

Before the enactment of the Cyber Crimes (Prohibition) Prevention Act of 2015, the Advanced Fee Fraud and other related Offences Act, 1995, Economic and Financial Crimes Commission Act, 2004 and the Money Laundering (Prohibition) Act 2011 contained provisions regulating cybercrimes in Nigeria. However, these Acts were inadequate to regulate cybercrimes in Nigeria, hence the need for an enactment of cybercime Act. Section 7 of the Act provides for the registration of cybercafé. It provides that from the commencement of the Act all operators of a cybercafé shall register as a business concern with the Computer Professional Registration Council in addition to business name registration with the Corporate Affairs Commission. This raises the issue of compliance and enforcement of this provision, as nobody is to carry out the enforcement. Most owners of cybercafés in Nigeria are not knowledgeable about the requirement of this provision or have the financial resources to register such business under Part C of Companies and Allied Matters Act. Hence, provisions like this makes the Act a mere Act lacking in power. Section 21of the Act, imposes a duty on any one operating a computer system to notify the National Computer Emergency Response Team of any attack or intrusion on its computer. Any person who fails to report such an incident is liable to pay a fine of 2,000,000 million to the National Cyber Security Fund. However, the Act failed to provide how and where the Computer Emergency Response Team will be contacted and the procedure for contacting them.

From the foregoing, it is evident that the Act did not make provision for mode of enforcement of its provisions. Thus there is a gap for the law enforcement agencies that are would be responsible for the enforcement of its provisions. It is necessary that proper detection and enforcement mechanisms should be put in place to give effect to the provisions of the Act.[13] It is important to note that the Attorney General of the Federation is empowered by the Act to make rules and procedure for the enforcement of the provisions of the Act. It is pertinent to note that Nigeria is not a signatory to any cybercrime convention; this makes international cooperation difficult and challenging. Nigeria needs to become a signatory to the Budapest Convention on cybercrime in order to enhance its international cooperation in combating cybercrimes. The Cybercrime (Prohibition Prevention etc) Act is a good step in the right direction but if the lacuna is not addressed it will be one of the dormant laws in Nigeria.[14]

United Kingdom

In the U.K, there is emphasis on the attack of compromising individual's work email accounts, often due to password reuse. A recent Industry Cyber Exposure Report found that organisations in every industry in the U.K have serious issues with version management of internet-facing systems[15]. The UK has been fighting cyber attacks based on their National Security Strategy since 2010. Then the UK Cyber security strategy was implemented in November 2011[16]. The National Cyber Security Programme (NCSP) is managed by the office of Cyber Security and Information Assurance in the Cabinet Office, under the Cabinet Office. The UK has invested in their cyber security strategy £ 860 million since its inception[17]. Government agencies to support the strategy include intelligence agencies and Ministry of Defence, the Government Communications Headquarters, the Ministry of Justice, the National Crime Agency, the Child Exploitation and Online Protection and a host of many other agencies[18]. In terms of cybersecurity awareness, the UK launched the Cyber Essentials and Cyber Streetwise programmes to improve awareness for organizations and small and medium size businesses. They also educate citizens using the Internet Service Providers (ISPs) Guiding Principles Publication. UK universities have also joined 'Academic Centres of

[13]See generally I. K.E. Oraegbunam and B. E. Ewulum, 'Assessing the Nigerian Cyber-Security Law and Policy for Protection of Critical Infrastructure for National Development' in G. N. Okeke et al. (eds), *Law, Security and National Development*, Awka: Amaka Dreams Ltd., 2017, pp. 62-87.

[14] See I.K.E. Oraegbunam, 'Effects of Cyber Criminality on Socio-Economic Development in Nigeria: Examining the Gains of Cybercrimes (Prohibition, Prevention, Etc) Act 2015', in A.A. Kana *et al* (eds.), *Law and Economy*, Ibadan: Yinkatec Printers Nigerian Limited, 2016, pp. 715-730

[15]M Rider, Annual Report on Cyber Security and Risk Management 2019: Financier Worldwide Magazine, November, 2019 available at http://www.financierworldwide.com accessed on 12 November, 2019.

[16]*Ibid*

[17]R Sabillon, V Cavaller & J Cano, 'National Cyber Security Strategies: Global Trends in Cyberspace', *International Journal of Computer Science and Software Engineering*, Vol. 5, Issue 5, 2016.7

[18]United Kigdom Cabinet Office, The UK Cyber Security Strategy- Report on Progress and Forward Plans. London: UK Cabinet Office, 2014. 23

Excellence' in the cyber research area[19]. It is important to state that in May 2019, several U.K organisations were victims of attacks targeting the Microsoft SharePoint remote code vulnerability[20].

United States of America

The USA published the first draft of cyber security strategy in 2003[21], when cyber attacks were not very common. The strategy was part of the National Strategy for Homeland Security and complemented by the National strategy for the Physical Protection of Critical Infrastructures and Key Assets. The cyber strategy includes five national priorities, a National Cyberspace Security; Response System, Threat and Vulnerability Reduction Program, Awareness and Training Program and Securing governments' cyberspace[22]. The changing spectrum of cyber security strategy has made it imperative to update the cyber security strategy to accommodate emerging threats and relevant counter measures. Countries like the USA and UK have constantly published subsequent versions of their strategies as well as a constant upward review. The USA recognizes cyberspace as a fifth domain of its own national security agenda in tandem with pre-existing domains such as land, sea, air, and space. As such the United States established the United States Cyber Command (US CYBERCOM) in 2009 to recognize that fact and organize a body under the US Department of Defence to address cyber issues[23]. On February 22, 2013, at the fourth annual Cyber Security Conference in Washington DC, the Director of Operations said that part of Cybercom's mission is to help in defending the homeland, especially against cyber attacks and other activities in cyberspace that could affect national security[24]. Major Cyber threats in the US include ransomeware, spearphishing, business mail compromise, and malware and insider malfeasance. In 2015, the US Office of Personnel Management experienced a cyber penetration that impacted over 21 million people and exposed serious counterintelligence vulnerability for the US government[25]. Some other data breaches affecting millions of consumers have also affected Mariott Starwood Hotels, where sensitive passport information was compromised, as well as Quora, Google, Anthem and T-Mobile[26].In the U.S, the California Consumer Privacy Act was born, drafted, passed and ratified in only few days. The Act will have profound implications as a number of technology giants will be caught up in it. The Act challenges U.S federal government to catch as many persons they can as its implementation on January 1, 2020 approaches[27]. The USA is the only country in the world that established a formal international strategy to promote cyber security in cyberspace[28].

South Africa

Just like most African countries, cyber threats are on the increase daily. This is most evident in the financial services sector especially banking. The attacks are mostly targeted at the consumer/customers of digital transaction services rather than attacks on the banks directly to penetrate their defences[29]. There is also a growing target to high-net-worth customers or politically exposed persons through coordinated attacks from bank staff and external third parties, typically by the service providers. South Africa's Cyber Security policy has been in existence since 2010; it is based on the National Cybersecurity Policy Framework that was created from National Cybersecurity Strategies like that of UK, Australia and some other countries. The South African Cybersecurity policy involves the government, public and private sectors, society and special interest groups to protect cyberspace from cyberdsecurity threats. The Framework was supported by the National Cybersecuirty Implementation Plan. The

[19]United Kigdom Cabinet Office, The UK Cyber Security Strategy- Report on Progress and Forward Plans. London: UK Cabinet Office, 2014. 23

[20] Ibid

[21]N Shafqat&AMasood, 'Comparative Analysis of Various National Cyber Security Strategies', *International Journal of Computer Science and Information Technology*. Vol. 14, No 1, 2016. P. 129

[22]R Sabillon, V Cavaller& J Cano, 'National Cyber Security Strategies: Global Trends in Cyberspace', *International Journal of Computer Science and Software Enginering*, Vol. 5, Issue 5, 2016.7

[23]W Harrop&A Matteson, 'Cyber Resilience: A Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the USA' (2015) in F Lemieux (eds) Current and Emerging Trends in Cyber Operations. Palgrave Macmillan's Studies in Cyber Crime and Cyber security (Palgrave Macmillan, London) 149-166.

[24]*Ibid*

[25]J S Campbell, Annual Report on Cyber Security and Risk Management 2019: Financier Worldwide Magazine, November, 2019 available at http://www.financierworldwide.com accessed on 12 November, 2019.

[26]*Ibid*.

[27]*Ibid*

[28]United States of America Government, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, Washington D.C: The White House, 2011.

[29]R Kamil, Annual Report on Cyber Security and Risk Management 2019: Financier Worldwide Magazine, November, 2019 available at http://www.financierworldwide.com accessed on 12 November, 2019.

Framework was created to address specific areas like cybersecurity measures to fight cyber threats, promotion of a cybersecurity culture, intelligence strengthening to face cybercrime, cyber terrorism and cyber warfare, to protect national critical information infrastructure, to build cybersecurity partnerships and to ensure proper cyber governance for South Africa's cyberspace. It is important to state that the Justice Crime Prevention and Security Cluster is a government agency saddled with the responsibility of overseeing the national cyber security strategy by coordinating other government clusters.

Israel

Israel owns a world renowned cyber defence and is constantly exporting cyber-related product and services second to the United States. Israel's cybersecurity was targeted to position Israel on the top five list of global superpower nations[30]. Israel's National Cyber Bureau (INCB) was founded in 2011 as an advising agency for the prime minister, the Israel government and all its committees to make inputs towards the national cyber field policy. The INCB operates based on the National Security Council framework. Other agencies involved with the Israeli cybersecurity policy includes; the Cyber Authority, the General Security Service of Israel and the Mossad[31].

5. Conclusion and Recommendations

Cyber security has gained more prominence in recent times more than issues of national physical interest. Countries, all over the world are formulating cyber security strategies to address this grave issue. It is observed generally that reporting on cyber risks is a purely compliance-based exercise; companies only do an elaborate reporting and disclosure in greater detail after they must have suffered a publicly disclosed cyber incident[32]. It was discovered that most countries have a cyber security strategy. However, these strategies are mostly static documents that do not or partially address the dynamic nature of the cyber space. It is also imperative to state that the study emphasize cyber security as a tool to reach national security goal, and not a solution for everything. Hence, there is the need to harmonize national cyber security strategy with other strategies. The following recommendations are hereby proffered.

Security Awareness Training

All cyber security strategies emphasize the need of raising cyber security awareness in general public. The fact is that most cyber attacks begin with a simple email. More than 90 % percent of successful hacks and data breeches stem from phishing, emails crafted to lure unsuspecting recipients to click a link, open a document or forward information to someone they shouldn't. One can have all the wonderful technologies and layers of security protections in place, but ultimately it comes down to the people being really aware of the threats and knowing how to detect them and report them. Some of the nations studied have defined nation-wide cyber security outreach programs for their citizens, where they provide cyber security tools and practical education, for example, the UK's 'Get Safe Online' and Cyber Security Month' annually of US.

Information Sharing: On the global scale in fighting cyber attacks, information is key and powerful in cyber security. If a breach occurs in one organization, we can be rest assured that the same tactics will be used on another organization in the near future. If the data about the first known breach is made available, other organizations can prepare themselves. Shared knowledge also allow regulators and law enforcement agents to objectively manage incentives to guide corporate cyber security governance, data gathering and information sharing.

Compliance and Communication: Regulators should as a matter of policy and practice require companies to disclose incidents of any data breaches. It was discovered that these regulators share too little of the data publicly and most times they don't even share at all. The Nigerian Securities and Exchange Commission should require publicly traded companies to disclose their risk exposure.

Public-Private Partnership: Public-private collaboration is necessary since private sector owns most of the internet infrastructures. The compliance level to most of our regulator's laws is inadequate. It is suggested that there should be a public-private partnership in Nigeria to give companies the operational support they need to monitor their security and share information via a trusted source. A good example is the Cyber Net, an online platform developed

[30]R Sabillon, V Cavaller& J Cano, 'National Cyber Security Strategies: Global Trends in Cyberspace', *International Journal of Computer Science and Software Enginering*, (2016) Vol. 5, Issue 5.
[31]*Ibid.*
[32]M Barrachin & A Pipikaite, 'We need a Global Standard for Reporting Cyber Attacks', *Harvard Business Law Review.* Available at htpp://www.hbr.org accessed on 15th November, 2019.

and managed by Israel's National Computer Emergency Response Team(CERT), part of Israel's National Cyber Directorate(INCD). The incentives for participation are access to data that help companies to identify potential threats. All data shared is anonymously done and the INCD does not share reported data with other government entities including law enforcement and investigative agencies.

Training Employees: Training of employees by organisations on how to recognise and defend against cyber attacks is the most important sector of the cyber security. As cyber defence tools are also expanding and evolving, company staff should be trained and retrained on modern day cyber defence programmes. New innovations in technology, such as machine learning (ML), artificial intelligence (AI) should also be taken into consideration.

Proactive Cyber security: Every company has gone 'Tech', FinTech (Financial services), LegalTech (Lawfims), GovTech(government) etc. and they all need to scale up their cyber protection. There is an urgent need to take preventive cyber security measures by all and sundry. Consumers and companies need to pay more attention to cyber security. Companies need to be proactive about risk, and the nature of risk has changed to become more inclusive of technology and information assets than before. Companies need to regularly engage internal and external cyber security resources in the same way it has historically engaged financial and legal resources.

Upgrade of Information Technology Budget: Companies must always allocate appropriate budget for information security and defence as a matter of practice.. It is not enough if the measures put in place are not properly updated as soon as new technologies are released and older technology replaced in line with the current state of art technology. This is not a once- and - done event. As the cyber threat landscape is constantly evolving, so are the regulatory requirements. Cyber preparedness has to be reviewed and adjusted regularly.

Increase in Penalty: As the frequency and the impact of data breeches continue to increase, the cost of cyber security compliance programmes also will increase, as well as the penalties imposed by government agencies on companies that suffer data breeches.

Cyber Insurance Plan: Companies should have cyber insurance plans, which can help companies recover in the event of data breaches. It is important to note that this arrangement should complement, and not replace a company's cyber security provisions.

International Collaboration: Since it is impossible to guarantee security of the national cyber space in an insecure global cyber environment, almost all the strategies have emphasized the need of international collaboration in the domain of cyber security, especially with neighbouring and regional countries. Cyber security strategies of USA and US have mentioned action plan to improve global cooperation.