E-commerce and Cyber Security Regulation in Africa[1]

Introduction

The advent of the internet and the dotcom era has strengthened the notion that the world is a global village. The internet has simplified human activities which could have been cumbersome.

The use of the internet has surge astronomically. Over 3,440,839,840 people are connected to the internet, accounting for 40% of the world population, and more than 1,070,397,120 websites have been created.[2] The world internet usage and population statistics as at June 30, 2016 showed that Africa with a population of 1,185,529,578 has 339,283,342 internet users[3].

The internet has provided easy access to information, simplified investigation for security agencies, enhanced social network, and advanced business to consumer sales (e-commerce).

However, the adage that every good thing has a dark side has found expression even in internet usage. Notwithstanding the laudable benefit of the internet, there are peril associated with it. The internet is continuously buzzing with vices which threatens the security of Nations, businesses of conglomerates, and the privacy of individuals. These vices have been qualified as cyberattacks. Cyberattacks include but are not limited to hacking, mail bomb, trojans, web defacement, Denial-of-Service ("DoS"), trap doors, spoofing, phishing, and vishing. These cyberattacks have resulted in theft of data and money, destruction of data, extortion, distribution of pornography, and disruption of online services amongst others.

The essence of this article is to discuss the growth of e-commerce in Africa, the threat posed by cyberattacks to Africa and the African Union Convention on Cyber Security and Personal Data Protection (the "Convention") as it relates to cybersecurity.

E-commerce in Africa

E-commerce has made purchase of goods and rendering of services easy. With a single click, goods could be purchased, shipped and delivered anywhere in the World within a short time. E-commerce has enabled companies to reach customers in countries where they do not have a physical presence. Enormous transactions are concluded daily on the internet which sum up to billions of dollars annually.

Statistics showed that in 2013, global e-commerce sales amounted to $839.8 billion and is expected to reach $1.92 trillion this year (2016)[4]. Meanwhile in 2013, e-commerce sales in the Middle East and Africa accounted for 2.2% of global e-commerce sales. With a projection that this could increase between 2016 and 2018 from 2.4% to 2.5%[5]. The projection demonstrate that Africa is an emerging e-commerce market.

---

[1] **Akinkunmi Akinwunmi Esq. LLM in Business and Technology Law (UC, Berkeley)**
NB: This article was first published in the Law Digest Journal, Issue 11 Autumn 2016, pages 26 – 30.

[2] Internet Usage Statistics, retrieved on August 23,2016 from http://www.internetlivestats.com

[3] Internet World Stats Population and Usage Statistics, retrieved on August 23, 2016 from http://www.internetworldstats.com/stats.htm

[4] B2C e-commerce sales worldwide, retrieved on August 23, 2016 from http://www.statista.com/topics/871/online-shopping

[5] B2C e-commerce sales by region, retrieved on August 23, 2016 from http://www.statista.com/statistics/244054/share-of-global-b2c-e-commerce-sales-in-middle-east-and-africa/

Threat Posed by Cyberattacks to the World and Africa

Due to the global nature of the internet, cyberattacks have become transnational. Every gadget connected to the internet is prone to cyberattack. The proximity of the Cyber-attacker is irrelevant, as the illicit act could be conducted from any location.

Statistics divulged that up to 60,740 websites could be hacked daily[6]. The 2016 Symantec Report noted that there were more than 430 million new unique pieces of malware in 2015, a 36% increase from 2014.[7] The number of zero-day vulnerabilities discovered in 2015 more than doubled to 54, a 125% increase from 2014.[8] According to Laura Ani,[9] "IT revolution has brought about a vast array of aides and conveniences that have indelibly influenced modern communication, travel, security and commerce. However the massive gains brought by the information age are not perfect, with the pervasive correlation of human activity with electronic resources and infrastructure there is a crucial vulnerability, which is the ever present risk of abuse, insidious manipulation and sabotage of computer and computer networks".[10]

Individuals, Companies, and Countries have been victims of cyberattacks. In 2013, the financial security system of Target[11]was hacked, this led to the loss of the credit and debit cards of up to 40 million customers[12]. This affected the shares of the Company as its shares fell by 46% year-on-year in the fourth quarter of 2013 to $520 million[13]. In 2015, the Office of Personnel Management of the United States was hacked and the breach led to the loss of data of approximately 21.5 million people made up of both current and former federal employees[14]. In January 2016, Ireland's National Lottery website and ticket machines were knocked offline after a DoS attack.[15]

Africa has also been a victim of cyberattacks. In East Africa, governments are the top target for cyberattacks (33%), telecommunications (22%), and financial services (17%).[16] Cyberattacks has caused Kenya up to 2 billion Kenyan shillings (over $23 million)[17]. In 2013, Google Kenya website was hacked[18].

[6] Internet Usage Statistics, retrieved on August 23,2016 from http://www.internetlivestats.com

[7] Internet Security Threat Report Volume 21, April 2016, retrieved August 23, 2016 from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16351507&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2

[8] Supra. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. PC Tools: What is a Zero-Day Vulnerability?, retrieved August 23 2016 from http://www.pctools.com/security-news/zero-day-vulnerability/

[9] Laura Ani is a Research Fellow, Nigerian Institute of Advanced Legal Studies.

[10] Laura Ani: Cyber Crime And National Security: The Role Of The Penal And Procedural Law, retrieved on August 22, 2016 from www.nials-nigeria.org/pub/LAURAANI.pdf

[11] Target cyber breach hits 40 million payment cards at holiday peak, published December 19, 2013, retrieved on August 24, 2016 from http://www.reuters.com/article/us-target-breach-idUSBRE9BH1GX20131219

[12] Dough Drinkwater, Does a data breach really affect your firm's reputation? CSO Online, published January 7, 2016 retrieved 24th August 2016 from http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html

[13] Supra

[14] Retrieved on August 24, 2016 from https://www.opm.gov/cybersecurity

[15] Irish lottery site and ticket machines hit by Distributed-Denial-of-Service attack published January 21, 2016 retrieved on August 24, 2016 from http://www.bbc.com/news/technology-35373890

[16] East Africa Telecoms Top Cyber Attacks Targets published June 26, 2016 retrieved August 23, 2016 from http://allafrica.com/stories/201606270369.html

[17] supra

[18] Google Kenya's Website Hacked, Defaced published April 15, 2013 retrieved on August 24, 2016 from http://techloy.com/2013/04/15/google-kenya-website-hacked/

A 2011 Deloitte Touche survey revealed that financial institutions in Kenya, Rwanda, Uganda, the United Republic of Tanzania, and Zambia had registered losses of up to $245 million due to cyber fraud[19]. In the first half of 2013, the Banks in Zambia lost more than $4 million to cybercrime[20].

In February 2016, the database of South Africa was hacked. Identities, details and passwords of approximately 1,500 government employees were posted online.[21]

In May 2016, the website of the University of Limpopo was hacked. Other than leaking exam papers, the details of over 18,000 students were leaked.[22]

In Nigeria, the websites of the Nigerian Police Force and the Central Bank of Nigeria have been hacked[23]. According to Dr. Vincent Olatunji[24], Nigeria has experienced 3,500 cyberattacks between 2015 and 2016, with over 70% success rate and a loss of $450 million[25]. According to Adebayo Shittu[26], Nigeria loses up to N127 billion yearly to cybercrime, which is 0.08% of her Gross Domestic Product.[27] In addition, Nigeria is ranked third in the world for cybercrimes[28].

Cyber Security Regulation in Africa

The deleterious effect of cyberattack has been dominant in Africa, but ignored, and in most cases, it has been dealt with internally by companies as an information technology problem without any coordinated continental effort to nip it in the bud.

Africa did not have any pan-African regulation on the internet and computer usage until 2014. While the European Union ("EU") in 2012 had its comprehensive regulation to govern cybersecurity[29]. In addition, the EU parliament on July 6, 2016 approved the first community-wide rules designed to bolster cybersecurity throughout the EU[30].

In addition, Nigeria and South Africa which boost of the largest economies in Africa dragged their feet on the enactment of cybersecurity laws. South Africa enacted her cybersecurity law in 2002[31] while Nigeria stalled until 2015[32]. When compared with other Countries, it is clear that African Countries arrived late to the party. The United States in 1984 made her first attempt at enacting a law

[19] Henry Quarshie and Alexander Martin-Odoom, "Fighting Cybercrime in Africa", Computer Science and Engineering, Vol. 2, No. 6 (2012), pp. 98-100.
[20] Michael Chawe, "Cybercrime costs Zambian banks $4million", Africa Review, 14 June 2013, retrieved on August 24, 2016 from www.africareview.com/News/Cyber-crime-costs-Zambian-banks--4millio/-/979180/1883006/-/128vr2iz/-/index.html.
[21] SABC cyberattack not unique, published June 13, 2016 retrieved August 23, 2016 from http://www.iol.co.za/news/south-africa/sabc-cyber-attack-not-unique-2034215
[22] supra
[23] NaijaCyberHactivists Shuts down Nigeria Police Force Website published January 27, 2012 retrieved on August 24, 2016 from http://techloy.com/2012/01/27/naijacyberhactivists-shuts-down-nigeria-police-force-website. Nigeria's Central Bank Website Hacked published January 27, 2012 retrieved August 24, 2016 from http://techloy.com/2012/01/27/nigerias-central-bank-website-hacked.
[24] Acting Director General of the National Information Technology Development Agency, NITDA,
[25] Nigeria records 3,500 cyberattacks in last one year, published March 31, 2016 retrieved on August 24, 2016 from http://www.vanguardngr.com/2016/03/nigeria-records-3500-cyber-attacks-last-one-year/
[26] Nigerian Minister for Telecommunication
[27] FG Moves to Curb Cybercrime Threat to National Security published August 3, 2016 retrieved August 3 2016 from http://www.thisdaylive.com/index.php/2016/08/03/fg-moves-to-curb-cybercrime-threat-to-national-security/
[28] Nigeria Ranked Third In The World For Cyber-Crime, Says Survey, retrieved August 24, 2016 from http://www.balancingact-africa.com/news/en/issue-no-302/computing/nigeria-ranked-third/en
[29] EU Directive (95/46/EC)
[30] EU Parliament Approves New Cybersecurity Rules, published July 8, 2016 retrieved on August 25, 2016 from http://www.powermag.com/eu-parliament-approves-new-cybersecurity-rules
[31] Africa increases cybersecurity efforts published on June 21, 2013, retrieved on August 25, 2016 from http://www.itworld.com/article/2705986/security/africa-increases-cybersecurity-efforts.html
[32] Cyber Crime (Prohibition and Prevention) Act, 2015

to curtail fraud and related activity in connection with computers[33]. Chile in 1993[34], China in 1996[35], Brazil in 2000[36], India in 2000[37], and Australia in 2001[38].

Now that Africa has a cybersecurity Convention, the questions that may confront the Convention are, how effective is the Convention? Has it resolved most, if not all issues arising from cyberattacks and crimes?

The Convention

The Convention was adopted on June 27, 2014 by the 23rd ordinary session of the African Union ("AU") Assembly made up of 54 Member States. The Convention is a demonstration of the AU to establish a legal framework for information in Africa. It is worthy of note, that the main impediment to the expansion of e-commerce in Africa is lack of a continental policy to regulate e-commerce and ensure cybersecurity. The terminus of the Convention therefore, is to protect personal data, regulate e-commerce, and ensure cybersecurity.

Acts that constitutes Offence under the Convention

Offences under the Convention are in 4 categories:

a. Attack on Computer systems;
b. Computerised data breach;
c. Content related offences; and
d. Property offences.

The Convention enjoin AU members to enact laws that criminalise acts that may fall under these categorises.

a. Attack on Computer systems

According to the Convention, an attempt to obtain or obtain unauthorised access to a computer is an offence.[39] Exceeding authorised access to a computer is also an offence. Also constituting an offence is an attempt to obtain or obtain unauthorised access to a computer with intent to commit another offence or facilitate the commission of an offence[40]. The Convention neither define "unauthorised access" nor "exceed authorised access".

In the same vein, it is an offence to hinder, distort or attempt to hinder or distort the function of a computer system.[41] The Convention did not criminalise conspiracy to hinder or distort the functions of a computer system.

An attempt to enter or entering of "data fraudulently" in a computer system is regarded as an offence. This pertains to entry of data on a computer without consent, which is the same as entry of data

[33] 18 U.S.C. § 1030. This was the first major law to regulate computer related activities in the US. There are other Federal and State Laws which have been enacted to further regulate the use of Computer and internet.
[34] Law on Automated Data Processing Crimes no. 19.223, published June 7, 1993
[35] Regulations on Safeguarding Computer Information Systems, February 1996
[36] Law No. 9,983 of July 7, 2000, insertion of fake data into systems of information Article 313-A
[37] Information Technology Act, 2000
[38] Cybercrime Act 2001
[39] Article 29(1)(a) of the Convention
[40] Article 29(1)(b) of the Convention
[41] Article 29(1)(d) of the Convention

without authorised access. Thus covered under Article 29(1) (a) of the Convention. Of importance is an attempt to enter or entry of "fraudulent data" on a computer system. Bizarrely, the Convention criminalised the entry of "data fraudulently" without criminalising entry of "fraudulent data". The implication is that fraudulent data may be entered on a computer so long as the holder of the fraudulent data has authorised access to a computer. But a counter-argument here is that, the Convention criminalise continuous act of fraud or attempt to remain fraudulent in part or all of a computer system[42].

Similarly, it is an offence to damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change Computer data fraudulently[43].

b. Computerised Data Breach

Under the Convention, acts that would constitute computer data breach include:

i. The interception or attempt to intercept computerised data fraudulently by technical means during non-public transmission to, from or within a computer system[44];
ii. The alteration or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.[45] An intention to defraud may be required before criminal liability attaches;
iii. To knowingly use data obtained fraudulently from a computer system[46];
iv. To fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system[47];
v. Negligence in the processing of data without complying with the preliminary formalities for the processing[48]; and
vi. Participating in an association formed or in an agreement established with a view to preparing or committing any of the offences under the Convention[49].

c. Content related Offences

Under this category, any act in respect of child pornography is regarded as an offence.[50]

Promoting racism or xenophobic through a computer system constitute an offence[51]. Any threat or attack of a person through a computer system due to race, colour, descent, national or ethnic origin or religion is an offence[52].

More so, deliberately denying, approving or justifying acts of genocide or crimes against humanity through a computer system is an offence[53].

[42] Article 29(1)(c) of the Convention
[43] Article 29(1)(f) of the Convention
[44] Article 29(2)(a) of the Convention
[45] Article 29(2)(b) of the Convention
[46] Article 29(2)(c) of the Convention
[47] Article 29(2)(d) of the Convention
[48] Article 29(2)(e) of the Convention
[49] Article 29(2)(f) of the Convention
[50] Article 29(3)(1)(a)–(d) of the Convention
[51] Article 29(3)(1)(e) of the Convention
[52] Article 29(3)(1)(f)-(g) of the Convention
[53] Article 29(3)(1)(h) of the Convention

d. Property Offences

The Convention require Member States to take necessary legislative measures to criminalise the violation of property such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds and blackmail involving computer data.[54]

In addition, the Convention criminalise the use of computer systems for terrorism and money laundering[55].

It is noteworthy, that the AU realised that Member States would need to amend their criminal laws in order to give effect to these offences. Thus, Member States are urged to amend their criminal laws to include "by means of digital electronic communication"[56]. The purpose of this inclusion is to ensure that the substantive criminal law of the Member States reflect the use of computer and other electronic devices for the commission of a crime is an offence.

To add more, the Convention require member States to enact laws that would restrict access to protected systems classified as critical National defence infrastructure due to the critical National security data they contain[57].

Liability for Offences

Under the Convention, any party including State, Local Communities, Public Institutions, Natural Persons, and Companies may be liable held liable for cybercrime.[58]

Sanctions for Offences

The Convention enjoin Member States to legislate on the punishment that would be proportionate to the cybercrime committed[59]. However, the Convention has recommended some sanctions, which are:

i. Fines[60];
ii. Injunction[61]; and
iii. Confiscation[62].

Admissibility of Digital Evidence[63]

The Convention enjoin Member States to legislate on the admissibility of digital evidence for the purpose of establishing offenses under their National criminal law. In admitting the digital evidence, the Convention require that it must have been tendered before the Court, originated from an identifiable person, made out and retained in a manner capable of assuring its integrity.

[54] Article 30 (1)(a)-(b) of the Convention
[55] Article 30 (1)(b) of the Convention
[56] Article 30 (1)(c) of the Convention
[57] Article 30 (1)(d) of the Convention
[58] Article 30 (2) of the Convention
[59] Article 31 (1)(a)-(b)of the Convention
[60] Article 31 (1)(c) of the Convention
[61] Article 31(3)(d) of the Convention
[62] Article 29(3)(2) of the Convention
[63] Article 29(4) of the Convention

Conclusion

The decision of the AU to recognise, and regulate data protection, e-commerce, and cybersecurity in Africa is laudable. Although the Convention may be imperfect, it is a good start.

The Convention is required to be ratified by at least 15 AU Member States before it would come into force.[64] Surprisingly, only 8 Member States have signed the Convention and it has not been ratified.[65]

It is expected that when the Convention becomes effective, that it would attract more technological investment to Africa, foster e-commerce, secure the cyberspace, gradually mitigate cyberattacks, and punish cybercrimes.

Overall, the Convention is a clear indication that Africa is joining the rest of the World to ensure cybersecurity.

[64] Article 36 of the Convention
[65] The Countries that have signed are; Benin , Chad , Congo, Guinea Bissau, Mauritania , Sierra Leone, Sao Tome & Principe and Zambia.