Nigerian harmonized cyber security bill

This paper talks about the types of cyber-crimes: hacking, data theft, spreading virus ND worms, identity theft, yahoo attack and cyber terrorism; causes and effects of cyber – crime on banking, transaction and reputation; finally It will also look at the measures In place to help reduce cyber- crime stateless. Types of cyber crime Various types of cybercafés have been discussed in the literature and have also been experienced by bankers and other financial institutions.

Notable worldwide cybercafés common in developing countries including Nigeria and Ghana are hacking, data theft, spreading virus or worms, fraud or identity theft, yahoo attack, and cyber terrorism. Hacking Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network. Also, in simple words Hacking is the unauthorized access to a computer system, programs, data and network resources. The term hacker" originally meant a very gifted programmer.

In recent years though, with easier access to multiple systems, it now has negative Implications. Unauthorized disclosure of access code, people's system interference, misuse of device, denial of service and records retention are acts criminality under the Harmonize Cyber Security Bill 2011 of Nigeria. Offenders are punishable by law which may extend to prison terms or with fine. Hacking offence is cognizable, boilable, compoundable with permission of the court before which the prosecution of such offence is pending and terrible by any magistrate.

Unfortunately, unlike Nigeria, there is no law in the statute books in Ghana that address these types of crime. The Police still rely on conventional crime laws on false pretence In the criminal Code Act 29/60 Section 131 and Its associate statutes. Crimes committed under these laws are boilable offences and carry lesser punishments which cannot therefore deter the fraudsters from molting cyber offences.

Data Theft is a rising problem, primarily perpetrated by office workers with access to technology such as desktop computers and handheld devices, capable of storing digital information such as flash drives, pods and even digital cameras. The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. The sections 2 – 18 of the Harmonize Cyber security Bill 2011 of Nigeria criminality the act of data theft and data forgery.

Also the Information Technology (Amendment) Act, 2008, crime of data theft under Section 43 (b) is stated as – If any person without permission of the owner or any other person, who is in charge of a computer, computer system of computer network – downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, then it is data theft.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable ND under Section 379, 405 & 420 of Indian Penal Code, 1860 also applicable. Data theft offence is also cognizable, boilable, compoundable with permission of the court before which the prosecution of such offence is pending and terrible by any magistrate. Spreading virus or worms Worms and viruses can do any amount of harm; the creator anticipates them to do. They can send your data to a third party and then delete your data from your computer.

They can also ruin and mess up your system and render it unusable without a re-installation of the operating system. Most have not done this much image in the past, but could easily do this in the future. Usually the virus will install files on your system and then will change your system so that virus program is run every time you start your system. It will then attempt to replicate itself by sending itself to other potential victims. Under the Harmonize Cyber Security Bill 201 loft Nigeria Section 2 – 18, it makes it unlawful for a person to have unlawful access to another person's computer and system interference .

Also under Information Technology (Amendment) Act of India, 2008, Section 43(c) & 43(e) with Section 66 is applicable and under Section 268 of Indian Penal Code, 1860 also applicable. Spreading of virus offence is equally, like data theft, cognizable, boilable, compoundable with permission of the court before which the prosecution of such offence is pending and terrible by any magistrate. Fraud – identity theft Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone.

For instance, making a false bank weapon to retrieve information of account of someone constitute an identity theft. This is known as saw in Ghana (Boating et al. , 2011). The concept is simple; someone gains access to your personal information and uses it for his own benefit. This could range getting access to ATM and using such people can make themselves a lot of money with personal information. In Nigeria people design web links forms requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes (Hosannas, 2011).

The Nigeria Harmonize Cyber Security Bill of 2011 Section 2 – 18 criminals computer – related offenders which include identity theft and unlawful access to a personals computer. According to the Information Technology (Amendment) Act of India of 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft. Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else is fraudulent.

According to the Identity Theft Resource Center (DIRT), identity theft complaints ranked first in 2012 in the Federal Trade Commission’s (FTC) list of complaints, with a 32 percent increase over 2011. Identity theft has been the Fat’s No. 1 complaint for 13 consecutive years. A Javelin Strategy & Research survey shows an increase of 13 percent in 2011 compared with 2010, and a total of 1 1. 6 million victims in the United states 201 leaven , 2012). Identity theft is not an industry specific crime. It can appear in any industry where personal information is used to gain credit or acquire customers.

In years past, this type of crime was not prevalent, but the influx of technology has caused it to grow at a rapid pace and become a significant issue in the public eye, as its insidious nature owes real trauma to consumers. Statistics reflect its growth; with estimates of 500, 000 to 700, 000 victims of identity theft in 2000. The growth of identity theft has reached epidemic proportions, and is quickly becoming the crime of the new millennium. The cost of investigating identity theft cases in 1997 was reported to be $745 million (National fraud center, 2010).

The National Fraud Center conservatively estimates to be $50 billion a year, has prompted “ Travelers Property Casualty Corp.. To launch the first-ever insurance coverage for victims of identity theft. The coverage offers policyholders as much as $1 5, 000 to cover expenses incurred in clearing their name. ” Identity theft in e-commerce transactions is estimated at 11% of total transactions. (National fraud center, 2010) Yahoo attack Yahoo attack popularly called 419 is a criminal offence under section 419 of the Nigerian criminal code has a law against such offenders.

It is characterized by using e-mail addresses obtained from the Internet access points using e-mail address harvesting applications (web spiders or e-mail extractor). These tools can automatically retrieve e-mail addresses from web pages. Nigerian fraud letters Join the warning of impersonation scam with a variation of an advance fee technique in which an e-mail from Nigeria offers the recipient the chance to share a percentage of trying to tap out of the country (Brenner, 2010).

Cyber terrorism A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Parker

(1983) defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. It means that any act intended to inculcate fear by accessing and altering any useful information in organizations or Government bodies using Computer and Internet is generally referred to as Cyber Terrorism.

Another form of cyber terrorism is cyber extortion is a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their services (Hosannas et al. , 2011) Factors that promote cybercafés Like any criminal act or intent, the advent of cybercafés hinges or are underpinned by a number of factors.

One can fundamentally use normalization theories to explain the factors. Other poverty theories are also relevant in the discussion of crimes in general and cybercafés in specific (Bradshaw, 2006). For the purposes of this discussion, the following factors are raised: arbitration, unemployment, and weak legislative regime. Arbitration Arbitration is one of the causes of Cyber-crime in Nigeria and Ghana; it is the massive movement of people from rural settlement to Cites. Arbitration may be referred to the increasing number of people in the urban areas.

It is predominantly results in the physical growth of urban area be it horizontal or vertical. This result in a heavy competition amongst the growing populace more especially the elites, as such the elites find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest and they are popularly called IMHO Boys" (Meek , 2012). Arbitration is one of the major causes of cyber-crime in Nigeria and Arbitration will be beneficial if and only if good Jobs can be created in the cities where population growth is increasing, arbitration without crime is really impossible.

As such the elites amongst them find it lucrative to invest in the cybercafé because it is a business that requires less capital. Unemployment Cybercafé can be associated with high rate of unemployment, harsh economic must also survive and this has led to cyber-crime. The population growth rate in Ghana and Nigeria that not correspond to the employment levels of the country. Unemployment has brought a great gab between the rich and the poor and as such many strive to level up using the quickest means possible, since for any business to hire well, the rate of return in the investment must be growing at a geometric rate with a minimal risk.

Most cyber criminals require less investment and a favorable environment. Nigeria is such an environment and many cyber criminals take advantage of that. Weak Implementation of Cyber Crime Laws and Inadequate Equipped Law Agencies The Ghanaian and Nigerian legislation must implement harsh laws regarding cyber criminals and when criminal offences occur, culprits must be punished for the crime they've committed because cyber-crimes reduces the nation's competitive edge, allure to prosecute, cyber criminals, can take lead of the weak gaps in the existing punishing proceedings.

Weak ‘ fragile laws regarding cyber criminals exist both in Ghana and Nigeria, unlike how criminals such as armed robbers are treated with maximum penalties. Unfortunate these nations are not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012) state that “ African countries have been criticized for dealing inadequately with cybercafé as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence ND infrastructure, and the private sector is also lagging behind in curbing cybercafé” Nigeria is not an exception to this rule.

Furthermore, It is therefore paramount that the nation’s legislation should ensure proper implementation of their laws against cyber-crime. Effects of cybercafé The cost of cybercafé can be difficult to account for. This is because there are direct and indirect costs associated with the phenomenon and the effects are both quantitative and qualitative.

Notwithstanding, the effects of cybercafé on banks, financial institutions and any other organization and a country are not only enormous UT some difficult to address especially those that touch on the goodwill and image of the organization or nation. The following are the effects of cybercafé discussed. Reduces the competitive advantage Computer crimes over the years have cost a lot of chaos to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage.

Owed to cyber-crime, there has being loss of billions of dollars annually globally speaking, such crimes may threaten a nation’s security and financial health, a company can suffers losses due to computer crime when a hacker steals information to a competitor company; this will automatically reduce the competitive strength of the company. Time wastage and slows financial growth Wastage of time is another problem because many IT personals may spend a lot of time on handling, resolving harmful incidents which may be triggered by computer criminals.

The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enter in an organization and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contains confidential information like credit cards of customers and as the information is stolen the customer will not trust the company again and will move to someone else who could protect their confidential information. (Hosannas et al. 2011). Slows production time and add to over head cost Computer crime reduces the productivity of a company, as a company will take measure to reduce cybercafé, by entering more password or other acts this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and mallard companies must buy strong security software to educe the chances of attacks from such attacks, and change them from time to time to help fight against cyber criminals.

Defamation of reputation Companies suffer reputation damaged and abridged valuation after public reporting of their being hacked, usually in the form of a drop in stock prices and loss of confidence by customers. These losses can be significant ranging from 1% to 5%, but appear not to be permanent. Stock prices usually recover by the next quarter. It would alter any calculation of loss to attempt to include these oscillations in stock prices.

However, it will be interesting to see if these changes as a result of new SEC regulations that require companies to report major hacking incidents, which may increase shareholder understanding about what hacks are commercially material. Shareholders are doubtful to have blameless information about what was taken, let alone by whom and for whose profit.

Recovery of stock prices may not be so quick if investors decide that there has been significant damage to a company’s intellectual property portfolio or if it sees a significant outflow of customers as a result (Center for Strategic and International Studies, 2013). Measures put in place Financial institutions and banks in general have confronted the issue of cybercafé. Although not totally successful, some efforts have been put in place and some gains have been recorded.

The efforts include internet banking, fraud preventive systems and use of automated teller machines (Atoms). Usual fraud detection systems have focused on determining which online customer requests are typical or unexpected. The deterrence of fraud requires banks to develop or enhance visibility to improve awareness of the criminal enterprise and its processes to their customers. This level of placing individual transactions or requests in a broader context in order to protect them from fraudsters is sometimes referred to as ; situational awareness. To achieve better situational awareness, banks are improving customer visibility across lines of business, enhancing coordination between channels, applying more rigorous technologies for identification as well as tracking hostile devices and using more sophisticated link analysis tools that search for connections between seemingly disparate events The prevalence of Distributed Denial of Service (Dodos) attacks is such that all online organizations are now having or planning to have defense mechanisms in place.

As a result, they are also working with their ISP (Internet Service Providers) or hosting service providers to understand what mitigation services they offer in order to adapt the most apposite technological strategies to track all forms of fraudulent acts allied with internet banking. As some banks are even more critical to have solutions in place to protect their own applications rather than relying on the consumer to keep their device free from mallard, the customers’ education is not left out.

Beyond taxation, a number of banks in particular are implementing solutions that are compliant with government regulations and provide visibility into the actual crimes that are being perpetrated against their customers’ accounts across their enterprises to avoid being preoccupied by any form of attack. It is common for fraudsters to access a group of accounts, perform reconnaissance and money movement activities and then immediately launch a Distributed Denial of Service (Dodos) attack in order to create a diversion.

This has prompted a number of banks to implement security layers beyond authentication systems to recognize gouge device activity within compromised accounts within their wide range of internet banking operations. However, some banks are still in the process of deciding what security measures they are prepared to invest in and what trade-offs they are prepared to make when it comes to computer crimes.

The specific protection measures deliberated for institution by the banks include hardware identification, access controls software and disconnecting critical bank applications but much caution must be taken because computers don’t commit crimes; people do. The perpetrator’s best advantage is inorganic on the part of those protecting the system though proper internal controls reduce the opportunity for fraud (Oilcan’s, 2011).

Apart from banking institutions, governments are gradually realizing the need for such protective measures particularly at the national level and thereby passing legislation relating to computer crime of which internet banking is not omitted. Again, financial institutions are gradually sensitizes the general public about their crime 2011).

Currently, a number of banks are able to detect usage of the compromised data by recognizing when a rogue device is attempting to gain access to an account, r if a group of rogue devices are acting across multiple accounts and this will be a very powerful tool if all banks are able to take such initiative. It will save both the bank and their customers from incurring losses (Oilcan’s, 2011).

Fraud preventive systems Fraud as a major strategy in cybercafé operations can be overcome through diverse measures already instituted some of which are initiated by governments, organizations as well as individuals. For consumers or service beneficiaries, vigilance is much esteemed in combating fraud of all forms on the internet especially in the months subsequent to an incident such as attackers attempt to use social engineering or pushing to dupe innocent victims into revealing sensitive data that can be used to open new accounts or take over existing ones (Britton, 2013).

Such attacks therefore serve as a reminder which has recently prompted regular change of passwords for online accounts and to never use the same passwords across accounts for numerous transactions. As a result a number of firms offer intermittent education to their customers on the need to consistently change their passwords in order to reduce their propensity of falling prey to fraudsters on the internet this is because using a single password across institutions could magnify the impact of a breach across other financial institutions, commerce sites and social networks.

Owing to this and other forms of fraud, a number of financial institutions have devised measures in place to check: observe and mitigate mallard, detect an infected victim’s device and work with their customers to clean the machine. This is a practice which some banks do proactively today and with time all other financial institutions will follow suit.

A robust fraud prevention environment is gradually underway and is focusing on owe to provide visibility into all aspects of the fraud enterprise such as; money mules and other cashing-out services, a maturation and standardization of software ; building blocks” that can be assembled to create specialized fraud campaigns, stolen credentials and descriptive narratives about victims that are packaged in a standardized format that can be rented by-the-hour and even offered as ; fraud-as-a- service” Currently mass education is embarked on by a number of organizations to their customers and seeks to emphasize on why customers should not open emails from unknown sources, not providing personal information over the phone, acknowledgement of the risks which may be involved by clicking on links in emails, changing passwords on a regular basis and avoiding using the same password across multiple accounts.

Furthermore, organizations are gradually enhancing their visibility and awareness of Risk Assessment (recognize compromised or aggressive devices), Account-Centric Awareness (detect and correlate events within an account, especially ones that involve account maintenance requests), Cross-Channel Awareness (correlate events across channels and lines of business) and Big Data Analytics (find patterns in the sieve amounts of operational data collected throughout the business). As networked or internet enabled devices become ubiquitous, and a significant number of government departments provide some or all of their services via the internet, there is a responsibility upon governments as well to provide leadership in responding to cyber crime at a policy level.

The Home Department of United Kingdom in 2010 declared that they believe they can and should enhance the fight against cyber crime at government level by ensuring an integrated response and in line with the strategic objectives laid out in the I-J Cyber Security Strategy. This quest led to the establishment of the Office of Cyber Security within the Cabinet Office to provide coordination of the overall response to threats from the internet. The Office of Cyber Security is the strategic lead for a broad programmer of work to secure the Auk’s advantage in cyber space. The global community is increasing considering measures to create a hostile environment for cyber criminals.

Among the number of provisions made in this regard include provision of an effective law enforcement and criminal Justice response, through peccaries units, and ensure that intelligence is shared where appropriate; developing, over time, a clear understanding of the scale and scope of cyber crime, including robust and easily accessible reporting systems for both the public and business, which will be monitored for trends; producing a regular strategic overview of the threat to children and young people from those who use technology to harm and abuse them; developing tools, tactics and technology, working with the internet industry, to ensure that law enforcement are able to detect, investigate and pursue inline criminals even when the technology changes. Automated Teller Machine (ATM) Technological advancement which has obliquely groomed criminal acts such as cybercafé pose a challenge to the global community about how to mitigate the ever increasing rate of cybercafé specifically in the areas of ATM usage, Internet banking and fraud. This aspects turn out to be some of the key areas cybercafé dominates in the global community. Since technological advancement has recently created a situation where all online and mobile interactions are ; machine-to-machine" (the user's device interacting with he banks server), cyber interactions naturally lend themselves to computerizing.

Once a fraudster secures the credentials required to access a victim's accounts, a process can be built in which multiple accounts are accessed automatically. For example, this can be done to check the balance or credit lines of accounts to identify which to target for attack. Electronic communication facilitates the ability to break the fraud process down to discrete steps which can then be carried out by different the standardization of fraud software building blocks and data formats, which make t easier to collaborate and exchange information between fraud rings. Conclusion Cyber-crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.

The main types of cyber-crime include; Hacking, Data Theft, Spreading Virus or Worms, Fraud – Identity Theft, Cyber Terrorism, Yahoo Attack. The causes of cyber-crime comprise arbitration, Unemployment, Weak Implementation of Cyber Crime Laws and Inadequate Equipped Law Agencies. Reducing the competitive advantage of organization, Time Wastage and Slows Financial Growth, Slows Production Time and Additional Overhead Cost, Defamation of Reputation: Companies, especially, banks suffer reputation damaged and abridged valuation when the public get to know that their system is being hacked, usually in the form of a drop in stock prices and loss of confidence by customers are some of the effects that come along with cyber-crime.