Assessing Cyber crime and its Impact on E-Banking In Nigeria Using Social Theories

F. Wada  
Nelson Mandela School of Public Policy  
Southern University  
Baton Rouge, USA  
friwada@yahoo.com

G.O. Odulaja  
Department of Computer Science  
Tai Solarin University of Education  
Ijagun-Ijebu Ode, Nigeria  
goddyseyi@yahoo.com

ABSTRACT
The information communication technology (ICT) revolution has had impacts in almost every area of human endeavor. From business, industry, government to not-for-profit organizations, ICT has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, ICT has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and other related cyber crimes. This study sought to assess cyber crime and its impact on the banking institutions in Nigeria. It also examined the existing policy framework and assessed the success of the institutional countermeasures in combating cyber crime in the banking industry. This papers X-rays cybercrime policy issues and provide insight into how cybercrime impacts on E-banking from a Nigerian perspective. Social theories were then used to explain causation with a view of guiding policy makers on behavioural issues that should be considered when formulating policies to address cyber criminal activities in Nigeria.

Keywords: E-banking, Nigeria, policy, social theories, frauds, banking.

1. INTRODUCTION
There are few innovations that have changed the dynamics of banking as much as the e-banking revolution. Throughout the world, banks are reorganizing their business strategies to take advantage of new business opportunities offered by e-banking. Electronic banking is believed to have started in the early 1980s [68].

It has since then been growing in an unprecedented dimension in line with the growth in ICT development. E-banking has enabled banks to overcome borders, adopt strategic outlook, and bring in new possibilities. According to Nitsure 55], information communication technology has reduced the cost of processing and facilitating the transmission of information leading to drastic changes in the banking business. It is worth noting that e-banking has not been limited to advanced countries, but is found even in countries with underdeveloped e-banking systems, as a result of the many new business opportunities offered by e-banking.

1. INTRODUCTION
There are few innovations that have changed the dynamics of banking as much as the e-banking revolution. Throughout the world, banks are reorganizing their business strategies to take advantage of new business opportunities offered by e-banking. Electronic banking is believed to have started in the early 1980s [68].

It has since then been growing in an unprecedented dimension in line with the growth in ICT development. E-banking has enabled banks to overcome borders, adopt strategic outlook, and bring in new possibilities. According to Nitsure 55], information communication technology has reduced the cost of processing and facilitating the transmission of information leading to drastic changes in the banking business. It is worth noting that e-banking has not been limited to advanced countries, but is found even in countries with underdeveloped e-banking systems, as a result of the many new business opportunities offered by e-banking.
Although no official definition of e-banking has been established, it generally implies a service that allows customers to use some form of computer to access account-specific information and possibly conduct transactions from a remote location like home or workplace. Additionally, e-banking has obvious advantages to the customer in terms of convenience where customers conduct routine banking transactions from the comfort and security of any location from which they wish to transact [43]. The emerging concept of e-banking has drawn the attention of the business fraternity as well as of scholars and researchers to the effects of such dynamics on the banking industry. For instance, Liao and Wong [43] in their study of the determinants of customer interactions with Internet-enabled e-banking found that factors such as perceived usefulness, ease of use, security, convenience, and responsiveness to service requests to be a strong measure of the variation in customer interactions. Based on this finding, they suggested that stringent security control is critical to e-banking operations. Such arguments do not only have managerial implications for enhancing Internet banking operations and developing viable electronic banking services, but also form the basis upon which this study is based.

Anguelov et al. [4] hold the same view which suggests that consumer acceptance and use of e-banking technologies are related to the characteristics of both the individual consumer and the specific technology. They further argued that acceptance of such technology is linked to a consumer’s socioeconomic, technological, and personal characteristics and preferences. Key investments in e-banking can be traced back to the early 1980s, when the home computer was still rare [70]. Since then, major innovations in electronically-enabled bank service delivery like automatic teller machines, touch-tone telephone banking, voice response units, and centralized technology-intensive telephone call centers have emerged. In 2000, for instance, e-banking was utilized by approximately 10% of all retail banking customers in the United States [51]. According to an August 2009 survey of U.S. consumers by the American Bankers Association (ABA), Internet banking now ranks first among the methods of banking.

Evidence from the existing literature indicates that many customers have adopted the electronic banking services. ATM, for instance, has turned out to be the most popular service delivery channel [18]. It is estimated that the world is now home to 1.65 million ATM’s and that number was expected to grow by 1.7 million by 2009 and beyond. Although the USA and other parts of the developed world were the first to experience ATM proliferation, the trend subsequently has stretched to other developing countries [34]. Banks in Malaysia, for instance, have introduced automated teller machines (ATMs) in order to ease the constraints on banking as far as time and geographica llocation are concerned.

E-banking technology created a revolution by extending banking hours beyond office hours and beyond national boundaries (Balachandran & Balachandher, 2000). In Nigeria, several studies on e-banking have been done. Chiemke, Evwickpaefe, & Chete [19], for instance, conducted a pragmatic study on adoption of e-banking where major hindering factors to Internet banking adoption such as insecurity and inadequate operational facilities, including telecommunications facilities and electricity supply, were identified.

In another study on Nigeria, it was revealed that e-banking is still at the infant level in the country with most of the banks having mainly information sites and providing little Internet transactional services. However, most studies in these areas revealed that there has been a very steady move away from cash as transactions are now being automated [2].

While the findings revealed that e-banking is able to enlarge customer relationships, and loyalty and to give banks a competitive advantage as far as market share is concerned, the problems of ineffectiveness of telecommunications services, supply of power, high cost, fear of fraudulent practices, and lack of facilities necessary for their operation still remain. Despite this, ongoing research on the impact of e-banking is inconclusive, especially in developing economies, and serves as an open ground for more research in the area of e-banking.
2. E-BANKING CRIMES

Crime and corruption represent a major concern for business executives not only in Nigeria but also in other parts of Africa. In Nigeria, for instance, the most serious impediments to economic activities and business are crime and corruption which averages 75% and 71% respectively. Theft and fraud are the second most popular crimes after burglary [28][29]. By definition, cyber crime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cyber crime is believed to have started in the 1960’s in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s. The 1980s witnessed the introduction of viruses 56]. The fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space. Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes. With e-banking gaining ground in Nigeria and other parts of SSA, customers and online buyers are facing great risk of unknowingly passing on their information to fraudsters. "Hackers" get information of those who have made purchases through websites and then make fake cards, which they use with less detection. Absence of a law specifically dealing with card-related crimes in Nigeria may be giving thieves a loophole to operate freely. Police treat card-related crimes like any other case of fraud.

2.1 Types of Cyber Crime
This study presents the types of cyber crimes that have economic impact either directly or indirectly on the financial system of a nation or having cross border ripple effects. Longe & Chiemeke (2008) simplified the list of unintended consequences of ICT to include acts such as Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy -cat websites. While some types of cyber crimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries.

2.1.1 PHISHING
According to Roger [62], phishing is simply a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Phishing is usually a social engineering crime pervasive in attacking organisations’ or individuals’ (customers’) information systems (IS) in order to gather private information to be used against organisations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts (Rodger, 2008). According to recent estimates from the Anti-Phishing Working group [6,7], phishing scams remain a relatively small percentage of spam sent worldwide today. Phishing attempts to pose significant dangers for unsuspecting victims. It has become one of the fastest-growing worldwide threats on the Internet. This rapid growth has made combating it a huge priority for electronic mail service providers, since phishing impacts every aspect of the Internet and computing and there is no single action from any one company or organization to solve the problem. The remedy can only come in a holistic fashion involving collaboration between technology innovation, industry, government, and user education as prescriptive guidance.

To build systems shielding users from fraudulent websites, designers need to know which attack strategies work and why. What makes a web site credible? This question has been addressed extensively by researchers in computer-human interaction. Successful phishing must not only present a high credibility web presence to its victims; it must create a presence that is so impressive that it causes the victim to fail to recognize security measures installed in web browsers [61]. Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites [45]. About two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 2003 [44].

If we hope to design web browsers, websites, and other tools to shield users from such attacks, we need to understand which attack strategies are successful and what proportion of users they fool. In an analysis of phishing attacks carried out in 2006, Rachna, Tygar, & Hearst [61] found that good phishing websites fooled 90% of participants. Existing anti-phishing browsing clues are ineffective and 23% of participants in the study did not look at the address bar, status bar, or the security indicators.
Perpetrators target both document categories to secure personal identifying information. Often they obtain a ‘set’ of point of information documents in order to present themselves as ‘legitimate customers’ to deceive the target organisation’s authentication and verification processes to commit identity fraud [41]. Increasingly, the mode of attack for the fraud, especially the identity fraud perpetrator, is tending to rely on electronic commerce or mechanical/digital devices to initiate the identity theft or identity deception act. This is to some extent enabled by Internet adoption. For example, 77% of United States (US) adults were online in May 2006, up from 74% in 2005, 66% in 2002, 64% in 2001, and 57% in 2000, according to e-Marketer [31].

In phishing e-mail messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters “spoof,” or mimic, a reputable company. The companies spoofed most often are financial services- Internet organizations such as the Bank of America, Citibank, eBay, PayPal, etc. Retailers and Internet service providers are also targeted [7,8, 44].

These phishing e-mails are usually mass mailed (Warner, 2004). Many of the recipients are not customers of the spoofed companies and may quickly realize that the e-mail is fraudulent, or may believe that the e-mail was mistakenly sent to them and ignore the e-mail. Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam. According to Longe, Mbarika, Korouma, Wada, & Isabalija [49], the scammers claim to be from reputable companies and go to great lengths to emulate the company’s visible branding.

Their fraudulent e-mails often contain the company’s logo and use similar fonts and color schemes as those used on the company’s web site. Some of the fraudulent e-mails simply reference images from the legitimate company’s site. The main link in a fraudulent e-mail sends the recipient to the fraudulent phishing web site, but many fraudulent e-mails include other links that send the recipient to sections of the real company’s web site.

To further convince the recipient that the e-mail originated from the reputable company, the scammers use a “from” e-mail address that appears to be from the company by using the company’s domain name (e.g., @ebay.com, @paypal.com) [49]. Phishing e-mails also try to assure the recipient that the transaction is secure in hopes of gaining the recipient’s trust. The following are assurances that were included in fraudulent e-mails:

“Remember: eBay will not ask you for sensitive personal information (such as your password, credit card, bank account numbers, social security number, etc.) in an e-mail.”

This e-mail then sends users to a fraudulent web site that asks for personal and account information while promising that the information is submitted via a secure server. The phishing perpetrators could then notify the victim of a “security threat.” Such a message may be welcomed or expected by the victim, who would then be easily induced into disclosing personal information [37]. The number of unique phishing websites detected by APWG during the second half of 2008 saw a constant increase from July to October with a high of 27,739 [7,8]).

In Nigeria, the most recent phishing attacks were on the customers of Inter-switch, which remains the organization with the highest customer base in electronic transactions. The Nigeria Deposit Insurance Corporation (NDIC) disclosed in its 2007 annual report and statement of account that underhand deals by bank staff, among others, resulted in attempted fraud cases totalling over N10.01 billion (over 65 million USD) and actual losses of N2.76 billion (13 million USD) in 2007 [3].

With the present situation in the world economy and the appropriate technology, fraudulent action is most likely to increase and phishing remains one of the main means of performing “fraud without borders.” The extent of readiness to stem phishing in Nigeria needs to be determined because fraudulent activities emanating from these nations have far-reaching consequences beyond her borders.
2.1.2 Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any “premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents” [67].

Unlike a nuisance virus or computer attack that result in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Apart from that, there is another dimension to cyber terrorism - the use of cyber infrastructure to launder money for financing physical terrorism. In 2005, FBI officials reported that Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases [73].

According to Wilson (2008), cyber terrorism is said to have taken place when the effects of a widespread computer network attack is unpredictable and might cause enough economic disruption, fear, and civilian deaths, to qualify as terrorism. At least two views exist for defining the term cyber terrorism [20, 27]. These are (1) Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals. (2) Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.

The terrorist’s use of the Internet and other telecommunications devices is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. Tighter physical and border security may also encourage terrorists and extremists to try to use other types of weapons to attack the United States. Persistent Internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations.

They will also probably consider attempting a cyber attack against the U.S. critical infrastructure [47]. Cybercrime has increased dramatically in past years, and several recent terrorists events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs [27]. These links with hackers and cybercriminals may be examples of the terrorists’ desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

2.1.3 Electronic Spam Mails

These are unsolicited bulk e-mail to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, web search engines, and blogs. Spamming is popular because the advertisers have no operating costs beyond the management of their mailing lists and it is difficult to hold senders accountable for their mass mailings. As a result, costs such as lost productivity and fraud are borne by the public and by Internet service providers that have been forced to add extra capacity to cope with the deluge [48].

A good example is 419 mails or the Nigerian advance fee frauds which in 1996 was estimated to have cost unsuspecting clientele over five billion dollars [70]. These mails emanate in a triangle called the “The Nigerian Connection” mostly in Europe and in some parts of Africa, “The 419 Coalition, 2005.” The Nigerian Scam, according to published reports, is the third to fifth largest industry in Nigeria [79].

It is the 419 Coalition view that, in effect, the elites from which successive governments of Nigeria have been drawn are the scammers. Therefore, victims have little recourse in this matter. Monies stolen by 419 operations are almost never recovered from Nigeria. Most 419 letters and e-mails originate from or are traceable back to Nigeria. However, some originate from other nations, mostly also West African nations such as Ghana, Cameroon, Togo, Liberia, Sierra Leone, Ivory Coast (Cote D’Ivoire), etc.
The effects of such scams have immense effects with confirmed losses of millions of dollars annually (Herald Tribune, 2007). According to Longe and Longe [46], governments have tried to come up with policies to try to curtail this menace. Nigeria, through the EFCC, banned night browsing. This is because most fraudulent activities are perpetrated at cyber cafés at nights. For now, there are no quantitative data to measure the effect of this action on the reduction or otherwise of cybercrime in Nigeria. Apart from the availability and usage of Internet facilities in cyber cafés for pornography and other cybercrimes, the evolution of fixed wireless facilities in Nigeria, for instance, has added another dimension to the cybercrime problem. Nigeria therefore enjoys a dubious distinction of being the source of what is now generally referred to as ‘419’ mails, named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud.

These crimes are similar to theft and the likes that have existed for centuries offline even before the development of high-tech equipment. Progress in the fight against Internet pornography has been moving at a very slow pace in Africa. A majority of public internet access point deals with the problem in unorthodox manners such as placing notices on cyber cafe walls warning against browsing pornographic sites and other spamming activities. Those with some technical expertise resort to the use of content filters which are downloaded and installed to filter unwanted Internet content [46].

2.1.4 Cyber Stalking

Stalking in the physical sense generally involves harassing or threatening behavior in which an individual engages repeatedly, such as following a person, appearing at a person’s home or place of business, making harassing telephone calls, leaving written messages or objects, or vandalizing a person’s property. According to Ellison and Akdeniz [30] cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. This term is used interchangeably with online harassment and online abuse. A cyber stalker does not present a direct physical threat to a victim, but follows the victim’s online activity to gather information and make threats or other forms of verbal intimidation.

The anonymity of online interaction, they argued, reduces the chance of identification and makes cyber stalking more common than physical stalking. Although cyber stalking might seem relatively harmless, it can cause victims psychological and emotional harm, and occasionally leads to actual stalking. Cyber stalking is becoming a common tactic in racism and other expressions of hate. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing website (e.g., blogs) and e-mail. The availability of free e-mail and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment [30].

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim’s immediate family; and still others require only that the alleged stalker’s course of conduct constitute an implied threat [74]. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously. The nature and extent of the cyber stalking problem is difficult to quantify. Indeed, current trends and evidence suggest that cyber stalking is a serious problem that will grow in scope and complexity as more people take advantage of the internet and other telecommunications technologies [17].

Important advances can only be made if industry, law enforcement, victims, service providers, support groups, and others work together to develop a more comprehensive and effective response to this problem. Ultimately, however, the first line of defense will involve industry efforts that educate and empower individuals to protect themselves against cyber stalking and other online threats, along with prompt reporting to law enforcement agencies trained and equipped to respond to cyber stalking.

Physical stalking, online harassment, and threats may be a prelude to more serious behavior, including physical violence. For example, the first U.S. cyber stalking law went into effect in 1999 in California. Other states include prohibition against cyber stalking in their harassment or stalking legislation. In Florida, HB 479 was introduced in 2003 to ban cyber stalking. This was signed into law in October 2003.
The crime of cyber stalking is defined in Florida Statutes 784.048(1) (d) which is one of the strictest such laws in the United States [69].

2.1.5 Fake Copy-Cat Web Sites
One recent trend in on-line fraud is the emergence of fake ‘copy-cat’ web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster’s personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud [78].

3. EFFECTS OF CYBER CRIME ON BANKING

According to Reuter’s media briefs from Cameroon [16], British prime minister, cyber crime costs the British economy some 27 billion pounds a year. On the other hand, the Economic and Financial Crimes Commission Report [28, 29] ranks Nigeria as third among the top ten sources of cyber crime in the world. It is estimated that after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent, Nigeria is the next hub of cyber criminals in the world with 8 per cent. The growth of online banking further presents enhanced opportunities for perpetrators of cyber crime. Funds can be embezzled using wire transfer or account takeover. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems [8]. Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions.

Therefore unless crime detection and prevention are confronted collectively, Nigeria like any other country will remain warm breeding grounds for cartels of such criminal activity. A global effort to combat this crime is of essence. Financial fraud is one of America’s largest growth industries, creating annual losses of $189 billion [39, 49]. The cost of application fraud alone, they argued, is more than $35 billion a year.

This is by far more damaging than delinquent or bankrupt accounts, fraud losses which are generally three times higher than normal charge-off rates. This situation poses a real and constant threat to profitability and may raise the price of goods and services for consumers. They further argued that by far, the greatest threats is from e-commerce fraud, identity theft and international criminal organizations, all of which are becoming more widespread and sophisticated every day.

As e-commerce continues to grow, it will become an even bigger attraction for criminals. The report indicated that identity theft is escalating at 40% a year and is particularly problematic compared with more traditional forms of financial fraud. Greater access to credit, an abundance of information, faster electronic communications, and intense competition among financial institutions make it easier than ever for perpetrators to steal identities and falsify information. The existence of cyber crime and its effects require the formulation of appropriate policies to address them. The next section presents existing policies on cyber-related crime in Nigeria.

4. CYBER CRIME POLICY IN NIGERIA

There is presently no law that is specific to cyber crime in Nigeria. However, this is not to say that cyber criminals are free to operate in the country. There are general laws that are not specifically related to cyber crime but are being enforced to deal with the crime. Some of these laws are: the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006 [32].

The Nigeria Criminal Code Act 1990
The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber crime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with “obtaining Property by false pretences-Cheating.” The specific provisions relating to cyber crime is section 419, while section 418 gave a definition of what constitutes an offence under the Act.
"Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence."

"Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years."

The Economic and Financial Crime Commission Act, 2004
(Source: National Assembly of Nigeria, 2004)

The Economic and Financial Crime Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provide the legal framework for the establishment of the Commission. Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

- the investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;
- the coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;
- the examination and investigation of all reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;
- undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same;
- Taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation;
- the coordination of all investigating units for existing economic and financial crimes, in Nigeria;
- The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud-Related Offences Act 1995; the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended; the Banks and other Financial Institutions Act 1991, as amended; and Miscellaneous Offences Act (EFCC, 2004).

Advance Fee Fraud and Related Offences Act 2006 (Source: National Assembly of Nigeria, 2006)

According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006): 'False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.' Section 383 sub-section 1 of the Nigerian Criminal Code states: 'A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing.' (Advance Fee Fraud Act, Laws of the Federation of Nigeria, 2006) [1]
Economic crime is defined by the Act as “the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally, either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labor, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods.”

Advance Fee Fraud and Other Fraud Related Offences Act 2006 is currently the only law in Nigeria that deals with internet crime issues, and it only covers the regulation of internet service providers and cybercafés, it does not deal with the broad spectrum of computer misuse and cyber crimes [32]. There are presently six bills on cyber crime being considered by the National Assembly (legislative arm) of Nigeria. These are: the Computer Security and Critical Information Infrastructure Protection Bill 2005 (sponsored by the Executive), the Cyber Security and Data Protection Agency (Establishment, etc.) Bill 2008 (sponsored by Hon. Bassey Etim), the Electronic Fraud Prohibition Bill 2008 (sponsored by Senator Ayo Arise), the Nigeria Computer Security and Protection Agency Bill 2009 (another executive bill), the Computer Misuse Bill 2009 (sponsored by Senator Wilson Ake) and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010, sponsored by Hon. Abubakar Shehu Bunu.

5. THEORETICAL UNDERPINNINGS

This section discusses some theories relating to the electronic media and security issues. Electronic media have been emphasized by various theoretical traditions. Sociologists, for instance, argued that point-to-point communication media— for instance, telephones— support shared aims which demonstrate a powerful collective representation. Some, especially the Marxists, look at communication media as an exploitative tool by the elitist groups for socioeconomic and political control [25]. In their own contribution to the digital communication.

Bell, Garland and Platt [14] argued that the invention of mini-electronic and optical circuits capable of speeding the rate of information flow through networks would have a big impact on society. Despite the positive impact of technology on society, it has on the other hand led to the unintended use in criminal activities like cybercrime. He concluded by saying, it is easier to steal a penny from millions of bank account owners using the internet than using physical robbery.

5.1 Routine Activity Theory

This theory proposes that three situations facilitate the occurrence of crime. Proponents argue that such events must happen at the same time and in the same space. The three situations are the existence of a suitable target, lack of security, and a motivated offender for the crime to occur [22]. The assessment of the situation determines whether or not a crime takes place.

5.2 Opportunity Theory

This theory does not focus on the events that contribute to the crime but on the opportunities that emerge as a result of preventive measures to curb the crime. Proponents of this theory argue that crimes transverse between location, time, target, direction, and method of committing the crime [33]. They further assert that Opportunity to commit a crime is a root cause of crime. Also, they posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby reducing opportunity of crime.

5.3 Technology Theory

The response of technology to the cyber crime problems centre on the use of computer security theories to design and evolve solutions that provides authentication, verification, non repudiation and validation. These theories and models rely on the use of cryptography, steganography, network protocols, and the use of software engineering process/models to develop systems that offer some form of protection for users and the information infrastructure. Cybercrime thrives on the web today because the internet did not inculcate in its protocols from the onset a mechanism that allows a host to selectively refuse messages [24].
This implication is that a benign host that desires to receive some particular messages must read all messages addressed to it. In essence, a malfunctioning or malicious host has the capacity to send many unwanted messages. This problem is exacerbated by the ubiquitous nature of the web and remains the Achilles heel of the issue of web security today. Although all the theories discussed above are related to cyber crime, we are inclined to adapt routine activity theory to this study because the theory captured the philosophical assumptions upon which this study is based.

5.4 Social Theories

From a social scientific point of view, security theories on providing and implementing protection against breaches and information system misuse have evolved. They focus on user security awareness, motivation, deterrents, technology and training [39, 36, 11, 23, 59, 60]. Researchers have theorized that user perception of risks and choices based on those perceptions can influence system security [9]. The situational characteristics theory proponents argued that situations within a system usage domain can impact on ethics and user behaviour [58, 52, 12]. Wood [76, 77] proposed the Human Firewall theory stating that those user actions can undo technical security measures. He advocated that organizations must sensitize and educate users and evaluate their compliance with security policies and procedures.

The theory of least possible privilege as proposed by Beatson [13] suggests psychological profiling of potential new users, while Bray [15] argues that new users are more vulnerable to security breaches when using information systems (IS). Denning [27] theorizes about defensive information warfare and proposes that security policy training and awareness will better equip users against threats. Forcht, Pierson and Bauman [35] theorized about ethical awareness and culture as factors that influence IT security. Kabay (2002) theorized about using social psychology as a tool to improve user security conduct. The importance of the interest of senior management and integrating security issues as part of the corporate asset protection model was highlighted by Katsikas [40], Kovacich and Halibozek [42] and Perry [58]. Vroom and von Solms [75] also modelled an Information System security awareness program to address end-users, IT personnel and management executives.

McLean [53] theorized about using values, perceptions and behaviour to change user attitude about security, while Murray [54] argues that ignorance and incompetence about the consequence of security policy abuse is a serious problem among users. Parker [57] proposed a theory that uses rewards and penalties to influence attitudes toward security in information systems.

Sasse, Brostoff, and Weirich [63] theorized that the nature of the technology with respect to the user’s goals and intentions significantly influence security features and usage in IS systems. They went further to propose the use of training, punishment, and reporting security as a motivation for creating security awareness among users. Schlienger and Teufel [64] adopted a socio cultural approach to information security and posited that the cultural theory can be used to enhance security at different cultural layers-namely, corporate policies, top management, and individuals. Siponen [66] used human morality as a force that can impact on security. Straub and Welke [72] theorized about using strong deterrents to convince potential violators of those organizations means in business about protecting information infrastructures. Tudor [73] argued for a theory that uses a holistic IS security architecture to incorporate infrastructure, policies, standards, awareness and compliance. He however, concentrated on awareness training at the expense of all the other components.

5.5 The Peel Theory

The Peel theory of community policing as highlighted by Longe et al [50] assumes that violators or criminals and victims are usually proximate and used spatial distribution as a basis for apprehending criminals and solving crimes. This theory subsumes the role of the citizens in responding to partial and completed crime, crime control, and internal order and makes the police responsible for all crime control and law enforcement activities. Although some consensus exists among nations on how to combat and deal with crimes across borders using international policing such as the Interpol, the underlying theory still relates to the Peel model and it is therefore inadequate to face the cyber crime problem. We cannot say as a matter of fact that there is any theory in existence from the criminal justice and policing angle that specifically addresses the problem of cyber crime.
5.6 Space Transition Theory:
Proponents of space transition theory argue that behavior of people in cyber space tends to bring out their compliance and noncompliance behavior both in the physical and in cyber space. This theory does not explain physical crime but cyber crime and how people move and behave from one space to the other (Schmalleger & Pittaro, 2009). This entails persons with repressed criminal behavior (in the physical space) having a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space, due to their status and position. It also implies that the status of persons in physical space does not transit to cyber space. Jaishankar [37], for instance, argues that the individual behavior repressed in physical space is not repressed in cyber space.

6. CONCLUDING REMARKS

This paper examined the impact of the information communication technology (ICT) revolution on business, industry and government in the light of the unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and other related cyber crimes. We specifically assessed cyber crime and its impact on the banking institutions in Nigeria. Existing policy framework were examined and their success as institutional countermeasures in combating cyber crime in the banking industry were assessed.

Finally, we provide insight into how cybercrime impacts on E-banking from a Nigerian perspective using social theories to explain causation with a view of guiding policy makers on behavioural issues that should be considered when formulating policies to address cyber criminal activities in Nigeria.

REFERENCES

1. Advance Fee Fraud and Other Fraud Related Offences Act 2006, Laws of the Federation of Nigeria


67. Search security (2009), Information Security magazine
78. www.bbc.co.uk