Journal of Information Technology Impact
Vol. 11, No. 2, pp. 85-100, 2011

Sakawa - Cybercrime and Criminality in Ghana

Richard Boateng[1]
University of Ghana
Ghana

Longe Olumide[2]
University of Ibadan
Nigeria

Robert Stephen Isabalija[3]
Southern University
USA

Joseph Budu[4]
PearlRichards Foundation
Ghana

Abstract

This paper investigates the prevalence of cybercrimes (caled 'sakawa') in Ghana and examines its forms and implications.Using qualitative approach, we explore efforts by organizations and government agencies in Ghana towards curtailing cybercrimes in terms of apprehension, prosecution, reporting, and law enforcement. Findings from our research showed that although awareness of cyber crimes is on the increase, the crimes mostly go unreported. The Ghana Police Service which is the organ of government responsible for arresting and prosecuting cyber criminals also lack the technical know-how and adequate legal support to effectively discharge their duties. We recommend that a multi-stakeholder effort and appropriate technical training for the Police and supportive legislation are required. For online financial transactions, developing strategies which incorporate offline business qualification requirements may be the necessary starting point. Since the perpetrators are young and have some degree of technical competence to commit computer-related crimes. This brings to question the need for appropriate youth development programs which utilize their technical competencies. In future research, we will explore how social theories in criminology can assist in understanding the behavior and intention of both the victim and perpetrators in cyber crime.

Keywords: Internet fraud, gold fraud, financial transactions.

Introduction

As compared to some decades ago, information and communication technologies (ICT) penetration and adoption is on the increase across Africa (ITU, 2008). Although rudimentary access to internet and other online facilities in most parts of Sub-Saharan Africa still depends on the use of public internet access points such as cybercafés, nations like Nigeria, Cameroon and Ghana now have facilities for mobile internet access through satellite connections and fiber optic cables. This increase in penetration of ICT, especially along the West African coast, has spurred a

growth in ICT-based businesses and services including electronic government, electronic commerce, teledemocracy, telemedicine, and electronic banking services. Unfortunately, this level of globalization that is being facilitated by ICTs has also simultaneously raised the specter of new criminal activities arising to exploit them. The internet has become a double-edged sword providing opportunities for individuals and organizations and also bringing with it an increased information security risk (Magele, 2005).

We conceptualize cybercrime as criminal activities or crimes in which computing devices or other forms of ICTs are the target source (Pati, 2003). From the perspective of ICT for development, it is not misplaced to say that cyber crime portends some dangers and have the potential to stall the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and usage in Sub-Saharan Africa. Cyber fraud has a potential to widen the digital divide, crumble the information infrastructure and affect consumer confidence in online transactions (Salifu, 2008; Longe et al., 2009; Oumarou, 2007). Literature is, however, sparse on nation-specific extent of these fraudulent cyber activities as well as nation-specific measures put in place to address them. For instance, Ghana, our country of interest, in this research ranked among the top ten for the source of fraudulent cyber activities in the world with Nigeria ranking 3rd in the 2008 Internet Crime Report (I3C, 2008). The Ghanaian government has made concerted efforts to create a 'knowledge-based economy' thereby making Ghana an ICT –driven economy. The use of the Internet in Ghana has also seen a significant increase since the liberalization of the telecommunication industry in the 1990s. The country had 43 Internet users per 1,000 people in 2008 as compared to 1 Internet user in 1999 (ITU, 2009). The number of PC ownership doubled to 52 owners per 1,000 people between 1999 and 2005 (ITU, 2007). With these developments also come negative effects and unintended consequences of ICT, particularly, cyber crime. Our effort in this paper is directed towards understanding the extent of fraudulent cyber activities as well as measures put in place to address them in Ghana.

The remaining part of the paper is organized in seven sections including the introduction. In the second and third sections we examine the scope of financial cyber crime and the jurisdiction of law in dealing with it. The fourth and fifth sections present the methodology for the research, and findings on cyber crime in Ghana. The sixth and seventh sections concludes the paper with a summary of findings, implications for research, and practice and future research directions.

Financial Cybercrime – A War without Walls

Cases of online fraud pertaining to credit card crimes, contractual crimes, offering jobs, and advanced fee fraud have been fairly documented (Magele, 2005; Longe et al., 2009). Cyber criminals capitalize on system vulnerabilities, ignorance and gullibility on the part of users to perpetrate their heinous crimes. Between 2006 and 2007, financial losses occasioned by cyber crimes in the United States alone increased dramatically from $52.5 million in 2006 to $67 million in 2007 (Richardson, 2008). Internet connectivity makes it much easier for criminals to act beyond national boundaries when conducting their illegal affairs. With over 300 countries connected to the internet and still counting, cyber crime has become a global issue that requires a multi-stakeholder effort including governments, the private sector, civic and legal institutions, and other social organizations (Westby, 2003; Broadhurst, 2006).

A genre of these fraudulent cyber activities that has emerged internationally and is believed to originate mostly from the West African coast, particularly Nigeria, is the "advance fee fraud" - a type of Internet fraud used to defraud victims willing to succumb to the temptation offered to make some "quick money" (Smith and Grabosky, 2001; Cukier et al., 2007). Skirmishes of these incidences are now being increasingly reported in other West African nations such as Senegal, Cote d'Ivoire, Cameroon, Sierra-Leone, the Gambia, Benin republic and Ghana (Oumaru, 2007). The frauds take the form of victims being approached by letter, faxes or, recently, electronic mail, without prior contact. Victims' addresses are obtained from telephone and email directories, business journals, magazines, newspapers or through web e-mail address harvesters (Longe and Chiemeke, 2006). These "419" mails generally describe the need to move funds out of one nation or the other, usually the recovery of contractual funds, crude oil shipments or over-invoiced payments, all of which are non-existent, and sometimes using apparently legitimate documents emanating from sources such as the Government, Multinationals and Banks. To facilitate arrangements, victims are asked to supply bank account details and later, money to pay legal fees, taxes, bank transfer fees or bribes for a commission, which could be up to 40 percent of the capital involved. Capital sums of US $20-40 million are often mentioned, thus creating a potential reward for the victim of up to US $16 million. These crimes, as Larkin (2006) posited, pose a threat to global well-being. It has made doing business on the Internet more risk-prone than dealing with a conventional customer. Further, anonymity in cyberspace conceals the cyber criminals' looks and intent (Laudon and Guercio, 2004), and thus, makes measures to address the challenge more difficult to prescribe. Cyber crimes will increasingly be initiated from jurisdictions that have few laws directed against cyber-crime and little capacity to enforce laws against it. This is the scenario in most of the Sub-Saharan African nations where some of these crimes are purported to emanate. Pati (2003) noted that, "the (de)creativity of human mind cannot be checked by any law. Thus, the only way out is the liberal construction while applying the statutory provisions to cyber crime cases".

Cybercrime and Legal Jurisdictions

Research has examined the implications of a globally diverge view on criminal laws as it relates to the apprehension and prosecution of cyber criminals (Brenner and Koop, 2004). Nations have different perspectives on the issue and existing statutes enacted over the past decades in various countries show varying and diverging jurisdiction clauses. The law of jurisdiction must address whether a particular event in cyberspace is controlled by the laws of the state or country where the website is located, by the laws of the state or country where the Internet Service Provider is located, by the laws of the state or country where the user is located, or perhaps by all of these laws (Brenner, 2007). However, in some countries, a number of cyber crimes are yet to be captured by national laws. For example, in Brazil hacking alone is not a crime, and under the law, fraud needs to be proved in order to prosecute (BBC, 2004). The burden of proof of online fraud is a daunting task for an ordinary internet user. In 2005, a Miami businessman filed a lawsuit against the Bank of America. Money had been transferred out of the claimant's bank account; the fraudster was able to get the businessman's account details through a key-logging virus which had infected the claimant's computer. The Bank of America said that they were not liable for the theft and transfer, as the transfer had been "completed with appropriate handling and security procedures" and their "own systems were not subject of hacking". The claimant said the bank was

negligent and should have "let him know of the virus threat prior to the transfer" (The Banker, 2005). If the ordinary internet user cannot take recourse from the bank, reporting future incidences will become discouraging.

Even with sophisticated users such as organizations and institutions, reporting cyber crime is a question of the trade off of reputation and image and the potential loss of confidence by key stakeholders. A British newspaper reported that banks and other financial institutions are deliberately failing to report incidents of online fraud to the Police and attacks on their system, possibly because of the potential damage to their reputations, concerns over public confidence or lack of confidence in the Police and legal system to deal with such crimes (Rupert, 2006). Thus, the true loss from cyber crime could be quite 'scary' when unreported cases of online fraud are taken into account.

This challenge in addressing cyber crime in developed countries is not far from that of developing countries. In India, most cyber fraud cases go unreported and this has been one of the drawbacks in fighting cyber crime in that nation. In Sub-Saharan Africa, records of report from victims of cyber crime are very sparse. These cases mostly come into limelight when foreigners are duped or defrauded by the cyber criminals. It is generally believed that victims are usually high profile citizens or rich expatriates who cannot face the embarrassment of people knowing that they have been duped. The implications of cyber crime and the limited options to address the issue are therefore far-reaching and emphasize the need for more research.

This research, in response, seeks to investigate the state of cyber crime in Ghana and measures being used to address it.

Methodology

This research seeks to investigate the state of cyber crime in Ghana and measures being used to address it. To achieve this, the research questions to aid us in gathering baseline information on the subject matter are:

1. What are the forms of cyber crime in Ghana?
2. How is Ghana addressing reported cases of cyber crime?

To develop an in-depth understanding of cyber crime, an exploratory case study method was adopted (Yin, 1994). We adopted qualitative interview approach with key stakeholders on cyber crime in Ghana to obtain richness of experiences regarding apprehension, prosecution, reporting, and law enforcement. A total of 40 respondents participated in this study. The respondents represented information and communication technology (ICT) services, banking, law enforcement and legal agencies. The 40 respondents include: 10 personnel of three selected Banks involved in international money transfer, 10 internet café operators, 10 Police investigators working at the Commercial Crime unit of the Criminal Investigation Department (CID) of the Ghana Police who are responsible for investigating Internet fraud, 5 legal practitioners who worked on cyber crimes cases and 5 internet fraud victims. The respondents were between 28 and 45 years old with a mean age of 35. Sixty percent of the respondents (24) had more than a bachelor's degree, 30 percent (12) had a bachelor's degree and 10 percent (4) had a diploma or professional certification. With the exception of the internet fraud victims, all respondents (35, 88

percent) selected had a minimum 3 years of working experience in their occupations in the ICT, banking, law enforcement or legal sector. In selecting the sample, the Ghana Police CID and one lecturer in a University of Ghana Business School were consulted. The discussions on the research theme led to referrals to the banking and legal agencies and the internet fraud victims to be involved in the study. The referred respondents had collaborated with the Ghana Police CID in cyber crime investigations and were willing to participate in the study without any compensation.

Data was collected over a nine-week period from September to November 2009. The primary instrument used in the data collection for the study was interviews - four sets of interviews with the selected respondents; the banks, the internet café operators, the Police and the internet fraud victims. The interview consisted of open-ended questions, which enabled the researchers to seek further explanation to issues that might not be covered by the questionnaire. Regarding the banks, the interview questions were tailored towards measures to prevent financial institutions to be used as the medium for defrauding people and the challenges in dealing with cyber crime suspects. Regarding the Police and legal practitioners, the interview questions were about the cases reported, their mode of operations in arresting the criminals and the preventive measures if any, being put in place to check the perpetrators of these crimes. Statistical data obtained from the Police covered 2006 to 2008; 2009 data on cyber crime was still being collated. Internet Cafe operators were also interviewed about their mode of operations. Regarding the internet fraud victims interviewed, they were all expatriates from the United States, Germany and the UK. They were interviewed in the offices of the Police where they were invited from their various countries to assist in investigation based on the complaints they had lodged. We failed to have access to any indigenous victims, since the few who usually reported and collaborated with the Police opted to stay out from any form of interviews.

The interviews were recorded and transcribed, with copies of transcribed interviews returned to interviewees to check and resolve discrepancies. Data was coded and analyzed in themes (apprehension, prosecution, reporting, and law enforcement) which address our research questions and also provide a better understanding on cyber crime in Ghana.

Data Presentation and Analysis

The data collected from the questionnaire and interviews with their analysis is presented in this section.

Internet Café Operators

The main item of the questionnaire requested the respondents (10) to indicate the approximate age of their customers. Figure 1 shows the age distribution table of the customers of the cafes according to the internet café operators.

From the Figure 1, the approximate age between 18 to 30 years constituted about 88 percent of their customers whilst the remaining 12 percent is shared among the ages of 31-35 and above 35 years. The age distribution above tends to suggest that, most of the people who patronize these cafes are young men and were likely to form a majority of perpetrators of the crime. The researchers at the time of administering the questionnaire observed that more adolescent boys

below the age of fifteen patronize their services, but in answering the questionnaires, the café operators tend to have reported a lesser number. In corroborating these findings with the Police unit interviewed, it was confirmed, as shown in Figure 2, that the majority of cyber crime suspects are the youth aged between 21-35 totaling 85 percent.

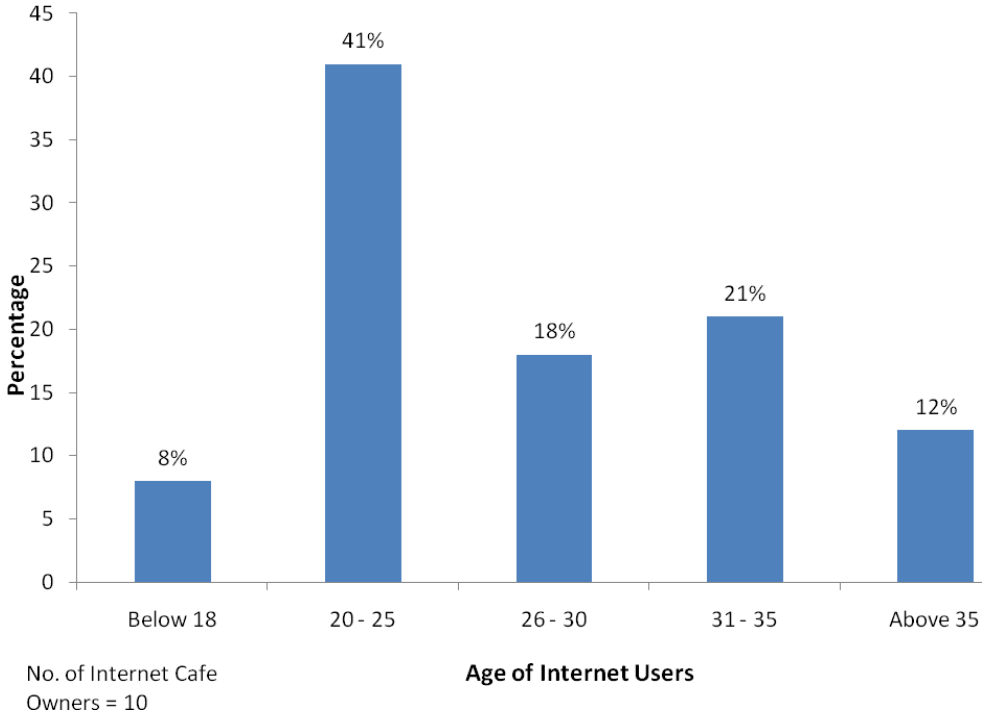

Figure 1. Perceived Age Distribution of Internet Users

The internet café operators stated the internet was being used for crimes including child pornography, hacking sites to get access to credit cards and downloading films for sale. They are aware of these crimes because the print and electronic media had increased awareness. The financially related crimes have been christened "Sakawa" in the country. They also mentioned that monitoring customer activities online will make them lose customers as there is very strong competition among internet cafes for customers. Although they are not sure of the nationality of some of those who engage in cyber crime in their cafes, the accent of some of them suggest they were of Nigerian descent. In corroborating this claim with the Police Unit, the Police stated that, based on the 2008 statistics (Figure 2), 40 percent of the arrested suspects are Nigerians and Ghanaians make up 38 percent. The nationalities of Liberia, Cote d'Ivoire and Togo total the remaining 22 percent.

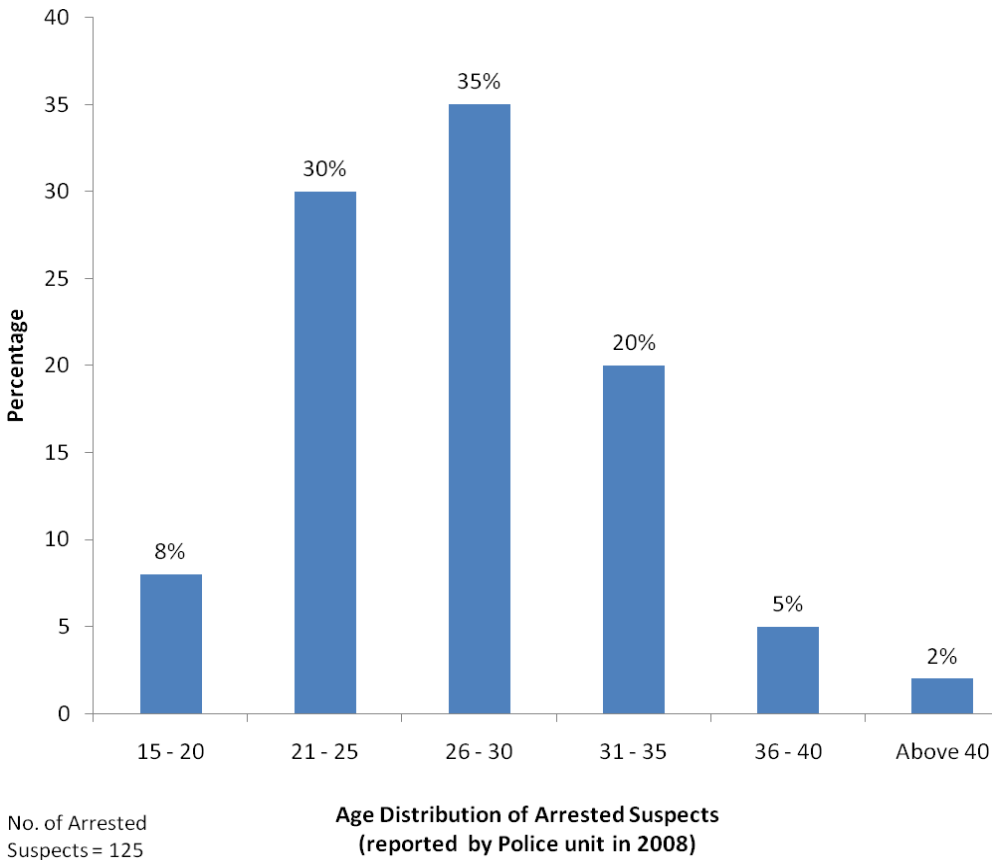

Figure 2. Age Distribution of Arrested Suspects

Banks that operate Money Transfer Service

The bankers indicated that they have been rendering fund transfer services for over a decade. Respondents were then asked to indicate the procedure a receiver of a transferred money passes through before he or she collects the money. They indicated the inspection of recipients' identity cards and the completion of required forms. A follow up question was whether they experience any fraudulent practices on the side of the customers. They all answered in the affirmative. One of the interviewees commented that "we don't report customers who we suspect to be engaged in criminal activities to the Police. We only refuse payments, and ask the recipients to go". Another set of questions tried to find out if the respondents have websites and if yes how secured they are. All the respondents indicated they have but could not adequately comment on the security of their websites. A follow up question was to find out whether or not they render online services, and if yes, have they experienced any fraudulent acts on the part of customers. They all said they have experienced some online fraudulent deals which had been reported by their customers. One respondent also explained that, "we usually detect some sort of fraud when there is a request by a

customer to empty an account or withdraw all the money in the account. In other circumstances we detect fraud from the frequency of withdrawal". When fraud is detected, the cheques are not honored and the banks investigate with the aid of the Police. Respondents of two of the three banks interviewed indicated that, they inform the Police since quite a number of the fraudulent practices are done with the connivance of bank staff. The respondents of the third bank indicated that they normally refuse to honor the cheque and ask the customer to leave. They cautioned that, the banking sector is now full of competition and therefore reporting such case to the Police especially when a staff is involved, could mar their image and reputation.

Concerning their perception on the antecedents of cybercrime, the respondents indicated that the main causes might be unemployment, the quest to get rich quick, gullible foreigners who are greedy and 'crazy" to buy gold, lack of strong legislation, and lack of commitment of Bank staff and money transfer operators. The recommended solutions include the need for strong legislation, resourcing the cyber crime unit of the Police and creation of more jobs for the youth.

Personnel of the Commercial Crime Unit of the Ghana Police Service

The Commercial Crime unit of the CID of the Ghana Police Service is the agency of the government that is charged with the responsibility of arresting, investigating, and prosecuting the perpetrators of Internet fraud in Ghana. Ten of the employees of the Unit were interviewed for this research. The respondents indicated that they received complaints about internet fraud that centered on gold deals, inheritance, 'money in account', 'marriage deals' and raffles. Regarding gold fraud, the Police explained that, the gold fraud suspects send emails to the email addresses of the victims and introduce themselves as friends and later as gold dealers who can help them get gold in Ghana. First, the suspects send a piece of pure gold to the Ghana Precious Mineral Commission for testing. The commission issues report and receipt for amount paid for testing. Second, the suspects scan and email the report to the victim. The victims usually call the commission for verification. However, since the report and the receipt are genuine, the confirmation from the commission increases the confidence of the victim. Hence, the victim sends any amount of money requested for and becomes duped in gold fraud. Some of the receipts are however not genuine. Figure 3 shows a copy of a fake receipt one of the fraudsters sent to his victim in Switzerland after the victim sent $1,850 for the purchase of gold.

Regarding inheritance and money in account fraud, the perpetrators contact victims through faxes, e-mail addresses which they obtain from telephone, web crawlers and business journals. They create letter heads that look very legitimate and from sources such as Ghana Government, Bank of Ghana claiming that they need to move funds out of Ghana. Such funds are usually contractual or inherited funds or over invoiced payments, all of which were non-existence. To facilitate the movement, victims are asked to supply bank account details and later, money to pay legal fees, taxes, bank charges or bribes for commissioners of oaths. These amounts if sent by the victim represent the amount stolen or defrauded. Online dating sites have also been used to defraud victims with 'ladies' posting pictures and claiming they want husbands. Money sent by interested suitors for marriage rites or plane ticket to join or visit victim abroad are defrauded.

GHANA SOLID MINERAL COMMISSION
ACCRA-GHANA

4823

GENERAL COUNTER FOIL RECEIPT

Date 17-12-2008

Received from INTERNATIONAL COMMERCIAL BANK LTD

The sum of ONE THOUSAND EIGHT HUNDRED AND FIFTY US DOLLARS, ONLY.

Being INCORPORATION FEE FOR " MIFTAR MINING COMPANY"

Cheque/Cash

US$ 1,850.00- - - - - - - -

GHANA SOLID MINERAL COMMISSION "ACCRA-GHANA"

Sign:

COMPANIES CODE 1963(ACT 179)

NOT VALID IF HANDWRITTEN

Figure 3. Sample Scam Check

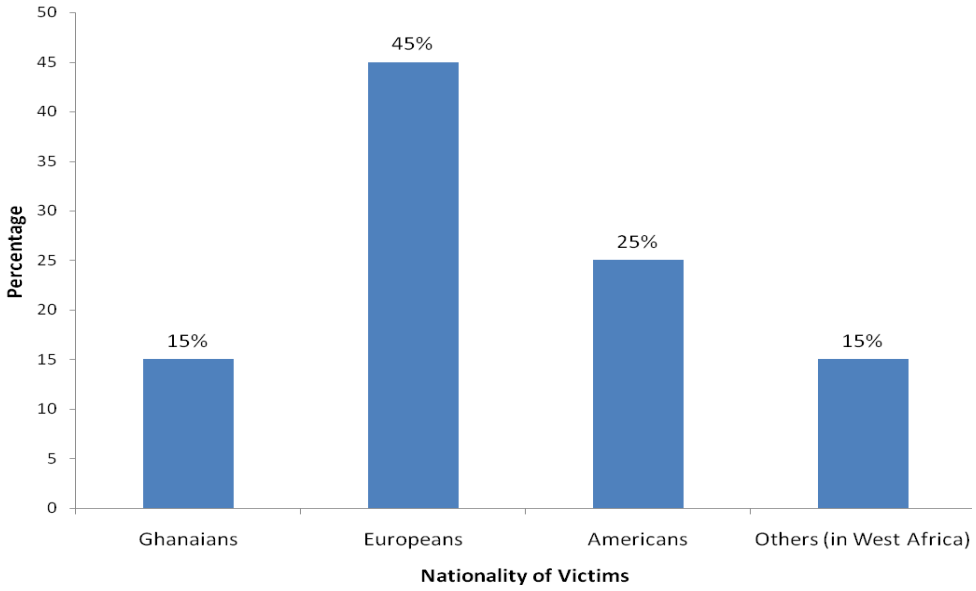

Figure 4. Graph of Nationality of Victims

From Figure 4, it could be observed that, victims are mostly from USA and Europe totaling 70% of reported cases. Only 15% of the victims come from Ghana whilst the remaining 15% came from other African countries. One of the respondents (Police) commented that "most victims of internet fraud are high profile and/or rich people in our society who feel reluctant to go to the Police station and report because of their status in society and the fact that, they don't want to look stupid before the Police". On the other hand, three of the victims of Internet fraud from Holland, Switzerland and the USA interviewed were of the view that, victims of many of these crimes decide not to report to the Ghana Police because of certain activities of the Police that tend to discourage them, for example, the unnecessary delay in persecuting the offenders. However, the Police argue that, the delays often stem from obtaining evidence and tracing accomplices to the crime. A number of cases, especially in 2007 and 2008, which had been rushed to the courts without adequate evidence, have been lost. Other cases could not be investigated further, because the complainants are mostly expatriates who refused to come to Ghana to assist in investigation. Table 1 shows the statistics of cases reported to the Police between 2006 and 2008.

Table 1. Statistics of Reported Cases

	2006	2007	2008
No. of cases reported	257	88	241
No. of cases prosecuted	121	40	125
No. of cases convicted	9	5	27
No. of cases Acquitted	9	-	-
No. of cases Pending	127	43	89

Source: Ghana Police Service Commercial Crime Unit of the Criminal Investigation Department.

The number of cases reported is declining with a drop of about 65 percent between 2006 and 2007. In 2008, the reported cases increased to 241 well above that of 2007. However, the respondents intimated that, the crime is on the increase. In a number of scenarios the victims were criminals who also engaged in internet fraud and therefore could not report when they were defrauded; and in other scenarios, the victims are indigenous public or popular figures and hence, avoided the Police and court. These scenarios often contributed to less cases being reported.

When requested to indicate their computer literacy level, the respondents claimed to have some computer knowledge but failed to state the levels of the computer literacy. A further question as to how they use the computer to detect the fraud or the modus operandi of the suspects. The Police explained that, though they have received some help from computer experts, arrests have been done primarily through the help of the victims by baiting the suspects. For example, upon receipt of complaint from a victim especially from abroad, the victim is asked to fly to Ghana presumably bringing more money without the knowledge of the suspect that, the Police are aware of the deal. Upon the arrival of the victim, the suspect meets the victim at a secret location with the intention of collecting more money and they are arrested. Victims that

could not come down after their complaint are made to transfer a little more money to the suspects. The suspects are arrested when they go in for the said money.

Legal Components for Cybercrime Prosecution

Respondents in this case consist of legal practitioners and were asked to indicate the type of law in the criminal code of the Republic of Ghana under which the suspects or internet fraud are charged and whether or not it is appropriate to charge them under these laws. All the respondents indicated there is no law in the statute books 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 bailable offences and carry lesser punishments which cannot therefore deter the fraudsters from committing cyber offences. The respondents also indicated that it is not wholly appropriate to use this law because the facts of some of the cases do not support the charges made against the suspects under that law hence most lawyers capitalize on such technicalities and have their clients acquitted. It was also noted that the Ghanaian Parliament is currently reviewing a bill to pass laws governing a wider perspective of crimes associated with technology and the Internet.

Summary of Findings

Three key findings can be summarized from the above discussion. First, this research brought to the fore the fact that cyber crime is fast gaining grounds in Ghana and the agencies responsible for investigating, controlling and apprehending online criminals lack the technical knowledge needed to tackle the problem. Second, in Ghana, the perpetrators are young and have some degree of technical competence to commit computer-related crimes. This research does not deviate from other findings relating to the social characteristics and level of expertise of the perpetrators. Offenders are more likely to share a broader range of social characteristics and are likely to be young, clever often without prior criminal records, possessing expert knowledge and often motivated by a variety of financial and non-financial goals (Balkin et al., 2006; Salifu, 2008; Coomson, 2006; Wall, 2001). However, it questions whether appropriate youth and community development programs can be developed to utilize the technical competencies of the youth in Ghana and perhaps, Sub-Saharan Africa. Third, the research data also showed that most cases go unreported due to lack of confidence in the prosecuting process and fear of embarrassment on the part of the victims. Ghana is yet to enact any law to specifically address these forms of crime. The laws under which the suspects are charged are the existing laws on fraud established in 1960. Defense lawyers often win over when the prosecution presents poor evidence.

These findings are indicative of the fact that measures adopted to curb internet fraud in Sub-Saharan Africa in general and in Ghana particular are grossly inadequate and therefore poses a serious danger to investment opportunities in the country and the region. Curbing the upsurge of cyber crime in resource-poor contexts, like Ghana, is particularly important if the promise of the Internet is to reach its full potential and if businesses and consumers are to avoid significant losses as a result of criminal activities. Perhaps, though not exhaustive, the most important and immediate measure is education. Educating individual citizens and businesses is primary and should be a multi-stakeholder effort involving government, financial institutions, internet service

providers and internet businesses. For individual citizens, education may focus on online conduct and measures to identify forms and behavior of perpetrators. Businesses, on the other hand, need to be educated on how to develop appropriate policies governing online conduct and technical security measures to protect organizational information systems and networks. Further, in the conduct of online transactions, there needs to be a more intimate collaboration between businesses and financial institutions.

Boateng et al. (2009) give an example of how two firms – a Ghanaian and a Tunisian firm – engaged in an online transaction used their individual local banks to verify and establish the credibility of each other before any financial transaction took place. Until developing countries develop and enact appropriate cyber laws, developing internet strategies which incorporate offline business requirements may be the necessary starting point. This may be the recourse to some of the financial cyber crimes for businesses. However, other forms of cyber crime like Internet terrorism and child pornography may require empowering law enforcement agencies with resources and laws (Longe et al., 2009), establishing forms of mutual legal assistance (Broadhurst, 2006) and researching into new technical security measures (Longe et al., 2010).

Conclusion

Cyber crime is common to both developed and developing countries. Its impact appears to be worse in developing countries where the technology and law enforcement expertise is inadequate. This shared challenge tends to be reflected in Ghana. The limited options for the Police, legal and financial institutions to address cyber crime call for a multi-stakeholder analysis at the national-level.

Concerning practice and policy implications, the research provides the basis for a concerted effort on the part of individual citizens and corporate bodies, to report cyber crime cases and demand that government put in place laws, policies and technologies to curb cyber crime. As with other forms of ICTs, since these laws are critical, there is the need to gain political support. This could be from the government, or political parties, interest groups, private sector advocates, thus key stakeholders who can push for these legislation and rules.

The government should empower the Police force by providing the needed training and technical resources required to discharge their duties effectively. The Bank of Ghana which regulates Commercial Banking operations must develop a reporting scheme on all the identity of all recipients of foreign remittances to it or other agencies of the state so as to create a database that can be reviewed regularly and used for investigating suspicious foreign remittances.

Internet service providers operating in the country should also be mandated to report suspicious traffic going through their networks. Since cybercrime is a global problem, the need also arise for law enforcement agents in Ghana to collaborate in the area of information sharing, infrastructure and personnel with other African Countries and major international security agencies such as the Federal Bureau of Investigation and INTERPOL to crack-down on cyber criminals.

Concerning research implications, the need for a multi-stakeholder effort and poor reporting behaviour of victims, emphasizes the social dimension of cyber crime. This calls for research into how DCs or Sub-Saharan African countries can draw on their collective culture (Hofstede, 1985) to develop strong interest or civic groups (local and international) who can become the pivot for education and lobbying for laws. Future research can also explore how social theories in criminal studies can help understand behaviour and intention of both the victim and perpetrators in cyber crime.

This research, though not exhaustive, has generated valuable insights which can help frame future research and policies. Not giving the right attention to this challenge poses a risk to ICT development in Sub-Saharan Africa and Ghana in particular.

Acknowledgments

The authors wish to thank Innocent Avevor, Kwafo Offei, Ebenezer Nketiah, Florence Tsakuor Nartey, Ebenezer Boryor, Shaibu Abubakar Osei for their support for this research as research assistants and Prof. Adenike Osofisan for her input and insights as a very senior colleague. This paper is based upon work supported by the Pearl Richards Foundation under the Cyber crime Research Project. Any opinions and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the PearlRichards Foundation.

References

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., and Zarsky, T. (2006). *Cybercrime: Digital Cops in a Networked Environment*. New York: New York University Press.

Boateng, R., Heeks, R., Molla, A. & Hinson, R. (2009). Developing E-commerce Capabilities in a Garment Manufacturing Firm – The Case of a Ghanaian Firm. In R. Hinson, R. Boateng, & V. Mbarika, (Eds.), *Electronic Commerce and Customer Management in Ghana*. Accra, Ghana: Pro Write Publishing.

Brenner, S. (2007). *Law in an Era of Smart Technology*. Oxford: Oxford University Press.

Brenner, S. & Kopops, B. (2004, October). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, *4*(1), 3-44.

British Broadcasting Corporation (BBC) (2004, October 21). *Brazil holds $30m fraud hackers*, BBC News Story.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime, *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408 – 433.

Coomson, J. (2006, October 4). Cyber crimes in Ghana, *Ghanaian Chronicle*. Retrieved February 23, 2010, from http://allafrica.com/stories/200610040856.html.

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, Narrative and the "Nigerian Letter" in Electronic Mail. In *Proceedings of the 40th Annual Hawaii international Conference on System Sciences*, January 03 – 06, HICSS. IEEE Computer Society, Washington, DC, 70.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: the convergence of technologies. In Wall, D. (Ed.), *Crime and the Internet.* London: Routledge.

Hofstede, G. (1985). The interaction between national and organizational value systems. *Journal of Management Studies*, *22*(4), 347-357.

International Telecommunications Union (ITU) (2007). *ICT Statistics Database*, ITU, Geneva. Retrieved January 10, 2010, from http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx

International Telecommunications Union (ITU) (2008), *Africa, ICT Indicators 2007*, ITU World Telecommunication/ICT Indicators Database, Geneva. Retrieved January 13, 2009, from http://www.itu.int/ITU-D/ict/statistics/at_glance/af_ictindicators_2007.html

International Telecommunications Union (ITU) (2009). *ICT Statistics Database*, ITU, Geneva. Retrieved January 13, 2009, from http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx

Internet Crime Complaint Center (IC3) (2008). *2008 Internet Crime Report, Internet Crime Complaint Center*, USA. Retrieved January 10, 2010, from http://www.ic3.gov/media/ annualreport/2008_IC3Report.pdf

Larkin, D. (2006). *Fighting online crime*. Retrieved January 10, 2010, from http:// usinfo.state.gov/ journals/itgic/0306/ijge/larkin.htm

Laudon, K. C., & Guercio Traver, C. (2004). *E-Commerce: Business, Technology, Society*. Reading, MA: Addison Wesley.

Longe & Chiemeke, S. (2006). The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. In *Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences,* June Covenant University, Ota, Nigeria, 1 - 7.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, *9*(3), 155-165.

Magele, T. (2005, February 16/17). *E-security in South Africa*, White Paper prepared for the ForgeAhead e-Security event. Retrieved October 22, 2009, from www.forgeahead.co.za/

Oumarou, M. (2007). Brainstorming advanced fee fraud: 'Faymania' – the Camerounian experience. In N. Ribadu, I. Lamorde, & D. Tukura (Eds.), *Current trends in advance fee fraud in West Africa*, EFCC, Nigeria, 33–34.

Pati, P. (2003). Cybercrime, New Delhi. Retrieved February 23, 2010, http://www.naavi.org/ pati/pati_cybercrimes_dec03.htm

Richardson, R. (2008). *2008 CSI Computer Crime and Security Survey*, Computer Security Institute. Retrieved January 12, 2010, from http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf

Rupert, J. (2006, December 5). Banks hiding online fraud, says Police. *The Guardian*.

Salifu, A. (2008). Impact of Internet crime on development. *Journal of Financial Crime, 15*(4), 432–444.

Smith R. G., Grabosky P. N., & Urbas G. F. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

The Banker (2005, March). Lawsuit raises online fraud issue for banks. *The Banker*, p.12.

Wall, D. (2001), *Crime and the Internet*. London: Routledge.

Westby, J. R. (2003). *International Guide to Combating Cyber Crime,* American Bar Association, Section of Science and Technology Law, Chicago, IL.

Yin, R. K. (1994). *Case Study Research, Design Methods* (2nd ed.). Newbury Park: Sage Publications.

---

[1] Dr. Richard Boateng is a technology researcher who focuses on developing, promoting and protecting ideas and concepts into sustainable projects of commercial value and development impacts. He is the Founder and Executive Director of PearlRichards Foundation, Ghana. Richard is also a Center Associate of the Center for Development Informatics at the University of Manchester, UK.. He can be reached at Richard@pearlrichards.org, richard@pearlrichards.org or +233261599344.

[2] Dr. Olumide Babatope Longe is the consulting director for cyber crime research at the PearlRichards Foundation. His research interests include cybercrime causation, apprehension, treatment, prevention using social theories and information security models. He is on faculty at the Department of Computer Science, University of Ibadan, Ibadan, Nigeria. He can be reached at longeolumide@ieee.org or +2348024071175.

[3] Mr. Robert Stephen Isabalija is the consulting director for projects monitoring and evaluation at the PearlRichards Foundation. He is the Head of the Institute of Change Management and Public Policy at the International Center for Information Technology and Development (ICITD), Southern University, USA. He is also a lecturer at Makerere University Business School, where he lectures and researches change management, innovation and organizational behavior. He can be reached at Robert@pearlrichards.org or +12252766479.

[4] Mr. Joseph Budu is project coordinator at PearlRichards Foundation where he coordinates research activities of the foundation.He be reached at Joseph@pearlrichards.org.

Page left blank