Computer Science and Engineering 2012, 2(6): 98-100
DOI: 10.5923/j.computer.20120206.03

Fighting Cybercrime in Africa

Henry Osborn Quarshie[1,*], Alexander Martin- Odoom[2]

[1]Lecturer Regent University College of Science & Technology, Accra,Ghana
[2]Lecturer School of Allied Health Sciences,University of Ghana

Abstract Cyber threat is a big issue in Africa. A lot of cybercrime emanates from the continent, and threats spread easily because many servers and computers are not properly protected. Africa, as a continent, is vulnerable to a range of online criminal activities, including financial fraud, drugs and human trafficking, and terrorism. A Deloitte survey published by BuddeComm, an independent research and consultancy company , in the year 2011, found that banks in Kenya, Rwanda, Uganda, Tanzania and Zambia alone had lost US$245 million to cyber fraud which is quite a lot of money for countries without ~~a~~ highly developed banking systems. The aim of this study was to assess the efforts being made by African countries in fighting cybercrime. Towards this direction, specific structures put in place by East and West African countries were reviewed with Africa's capacity to win the fight against cybercrime as an overriding concern. The research revealed that the way forward is for Africa to learn from the experience of developed countries in fighting cybercrime. The fight against cybercrime requires coordinated effort among all stake holders such as government bodies, educational institutions, business organizations and law enforcement authorities.

Keywords Cybercrime, Africa

1. Introduction

According to computer security experts, a lot of cyber crime emanates from the African continent, and these threats spread easily because many computer systems are not properly protected. The fight against cybercrime requires a cohesive and coordinated approach, but in Africa, poverty and underdevelopment are the major causes for growth of cybercrime in the region. The potential for internet abuse in Africa is also high. This is due to the lack of security awareness programmes or specialised training for the law enforcement agencies. Many watchers are warning that Africa is becoming a major source of cyber-crimes; for example, Nigeria is ranked as the leading State in the region as the target and source of malicious internet activities; and this is spreading across the west African sub-region[4].

Cybercrimes are crimes committed on the internet using the computer as either a tool or a targeted victim[10]. Cybercrimes involve both the computer and the person behind it as victims, depending on which of the two is the main target. Hence, the computer could be looked at as either a target or a tool[10]. For example, hacking involves attacking the computer's information and other resources. When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world and human weaknesses are generally exploited.

The damage caused is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries offline. Scams, theft and other fraudulent activities have existed even before the development of high-tech equipment. The same criminal has simply been given a tool which increases his/her potential pool of victims and makes him all the harder to trace and apprehend. There are numerous crimes of this nature committed daily using the computer and the internet.

In achieving the aim of the study, assessing the efforts being made by African countries in fighting cybercrime, the authors interrogated the pervasive nature of the phenomenon of cybercrime. Factors that contributed to the thriving state of this kind of crime was looked at across the African continent, citing the East and West African blocks. The study sought to establish the need for collaboration with developed countries that achieved better results in the fight against cybercrime.

Lack of legal framework and the existence of weak infrastructures for dealing with cybercrime in the studied African countries justifies the need for such a study. The involvement of top level government officials, policy makers and implementation groups must be highlighted at all levels of discussion and coupled with cross-border collaboration, is a justifiable route for success in fighting cybercrime.

2. Methods

* Corresponding author:
hquarshie@yahoo.com (Henry Osborn Quarshie)
Published online at http://journal.sapub.org/computer

The paper interrogated the efforts being made by African countries in fighting cybercrime. This research reviewed the efforts being made by East and West African countries.

2.1. Efforts In Fighting Cybercrime In East Africa

East African countries have scaled up efforts to combat cyber crimes through a multi-stakeholder approach involving the government, industry and civil society organizations. A cyber security management task force chaired by Kenya has been coordinating activities aimed at rooting out cyber crimes in the five East African Community member countries. This taskforce deals with cyber security at legal, policy and regulatory levels.

A plan for the five East African states of Uganda, Kenya, Tanzania, Rwanda and Burundi to set up Computer Emergency Response Teams (CERTs) to fight cybercrime is under way, as countries concerned seek to involve the International Telecommunications Union's (ITU) help. The East African Communications Organisations (EACO) Congress, an umbrella body of all five regulators, will pursue ITU support for the establishment of the national CERTs.[2][7]

The five regulators will also establish a collaborative framework for the national CERTs at regional and international levels.

EACO will work to establish and harmonize Internet security policies and Internet laws in the East African region.

EACO has also adopted a proposal for telecommunications operators to form and run sectoral CERTS and nominate representatives to sit on national CERTs.

The five member states are each at different stages of developing their Internet laws, but the laws will be uniform across the board, with just a few in-country peculiarities sticking out.

Uganda's Internet security legal framework, for example, has three sets of draft laws -- the Electronic Transactions Bill, the Computer Misuse Bill and the Electronic Signatures Bill. All three pieces of legislation are in Parliament, due to be acted on before the end of the year.

Uganda's Electronic Transactions (eTransactions) Bill is meant to facilitate the development of electronic commerce in the country, and the Electronic Signatures (eSignatures) Bill will ensure transactions are carried out in a secure environment. The Computer Misuse Bill spells out computer misuse offences like unauthorized modification of computer material[2].

2.2. Efforts In Fighting Cybercrime-West Africa

The first West African Cyber Crime Summit was convened on 30th November, 2011 to 2nd December, 2011 in the Nigeria capital, Abuja. The Summit, organized by the Economic and Financial Crime commission (EFCC) in collaboration with United Nation on Drugs and Crime (UNODC), the Economic Community of West African States (ECOWAS) and Microsoft, focused on the theme, "The Fight against Cybercrime: Towards Innovative and Sustainable Economic Development". Participants from all over the world considered local and international cybercrime strategies and policies with a view to strengthening international cooperation and developing a regional road map that tackles cyber crime and fosters economic growth.[3]

Over 450 people were in attendance from across the world including Togo, Guinea, Guinea Bissau, Gambia, Ghana, Senegal, Ivory Coast, Niger, Austria, UK, France, USA, Turkey, South Africa, UAE, Tunisia and Nigeria. Various international and regional organizations were present, including United Nation on Drugs and Crime (UNODC), Council of Europe (CoE), INTERPOL, US Federal Bureau of Investigation, US Federal Trade Commission, US Department of Homeland Security, Economic Community of West African States (ECOWAS), European Union and FRANCOPOL.

The summit focused on how to:

- Position the fight against cybercrime as a national priority to help the economic development in the region.
- Provide a platform to develop capacity building with scalable and sustainable resources.
- Strengthen trust by developing partnerships among various stakeholders at the national and international level; government, civil society, academics, industry and international organizations.
- Showcase best practices and case studies of partner organization in combating cybercrime.[5]

One form of cybercrime that has become especially associated with the region is the advance fee fraud, collectively known as "Nigeria" or "419" scams. Through schemes such as fake lotteries, bogus inheritances, romantic relationships, investment opportunities or - infamously - requests for assistance from officials, scammers promise an elusive fortune in exchange for advanced payments.

In Nigeria, the federal government is fighting cyber crimes in the country with the help of some security outfits, part of which are the Economic and Financial Crime commission (EFCC), the National Security Adviser (NSA) and Nigeria Police Force. Other actors in the fight also include Nigerian Communications Commission (NCC), Department of State Service (NSS), National Intelligence Agency (NIA), Nigeria Computer Society (NCS) and Nigeria Internet Group.

World Bank and Microsoft Corporation had also enjoined the National Assembly to pass the Cyber Crime Bill in an effort to reduce the rate of internet fraud in the nation as it is damaging to the image of the nation.

Among other actions was the creation of the Directorate for Cyber security (DfC) by Nigerian Cybercrime Working Group (NCWG), as a permanent autonomous body within the Office of the National Security Adviser (ONSA).

The recently created computer Crime Prosecution Unit (CCPU) for the Office of the Attorney General by the presidency is also another act set to curb cybercrime.

The DfC is mandated to implement the National Cyber-security Initiative (NCI). It's also charged with the responsibility of drafting all relevant laws for the protection of computer systems and networks in the nation; such laws would be passed by the National Assembly.

There has also been a legal framework with the goal of protecting critical information infrastructure in Nigeria. The legislation also seeks to criminalize conducts against ICT systems and conducts utilizing ICT systems to carry out unlawful/illegal acts.[9]

In line with Ghana's aim of becoming the hub of the information superhighway on the west coast of Africa, the government in 2008 passed the Electronic Transactions Bill to protect private rights of Internet users and owners' websites.[6]

3. Conclusions

In East Africa, a taskforce comprising government, industry and civil groups have been set up to deal with cyber security at the three levels of legal, policy and regulation. Also Computer Emergency Response Teams (CERTs) have been set up in five East African states to fight cybercrime with other collaborative partners such as ITU and EACO.

In West African countries, led by ECOWAS, policies have been initiated in capacity- building, prioritising cybercrime issues and developing networks across the borders as a definite way in fighting cybercrime.

The study can confirm that cybercrimes have increased in sophistication and frequency. Individuals, business organizations and government bodies are all affected by cybercrime. Cybercrime also poses threat to the national security and the continent as a whole. Cyber attacks are a recurrent phenomenon in Africa due to infrastructural, legal and policy loopholes. There is no clear legislation. Some countries have not made the attempt to look at it yet.

The way forward is that, Africa should learn from the experience of developed countries in fighting cybercrime.

4. Recommendations

There is the need to develop a common platform to address cyber security since cybercrime crosses borders and cannot be fought by one country. As a region, Africa must begin to cooperate to deal with cyber threats at national and regional levels. Africa should establish a body to monitor and report cybercrimes across borders.

The approach should also involve governments, industry, civil society organizations and to a large extent security agencies. The fight against cybercrime requires coordinated effort among all stake holders such as government bodies, educational institutions, business organizations and law enforcement authorities.

Lawmakers must be well trained and sensitised to help implement legislation that addresses cyber threats at all levels,

Africa needs strong Information and Computer Technology institutions to train cyber security experts with a strong expertise in system administration, security audit, forensic investigation, information security and software development to deal with the future challenges of cybercrime.

REFERENCES

[1] Buddecomm African Research, The fight Against Cyber Crime in Africa. www. buddeblog.com.au.2012.

[2] East Africa Seeks Joint Approach to Combat Cyber Crimes. www. hallafrica.com. 2012.

[3] Eccuni u, West Africa to Fight Cybercrime - Online Computer Training Can Create IT Security Awareness, www.EzineArticles.com.2011.

[4] Fighting Cybercrime in Nigeria, www.thorpepodcast.wordpress.com.2011.

[5] *First regional event on combating cybercrime held in Nigeria*, www.waccs.net.*2011.*

[6] Ghana News Agency, Fighting cyber crime in Africa. 2010.

[7] James Gashumba, East Africa region moves to curb cyber crime, Buddecomm Africa research. 2012.

[8] Jeff Lule. Africa joins fight against Internet crime, www.newvision.co.ug. 2010.

[9] Jummai Umar-Ajijola, Citizenship Manager Lead, Microsoft Anglophone West Africa. Fighting Cybercrime in Nigeria. 2011.

[10] The Indian Law Institute. Introduction to the cyber world and cyber Law. 2010.