NATIONAL STRATEGIES ON CYBERCRIME SECURITY SKILL AND MAN POWER DEVELOPMENT AS A REMEDY TO CYBERCRIME IN NIGERIA

BY

DR AKPAN, E. EBENEZER, *FCICN, AP*
CORPORATE INSTITUTE OF RESEARCH AND COMPUTER SCIENCE
140 IKOT EKPENE ROAD
UYO, AKWA IBOM STATE.

ABSTRACT

The study examines the national strategies on cybercrime security skill and man power development as a remedy to cybercrime in Nigeria. One specific research objective was formulated to guide the study. The research design was survey design. The population of this study comprised all the personnel of; NCC, ICPC, EFCC, NPF, NCWG, NCIC, CBN, and Commercial banks from which a sample of 350 respondents was chosen using stratified sampling method. The instrument known as "Cybercrimes and combating strategies Questionnaire (CCSQ)" was used to collect data from the respondents. Data were collected and analyzed. From the findings of the data collected and analyzed, it was shown that highest percentage of the respondents affirmed very great extent of the national strategy on cyber security skill & manpower development helping in combating cybercrimes in Nigeria and that National strategy on cyber security skill and manpower development significantly helps in combating cybercrimes in Nigeria. One of the conclusion was that the controls of operational cyber security of the energy utilities are not applied in compatibility with the risks predicted and regularly tested, monitored and revised and one of the recommendation was that the Nigerian Police should be ensure that proper use of network information technology, the knowledge on mobile network devices, as well as the length of internet use were should be considered and carefully put in place to avoid danger.

KEYWORDS: National strategy, cyber security skill, manpower development, cyber crime

INTRODUCTION

The proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way in which we socialize and do business. While overwhelmingly positive, there has also been a dark side to these developments. There is no denying the fact that the internet has changed the way we do things. It has become a driving force in every aspect of human endeavour. The internet has become an invaluable tool for governments, businesses, military, associations and individuals. Cyberspace is constantly evolving, so too is the threat of cyber crime on national security, prosperity and quality of life of the citizenry and the world as a global village. Just like governments of all sovereign nations, the government of Nigeria is committed to protecting Nigerians from the threat of cybercrime.

According to Okeshola (2013), cyber crime is the most complicated problem in the cyber space and many nations are battling to protect their cyber space from criminals, for national security and integration. Cyber crime refers to unlawful practices carried out using computers, electronic and ancillary devices. It involves disruption of network traffic, email bombing, distribution of viruses, identity theft, cyber stalk and cyber squatting (Fanawopo, 2004). (Maitanmi, 2013) asserts that cybercrime is a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam

mailing and the likes. Cyber-crime evolves from the wrong application or abuse of internet services. Since the advent of the internet, cybercrime has become a recurring decimal in Nigeria. Cyber crime is the most complicated scourge in the cyber space. Many nations are battling to protect their cyber space from criminals, for national security and integration. As a result of this, efforts are being made by governments to protect their citizens and image from online crime. Ifukor (2006) stated that cyber crime includes all forms of crime committed through the use of the internet. They are referred to as internet fraud. This means using one or more components of the internet such as chart rooms and emails among others, to present fraudulent solicitation to prospective victims or to defraud individuals or financial institutions. According to Laver (2005) drug cartels, organized crime, international money launderers and computer hackers are unleashing themselves on the information high ways and they are becoming even more successful. There is also a mounting concern about cyber terrorism through the use of computers sabotage. This is one of the fastest, growing criminal activities on the planet. Organized crimes are using cyber space more frequently to target credit cards information, personal and financial details for internet fraud. In Nigeria, and other parts of Africa, the perpetrators of this illegal act have even upgraded their nefarious activities from the physical to the mystical, in what can be described as Yahoo- Yahoo. This involves using occult powers to target individuals for their scams. This, undoubtedly, has increased Nigeria`s notoriety in the world rating on cyber- related offences (Atili, 2011). The need to improve combat on cyber crime and protect critical and delicate information is extremely necessary for every nation's security and economic well-being. The Nigerian government has adapted different measures in combating cybercrime and salvaging the image of Nigeria from the negative consequences of cyber crime but how effective has it been? This study hereby examines the major strategies in combating cyber crime in Nigeria.

Statement of the Problem

In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gain in productivity, efficiency and communication, they also create a loophole which may totally destroy an organization. Recently, cybercrime has turned into a growing threat to all companies worldwide, and there is a need to address the issue for the protection of the companies and their stakeholders. As a result of cyber-attacks, public trust and investors' confidence have been reduced towards banks, companies, their directors, managers and auditors. The Nigerian Government set up the cybercrime committee which formed the Nigerian Cybercrime Working Group (NCWG), so as to accelerate the implementation of its Cybercrime research efforts; the Nigerian National Assembly has also passed the Cybercrime Bill into law. This research hereby tends to assess

national strategies on cybercrime security skill and man power development as a remedy to cybercrime in Nigeria.

Objectives of the Study

The main purpose of this study is to examine national strategies on cybercrime security skill and man power development as a remedy to cybercrime in Nigeria.

Specifically, the study seeks to achieve the below objective:

i. To find the extent to which national strategy on cyber security skill & manpower development helps in combating cybercrimes in Nigeria.

Research Questions

The below research question will be answered:

1. To what extent does national strategy on cyber security skill & manpower development help in combating cybercrimes in Nigeria?

Hypotheses

The below hypothesis was formulated for the study. The hypothesis to be tested in this study is stated in the null form.

1. National strategy on cyber security skill and manpower development significantly helps in combating cybercrimes in Nigeria.

Literature Review

Strategies of Combating Cyber Crime in Nigeria

According to Wada and Odulaja (2013), learning the different types of cyber-crimes and ways that can help combat these crimes is an important step in helping to catch these cyber criminals and keep them from continuing to commit cybercrimes against others. Cybercrime cannot be easily and completely eliminated, but can be minimized. However, collaborative efforts of individuals, corporate organization and government could go a long way to reduce it to a minimal level. Firms should secure their network information. The followings are ways to combat cybercrime.

1. Government should ensure that their laws apply to cybercrimes. African countries are bedeviled by various socio-economic problems such as poverty, AIDS, fuel crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cybercrime. Nevertheless, it is important that Nigeria as a nation take measures to ensure that its penal and procedural laws are adequate to meet the challenges posed by cybercrimes. The Government must ensure laws are formulated and strictly adhered to (Wada and Odulaja, 2013).
2. Individuals should observe simple rules. Individuals on their part should ensure proper anti-malware protection on their computer systems; they should be encouraged to avoid pirated software, never to share their Personal Identification Number (PIN), bank account, email access code to unknown persons, and never disclose any confidential information to anybody as none of these networks were designed to be ultimately secure. Ignore any e-mail requiring any financial information. All ill intended spam must be reported immediately to the appropriate authorities. Telecommunication Regulatory Agencies should enhance security on internet service providers' server in other to detect and trace cybercriminals. This will create job opportunities for the unemployed youths, thereby reducing the cybercrime menace. The success in harnessing cyberspace will help Nigerians achieve unprecedented personal productivity and prosperity. Government must take immediate steps to protect cyberspace from becoming a criminal haven. Cyber criminals must be denied the anonymity they are seeking, while at the same time protecting the safety and privacy of Nigerians.

Cyber crime awareness allows the relationship between user's action or inaction and cybercrimes attacks or commission to become clear. The awareness makes it easier for the users and system administrators to be able to maintain and monitor an intrusion detection system that requires investigation. The first line of defense in cybercrime is users' awareness of the existing dangers or threats. From a research done in United States of America by Ponemon Institute in 2010, lack of awareness about cyber threats among employees and users of internet was pointed out as the number one cause of data breach in an organization. Informed internet users who can recognize incidences of computer crime are more likely to be proactive rather than reactive when going online. An informed user is likely to unearth other situations that can decrease performance of a computer system and cost money; thus

these situations can be dealt with before damage is caused. Computer crime awareness will generally tend to increase knowledge and better computer practice by individual users of computers. “It is important that Management in an organization obtain a feedback on user awareness of computer security practices in order to develop strategies towards ensuring the effectiveness of the policy” (Antwi-Bekoe and Nimako, 2012). Any organization that has a policy on the use of the organization computer systems will once in a while require getting feedback on how well the end users of the systems are aware of the issues likely to compromise the organization computer systems; and how well they adhere to the policy.

Cyber Security Skill & Manpower Development Strategy

Chen, Shaw and Yang (2006) carried out an empirical study of 300 employees in the public and business sectors of Hungary to assess their level of Cyber security skill and manpower development against cybercrime. The level of digital literacy was measured and assessed by several questions relating to several areas in the questionnaire. In order to survey the use of network information technology, knowledge on mobile network devices, as well as the length of internet use, was questioned. Hardware skills were determined by questions aimed at the knowledge about storage devices, and the duration of computer use. The level of software skills was measured by questions about the knowledge on computer installation and deployment. Finally, general information security knowledge was assessed by questions relating to computer viruses and cybercrime. They found that due to the low level of information security awareness, some parts of the micro and small-sized enterprises are in need of immediate changes in terms of organizational operations. The deficient knowledge of employees about information security gives room for grave concern at several local government organizations. Our sample also indicated that people with higher level of digital literacy show a higher level of information security awareness both in the business and the public sector. Also, poor level of information security awareness was measured in microenterprises and small-sized enterprises in the business sector, and non-profit local government organizations in the public sector. The employees belonging to this group are partly aware of the dangers and they know in most cases that certain security principles should be met but they are in need of further education on the subject. Some of them are neither aware of the dangers and safety principles, nor of the security regulations in their workplace at all.

METHODOLOGY

Research Design

The research design to be used for this study is the survey design. The design enabled a large population to be sampled such that the result of the sample can be generalized over large area or population. In this research design, questionnaire will be used to gather data for the study.

Area of stud

The study areas were Jigawa and Kano states which are among the thirty six (36) states of the Federal Republic of Nigeria.

Population; Sample and Sampling Techniques

The population of this study comprised all the personnel of; NCC, ICPC, EFCC, NPF, NCWG, NCIC, CBN, and Commercial banks that are involved directly or indirectly in the fight against cybercrime. The population covered the personnel’s of those departments that

have direct relevance within the study area. These are chosen because personnel's of these agencies understand the nature of cybercrime with their associated problems. They have the training and intellect to identify and analyze the problems, and proffer meaningful solutions.
A sample of 350 respondents was chosen using stratified sampling method from the above government agencies responsible for designing and implementing cyber security strategies and implementation, and the general public who are victims of cybercrime.

Method of Data Collection
Data for this study were collected from both primary and secondary sources using well-structured questionnaire (instrument). This were done personally in collaboration with five trained research assistants who will be carefully selected and trained for the exercise by the researcher.

Instrumentation
The researcher developed an instrument tagged: 'Cybercrimes and combating strategies Questionnaire (CCSQ).

Techniques for Data Analysis
This study used descriptive statistic such as percentage analysis to analyze the data in respect of the research questions. However, for the hypothesis the researcher used Chi-Square to test it. Test for significance was done at 0.05 alpha level.

Decision rules
When the calculated result is either equal to or greater than the critical value, the result will be considered significant but if less, the result will be considered not-significant.

Method of Data Analysis
Descriptive statistics was used to answer the research questions, while chi-square analysis was used in testing the hypothesis.

Data Analyses and Results

Research Question

To what extent does national strategy on cyber security skill & manpower development help in combating cybercrimes in Nigeria? Table 1 was used to answer the research question.

Table 1:

Descriptive analysis of the extent to which national strategy on cyber security skill & manpower development helps in combating cybercrimes in Nigeria

National strategy on cyber security skill & manpower development	Freq	%
Very Great Extent	117	33.43
Great Extent	112	32
Average	57	16.29
Low Extent	41	11.71
Very Low Extent	23	6.57
TOTAL	350	100

Source: Field Survey

The result in Table 1 shows the extent to which national strategy on cyber security skill & manpower development helps in combating cybercrimes in Nigeria. From the result, it was observed that 117(33.43%) of the respondents affirmed very great extent of the national strategy on cyber security skill & manpower development helping in combating cybercrimes in Nigeria while 23(6.57%) of the respondents affirmed very low extent of the national strategy on cyber security skill & manpower development helping in combating cybercrimes in Nigeria.

Hypothesis

The Null hypothesis states that National strategy on cyber security skill and manpower development significantly helps in combating cybercrimes in Nigeria. To test the hypothesis, chi-Square analysis was performed on the data (see table 2)

Table 2:

Chi-square analysis of National strategy on cyber security skill and manpower development significant helps in combating cybercrimes in Nigeria

Cyber Security Strategies	Observed Freq	Expected Freq	X^2
Very great extent	117	70	
Great extent	112	70	
Average	57	70	102.74*
Low extent	41	70	
Very low extent	23	70	
TOTAL	**350**	**350**	

***Significant at 0.05 level; df = 4; Critical = 9.49**

Table 1 shows the calculated X^2-value as (102.74). This value was tested for significance by comparing it with the critical X^2-value (9.49) at 0.05 levels with 3 degree of freedom. The calculated X^2-value (104.74) was greater than the critical X^2-value (9.49). Hence, the result

was significant. The result therefore means that National strategy on cyber security skill and manpower development significantly helps in combating cybercrimes in Nigeria. The significance of the result caused the null hypothesis to be rejected while the alternative was accepted.

Discussion of Findings

The results of the data analyses in tables 1 and 2 were significant due to the fact that the calculated X2-value (102.74) was greater than the critical X2-value (9.49) at 0.05 level with 4 degree of freedom. The result implies that National strategy on cyber security skill and manpower development significantly helps in combating cybercrimes in Nigeria. The result therefore was in agreement with the research study of Bodeau and Graubart (2010) who carried out a study with the aim of building a theoretical-empirical model of cyber security governance and risk management and testing it along with academic experts and professionals from the energy sector. The significance of the result caused the null hypotheses to be rejected while the alternative was accepted.

Conclusions

Based on the findings of the research work, it was concluded that National strategy on cyber security skill and manpower development significantly helps in combating cybercrimes in Nigeria, but that the controls of operational cyber security of the energy utilities are not applied in compatibility with the risks predicted and regularly tested, monitored and revised.

Recommendations

Based on the findings of the research, the following recommendations are deemed necessary:

1. Controls of operational cyber security of the energy utilities should be applied in compatibility with the risks predicted and regularly tested, monitored and revised.
2. The Nigerian Police should ensure that proper use of network information technology, the knowledge on mobile network devices, as well as the length of internet use, should be considered and carefully put in place to avoid dangers.

REFERENCES

Antwi-Bekoe. E. & Nimako .G. S. (2012) "Computer Security Awareness and Vulnerabilities: An Exploratory Study for Two Public Institutions in Ghana" *Journal of Science and Technology* Vol.1 No. 7, July, 2012 pp 358 –375

Atili, R. S. (2011) *Cybercrime and Telecommunication Law.* Rochester Institute Of Technology USA.

Bodeau, N. A. & Graubart P. W. (2010) *Cyber Crime Embarrassing for Victims*. Retrieved September 2011 from http//www.heraldsun.com.au

Fanawopo, R. D. (2004) Scene of the Cyber crime: *Computer Forensics Handbook*. Syngress Publishing Inc. 88 Hingham Street, USA.

Ifukor, G. (2006) Retiree in Trouble over Internet Fraud. *Economic and Financial Crime Commission, Vol1, No. 2*

Laver, S. E. (2005) Improving Cyber Security and Mission Assurance Via Cyber Preparedness Cyber Prep Levels. *In IEEE Second International Conference on Social Computing* 1147-1152.

Maitanmi, O. S. (2013), Impact of Cyber Crimes on Nigerian Economy, *The International Journal of Engineering and Science* IJES, vol. vol 2(4), 4551.

Okeshola, F. B. (2013) The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, *Nigeria American International Journal of Contemporary Research*, vol. 3(9), 98-114.

Shaw, T. K. & Yang, S. M. (2006) Cyber Crime and Commercial Fraud; A Nigerian Perspective. *A paper presented at the Modern Law for Global Commerce*, Vienna 9th – 12th July.

Wada, F. R. & Odulaja G. O. (2013) *Assessing Cyber crime and its Impact on E-Banking in Nigeria Using Social Theories.*