AN INQUIRY INTO THE AWARENESS LEVEL OF CYBER SECURITY POLICY AND MEASURES IN NIGERIA

Kayode S. Adewole  
Department of Computer, Library and Information Science  
Kwara State University, Malete, Nigeria  
kayode.adewole@kwasu.edu.ng

Rafiu M. Isiaka  
Department of Computer, Library and Information Science  
Kwara State University, Malete, Nigeria  
abdulrafiu.isiaka@kwasu.edu.ng

Raphael T. Olayemi  
Department of Computer, Library and Information Science  
Kwara State University, Malete, Nigeria  
rapheal.olayemi@kwasu.edu.ng

Abstract - Cybercafé administrator used to be a major player in cybercrimes control in conjunction with security operatives, until the advent and popularity of internet service by the GSM operators in Nigeria. This study investigates the level of awareness of the existing cyber security measures among the cyberspace users and the level of enforcement of these measures by the cybercafé administrators and government security agencies within Ilorin metropolis, Kwara State, Nigeria. Questionnaires were administered to 10 cybercafé administrators and 100 cyberspace users in both University of Ilorin and Kwara State University. The findings show that 76% of the respondents are not aware of any existing cyber security policies, or any standard agency or outfit charged with the responsibility of enforcing cyber security policies. 80% of the cybercafé administrators agreed that most of the cyberspace users overlook the cyber security measures being used in the cybercafés. The paper suggested the way forward, presents various preventive and control measures of cybercrimes most especially the one being committed by the GSM users when accessing the internet and observed that if nothing urgent and precise is done, the combined effect of the present world economic meltdown with the raging cybercrimes will cripple the nations’ fragile political and socio-economic systems. This will no doubt, make the nations’ effort at becoming one of the twenty top world economies by 2020, a mission impossible or a mirage. The need for inclusion of cyber ethics into citizenship education in Nigeria, and the need for establishment of relevant cyber security agencies were recommended among others.

Keywords: Cyber policy, cybercrimes, cyber security, cyber ethics, spoofing, cyberspace, socio-economic systems, cripple.

INTRODUCTION

In this age of technology and communication convergence, you cannot help but be impacted by technologies and innovations that center on computers, cell phones and the internet. But as we revolve our daily lives with these technologies, there are times that we set out to feel truly distrust about our own safety, be it physical safety or the security of our personal hardware and software. The advent of digital technology gave birth to modern communication hard-wares, internet service and powerful computer systems to process data. Hence, cyberspace has provided a safe haven for internet platform, which has created geometric growth and accelerated windows of opportunities for businesses and the removal of
economic barriers hitherto faced by nations of the world [5]. People from diverse areas of human endeavour can now freely access and utilize the advantages offered by internet platform. However, information technology revolution associated with the internet in Nigeria has brought about a new wave of cybercrimes. Cybercrime or computer crime can broadly be defined as criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (cybertheft), and electronic fraud [5]. Hence, the need for cyber security policies and measures. Cyber security is in fact protecting your personal information or any form of digital asset stored in your computer, on the internet or in any digital memory device. There are different forms of threats that could be encountered when using the cyberspace and each one has its own level of seriousness which require its own level of solutions. The higher the degree of terror, the more advanced or complicated the approach to enforce safety measures to protect yourself. These could range from simple malevolent codes, otherwise called malware and spyware to serious virus that can erase the whole contents of your computer and hackers that can access and use your personal data for their own personal gain. This according to [8] is “harmful acts committed from or against a computer or a network”. These are some of the dangers this paper tried to address by recommending various measures of combating them. This paper also investigates the level of awareness of the existing cyber security policies among the cyberspace users and the level of enforcement of these policies or measures by the cybercafé administrators and government security agencies.

II. RESEARCH METHOD

Questionnaires were distributed to 10 cybercafé administrators and 100 cyberspace users in both University of Ilorin and Kwara State University in order to ascertain the level of awareness of the existing cyber security policies or measures and the level of enforcement of these policies by the cybercafé administrators and government security agencies. Also, we critically reviewed various types of cybercrimes, their socio-economic consequences and the damage or negative impact it had on the image of Nigeria as a nation.

A. Cybercrime and Cyber Security Policy

There is no doubt that cybercrime is an image nightmare for Nigeria. The decision of the former President Olusegun Obasanjo to constitute a working group, the Nigeria Cyber Crime Working Group (NCWG) is an indication that cybercrime, especially internet 419 is a source of concern and embarrassment [3][9].

This internet 419 is usually referred to in Nigeria as “yahooyahoo business”. Some perpetrators of this crime are called “yahoo boys” who take advantage of e-commerce system available on the internet to defraud unsuspected victims who are mostly foreigners. [4] stated that “Among the numerous crimes committed daily on the Internet, Nigeria and some other nations on the West African coast are reputed to be at the forefront of sending fraudulent and bogus financial proposals all over the world. The damaging implications resultant on the image of the Nigerian nation and the negative impact this trend has had on e-mail infrastructures are clearly evident.” They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. According to [5] in their recent research on cybercrime in Nigeria stated that “sometimes they pose to have financial institution where money can be loaned out to prospective investors”. In this regard, so many persons have been duped in Nigeria. These fraudulent acts has violated existing legislation governing the economic activities of
government and its administration to includes any form of fraud; cyberlaundering, cybertheft, cybervandalism e.t.c. According to media reports in Nigeria, a bill is presently being prepared to deal specifically with the menace of cybercrime. This indeed means that no serious impact has been made by our law enforcement agencies to arrest and prosecute these criminals. Nigeria is a place where computer can be used to commit all sorts of crimes without prosecution, as there is no law on cybercrime [3]. Nigerian law enforcement agencies are basically technology illiterate; they lack computer forensics training and often result to conducting police raids on Internet service site mainly for the purpose of extortion. It is very common for the police to demand bribe from cybercafé operators where suspicious activities are taking place. There are so many reports on Nigeria cybercrime situations that well-meaning Nigerians are no longer comfortable with anymore. These reports are damaging the dignity of our country as a sovereign nation. They are humiliating and injuriously affecting our international image, our business, our mental psychology and even our children [5]. However, these reports points towards the fact that Nigeria is operating on a weakened technology platform and digitally illiterate environment that is in urgent need of expert solution, laws on cybercrime, and indeed effective and efficient cyber security policies.

There are various forms of cybercrime which include: malware, spoofing, cyber contraband, child pornography, cyberlaundering, cybertheft, cyberterrorism, cybervandalism, spam, keylogging, etc.

**Malware:** Malware, short for malicious software, (sometimes referred to as pestware) is a software designed to secretly access a computer system without the owner's informed consent.

**Spoofing:** Spoofing or decoying is the practice of inundating online networks with bogus or incomplete files of the same name in an effort to frustrate the user.

**Cyber Contraband:** This is transferring illegal items through the internet (such as encryption technology) that is banned in some locations.

**Child Pornography:** This is the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

**Cyberlaundering:** Is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

**Cybertheft:** This is an act of using a computer to steal. This includes activities related to; breaking and entering, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy.

**Cyberterrorism:** Premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of computer technology.

**Cybervandalism:** Damaging or destroying data rather than stealing or misusing them (as with cybertheft) is called cybervandalism.

**Spam Message:** Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. The most widely recognized form of spam is e-mail spam [7].

**Keylogging:** Keystroke logging (often called keylogging) is the practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

**B. NCWG and Directorate for Cybersecurity (DFC)**

Nigerian Cybercrime Working Group was inaugurated by the former President Olusegun Obasanjo on March 10, 2004 [6]. Since the inauguration of the NCWG, some years back, the body has very little to show. In short, the only significant accomplishment of the NCWG is a document (Nigerian Cybercrime Bill) which may one day become the Nigerian Cybercrime Law [6]. NCWG is made up of National Security Adviser (NSA), Nigerian Communications Commission (NCC), Department of State Services (DSS), National
Intelligence Agency (NIA), Nigeria Computer Society (NCS), Nigeria Internet Group (NIG), Internet Services Providers’ Association of Nigeria (ISPN) and National Information Technology Development Agency (NITDA).

According to [1][2], Directorate for Cybersecurity (DfC) was created as a permanent autonomous body within the office of the National Security Adviser (NSA) to takeover all assets and liabilities of the NCWG, including all uncompleted projects. [1][2] further stated that the main mandates of DfC are to develop and implement a National Cybersecurity Policy for Nigeria, drafting and/or proposing all relevant laws required to be enacted by the National Assembly for the security of computer systems and networks in Nigeria pursuant to our national strategies on cybersecurity, establishing a National Computer Emergency Readiness and Response Mechanism with Early Warning System (EWS) and alerts for all cyber related emergencies in the country, establishing a National Computer Forensics Laboratory and coordinating the training and utilization of the facility by all law enforcement, security and intelligence agencies, creating requisite technical capacity across law enforcement, security and intelligence agencies on cybercrime and cybersecurity, developing effective framework and interfaces for inter-agency collaboration on cybercrime and cybersecurity, establishing appropriate platforms for public private partnership (PPP) on cybersecurity, coordinating Nigeria’s involvement in international cybersecurity cooperation to ensure the integration of our country into the global frameworks on cybersecurity, executing such other functions and responsibilities as it shall consider necessary for the general purpose of promoting cybersecurity in Nigeria and fostering a framework for critical information infrastructure protection in the country. These two bodies have performed below expectation in fighting cybercrime in Nigeria. Therefore, as measures, there is need for enacting cyber law, creating public awareness, institutional capacity building, and public private collaboration to mention just a few.

III. RESULTS AND DISCUSSION

To what extent are Ilorin cyberspace users aware of the cyber security laws or policies or of any government agencies charge with the responsibility of formulating or implementing cyber security laws or policies? The data obtained from the responses of all 100 cyberspace users in order to test their level of awareness of cyber security laws or policies shows that 76% of the respondents were not aware of any cyber security laws or policies. Chi-Square was used to analyze the distribution of this percentage based on the frequency of their visit to cybercafé. The result of this analysis is shown in Table 1 and 2 below:

### Chi-Square Test

#### Table 1: Frequencies- Frequency of Visit

<table>
<thead>
<tr>
<th>Freq. of Café Visit</th>
<th>Observed N</th>
<th>Expected N</th>
<th>Residual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occasionally</td>
<td>12</td>
<td>19.0</td>
<td>-7.0</td>
</tr>
<tr>
<td>Daily</td>
<td>23</td>
<td>19.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Weekly</td>
<td>31</td>
<td>19.0</td>
<td>12.0</td>
</tr>
<tr>
<td>Monthly</td>
<td>10</td>
<td>19.0</td>
<td>-9.0</td>
</tr>
<tr>
<td>Total</td>
<td>76</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Test Statistics

<table>
<thead>
<tr>
<th>Frequency of Visit</th>
<th>Chi-Square</th>
<th>df</th>
<th>Asymp. Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>15.263</td>
<td>3</td>
<td>.002</td>
</tr>
</tbody>
</table>

Chi-Square test with degrees of freedom (df) of 3, the Chi-Square distribution table was used to get the table value using confidence interval of 0.050 and the corresponding table value is 7.815. Having shown that the calculated Chi-Square value is greater than the table value, this emphasized that the frequency of visit of cyberspace users to the cybercafé does not affect their level of awareness of cyber security laws or policies.

To what extent do the cyberspaces users comply with the cyber security measures put in place by the cybercafé administrators?

The responses of the 10 cybercafé administrators who were given questionnaire are summarized in the following tables:
Table 3: Administrators’ responses to security measures available in cybercafé

<table>
<thead>
<tr>
<th>Paper notice</th>
<th>Scrolling marquee on PC</th>
<th>Disabling of office application</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 4: Administrators’ responses to various Yes/No questions

<table>
<thead>
<tr>
<th>Questions</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do your customers comply with your cyber security measure(s)?</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Have you ever had a course to report a customer to a security agency?</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Will you be willing to handover any erring customer to the appropriate security agency?</td>
<td>1</td>
<td>9</td>
</tr>
</tbody>
</table>

From table 4 above 80% of the cybercafé administrators agreed that most of the cyberspace users overlook the cyber security measures being used in the cybercafé.

In this regard, their responses to the various questions in the questionnaire show that the level of awareness of NCWG and Directorate for Cybersecurity (DfC) or any of their policy by the cyberspace users in Ilorin, Kwara State, Nigeria is very low since only 24% out of 100 respondents claimed of ever heard of such government bodies. Also, 90% of the cybercafé administrators stated that they cannot force cyberspace users to comply with their measures since the business is no more lucrative as it was in the years back and they are not encouraged by the way the law enforcement agencies handled victims of previous raids.

IV. CONCLUSION AND RECOMMENDATIONS

From our investigation on cybercrime we observed its threat to the economy of a nation and even peace and security. To fight cybercrime, those involved have to spend time to learn how cybercrime operates and then devise strategies and policies to fight the menace. According to [10] “Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures”. This indeed emphasizes the need for the government security agencies to note that, learning in IT is not one-off but lifelong. One cannot fight today’s crime with yesterday’s technology. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime require holistic approach to combat this menace in all ramifications, not just addressing the cybercafés alone. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire. Enforcement can only work if it avoids harassment, abuse of privacy and extortion.

We also recommend other measures such as; replacing SIM card with Universal Subscriber Identity Module (USIM) that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user, enforce SIM card registration on all the GSM users in Nigeria so that it will be easier to trace any crime perform using mobile phones, keeping track of web sites accessed on the GSM phones by the GSM service providers through the integration of a cybercrime monitor software on all the GSM phones, keeping database of languages of spammers and designing of automatic alert notification to the GSM users informing them if a malicious activity is detected, inclusion of cyber ethics into citizenship education in Nigeria, and the need for establishing relevant cyber security agencies and empowering the existing ones such as Directorate for Cybersecurity (DfC) currently in the office National Security Adviser (NSA) and the need to replicate same across the state and local government in the federation.

REFERENCES

Adewole Kayode Sakariyah is currently a lecturer in the Department of Computer, Library and Information Science, College of Information and Communication Technology, Kwara State University, Malete, Nigeria. He obtained National Diploma in Computer Science from Federal Polytechnic, Ede, Nigeria, Bachelor of Science Degree in Computer Science from University of Ilorin, Nigeria. His research focuses on Data Mining and Software Engineering.

Isiaka, R.M. is a Lecturer in the Department of Computer, Library and Information Science, Kwara State University, Malete, Nigeria. His research is in the area ICT4D with specific interest in e-learning, e-Health, e-Governance, Software Engineering and information security. He obtained B.sc. Computer Science from Usmanu Danfodio University, Sokoto and M.sc. Computer Science from University of Ibadan, Nigeria. He is a member of Nigerian Computer Society (NCS) and Computer Professional Registration Council of Nigeria (CPN).

Olayemi, R. T. is a Lecturer in the Department of Computer, Library and Information Science, Kwara State University, Malete, Nigeria. He obtained B. Sc. Computer Science from University of Ilorin, and M. Sc. Computer Science from University of Lagos, Nigeria. His Research is in the area of Operating System and Database Management.