Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2020. Vol. 14(1): 283–299. DOI: 10.5281/zenodo.3753223
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment

Ogochukwu Favour Nzeakor[1]
Michael Okpara University of Agriculture, Abia State, Nigeria

Bonaventure N. Nwokeoma[2] **& Peter-Jazzy Ezeh**[3]
University of Nigeria, Nsukka, Nigeria

Abstract

Using questionnaire, and In-depth Interview, data were collected from 1,031 staff and students of selected tertiary institutions in Imo State, Nigeria in order to evaluate the pattern of public awareness of cybercrime. It was found that (1) the level cybercrime awareness was very high(N=915; 89%); (2) the knowledge of cybercrime menace appeared very superficial because majority (78%; N=804) of the respondents tend to be only informed of computer-related/assisted category of cybercrime; while as low as 22% (227) were aware of only computer-focused cybercrime categories; (3) cybercrime awareness appeared to be gender sensitive in the sense that more males (91%; N=347) than females respondents (88%; N=572) tend to be aware of cybercrime; (4) there seems to be a positive relationship between level of education and awareness of cybercrime- in the sense that the highly educated Internet users tend to be more informed (N=332; 92%) about online criminal activities that the lowly educated ones (N=583; 87%); and (5) the level of cybercrime awareness increases (N=305; 97%) as Internet users get older. It was recommended that more effective and holistic cybercrime awareness campaigns, targeted more on the women and children, should be embarked upon by the stakeholders.

Keywords: Level of Awareness, Category of Cybercrime Awareness, Superficial Awareness, Socio-Demographic Trend of Awareness, Depth of Awareness.

Introduction

Crime, as a component of deviance, is relative to time and space. In this sense, crime changes in tandem with a given epoch and society due to changing social, economic, political and geographical conditions (Haralambos & Holborn, 2004; Igbo, 2007). Consequently, the current information society, amidst its numerous positive features,

[1] Peace and Conflict Studies Unit, School of General Studies, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria. Email: nzeakor.ogochukwu@mouau.edu.ng

[2] Department of Sociology & Anthropology, University of Nigeria, Nsukka, Nigeria. Email: peter-jazzy.eze@unn.edu.ng

[3] Department of Sociology & Anthropology, University of Nigeria, Nsukka, Nigeria. Email: bonaventure.nwokeoma@unn.edu.ng

ushered in cybercrime to the contemporary world. Cybercrime is conceptualized as any criminal activity in which computers or networks are a tool, a target or a place of such activity (Mali, 2008; Reyes, 2007; Finnie et al. 2010; Malby, Mace, Holterhof, Brown, Kascherus & Ignatuschenko, 2013; Siegel, 2010; Gercke, 2012). Cybercrime also has unique characteristics- such as ambiguity, dynamism, speed of occurrence, anonymity, extraterritoriality, etc., that make its control and prevention a daunting task amongst the community of nations.

Although the criminal abuse of information technology has a very long history in the literature, but its devastation has equally been on increase- defiling several efforts towards curbing it. For instance, the first recorded cybercrime took place in the year 1820: the sabotage of Joseph-Marie Jacquard's loom by his employees in France (Mali, 2008, p. 4). Since then, the impact of cybercrime has been overwhelming- with its victimizations increasing on daily basis as evidenced by empirical studies. For instance, the strategic study by the United Nations Office on Drugs and Crime in 2012, found that individual cybercrime victimization is significantly higher than conventional crimes. Victimization rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorized access to an e-mail account, vary between 1 and 17% of the online population. Individual cyber crime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries (Malby, et al, 2013, p. xviii-1).

In the same light, Harvey (as quoted in Yar, 2005) opined that the information networks seemingly renders individuals vulnerable to an array of potentially predatory others who have their targets within instantaneous reach, unconstrained by the normal barriers of physical distance. In the same vein, Siegel, (2010, p. 486) concluded that "it may even be possible that the recent crime drop is a result of cybercrime replacing traditional street crime. For instance, instead of robbing a bank at gunpoint, a new group of contemporary thieves finds it easier to hack into accounts and transfer funds to offshore banks".

In the light of the above, the Global Cyber Security Agenda advanced seven main strategic goals towards curbing cybercrime scourge; including: legal, technical, organizational/institutional, public-private partnership (third-party policing), international cooperation, law enforcement/capacity building, and public awareness strategies (Gercke, 2012; Malby et al., 2013).

On the case of cybercrime awareness strategy, though there are limited studies on this, but a very few studies, like those of Gercke, (2012), Malby et al., (2013), Boateng et al., (2011), Leukfeldt et al., (2013), and Lee, (2018) have advanced a possible correlation between cybercrime awareness and cybercrime prevention and control. For instance, as Liebel (2013) put it: "if someone knows that there are chances of losing his/her money by clicking open an email from an oversea criminal hacker, and paying for an offer, he/she would not have done that". In the same token, Leukfeldt et al. (2013) concluded that the first problem in detecting and investigating cybercrime in Singapore lies in the fact that victims of cybercrime don't always notice that they are being victimized. They therefore conclude that the first bottleneck in the fight against cybercrime is the fact that significant part of cybercrimes will never enter or leave the criminal justice system as a result of lack of knowledge of cybercrime. Similarly, Boateng et al. (2011) posited that that although cybercrime awareness is on the increase in Ghana, the crimes mostly go unreported. The researchers also revealed that the Ghana Police Department, responsible for arresting and prosecuting cyber criminals lack the technical know-how and adequate legal support to effectively discharge their duties. What is more, Malby et al. (2013, p. 1) found that individual cybercrime victimization is significantly higher than conventional crimes; and individual cyber crime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts (like intensive users' education and awareness) in these countries (p.1).

a. Research Gap

From the foregoing, there is seemingly lack of consensus in the pattern of cybercrime awareness. In this regard, some scholars in the camp of Kazeem (2019), and Boateng et al. (2011) hold that cybercrime awareness is on the increase. For instance, Kazeem (2019, p.1) reported that unsealed indictment shows the evolving tactics of online fraudsters which has seen them continue to dupe unwitting victims despite numerous awareness campaigns about the online scams (Kazeem, 2019). On their own, Boateng et al. (2011) reported that cybercrime awareness is on the increase in Ghana.

On the other hand, the likes of Hansen (2007); Malby et al. (2013); Sasse, Brostoff and Weirich (2001), and Leukfeldt et al. (2013) hold that there is poor cybercrime awareness; just as the efforts towards increasing its awareness is at the best very challenging. For them, the reality of poor users' education on the potential risks associated with information and communication technological gadget holds water both on the side of the security personnel and that of the general public. For instance, Hansen (2007, p. 263) concluded that with all the remarkable and amazing technological introductions over the past 30 years, both with personal computer systems and today with handheld devices, we (sic) are still vulnerable to the frailties of human behavior". Malby et al. (2013, p. 236) reported that despite a growing number of such cybercrime awareness campaigns, a number of countries reported the view that it will take a while for the public awareness campaigns to build up the public trust. In the same token, receipt of information about cybercrime did not necessarily translate into "feeling informed" about cybercrime. They also highlighted challenges in developing appropriate and cost-effective campaigns, and noted that providing information to users without additional training and skills acquisition activities can have a limited impact on their online behaviour.

Sasse, Brostoff and Weirich (2001), on their own, concluded that simple campaigns focused on a specific target group seemed to be most cost-effective. There are also limits as to how far users can be expected to learn complex security mechanisms, remember long and varied passwords for every online service they sign up to, and take other precautions that often directly interfere with the task at hand.

What is more, none of the positions (as espoused above) reflects the situation in Nigeria, especially in the Southeastern part. Based on the literature, nothing is currently known on the pattern or trend on the cybercrime awareness. Instead, most cybercrime related studies in Nigeria tend to focus more on incidence, financial cost, public-private partnership, and other anti-cyber crime measures. Such studies have also focused more on the South-Western and South-Southern Nigeria; thereby leaving other parts of Nigeria in the dark- especially the South-Eastern Nigeria (see, for example, Ndubueze, 2012; Longe & Chiemeka, 2008; Boateng et al., 2011; Akuta et al, 2011; Wada & Odualaja, 2012; Ashaolu, 2011; Hassan & Makinde, 2012). The current study therefore aims at filling the gap by evaluating the pattern: the level and depth of cybercrime awareness; and the socioeconomic landscape of cybercrime awareness in southeastern Nigeria.

b. Aims and Objectives of the Present Study

The aim of the study is to evaluate the pattern of cybercrime awareness as a strategy of cybercrime prevention and control in Imo State, South-Eastern Nigeria. The specific objectives of the study are as follow:

1. To ascertain the level of cybercrime awareness in Imo State.
2. To determine the depth of such awareness by ascertaining the categories of cybercrime to which respondents are actually aware of.
3. To find out the relationship between socio-demographic characteristics of the respondents and cybercrime awareness.

1. Literature Review

1.1. Cybercrime Trends

In 2009, internet related criminal activities resulted in about $559.7 million in reported losses, showing a significant increase from $264.6 million and $239.1 million reported losses in 2008 and 2007 respectively. A majority of the 146, 663 cases referred for investigation by IC3 involved alleged fraud and had a median financial loss of $575. The details of the report show that perpetrators were predominantly male (76.6 %). The majority of reported perpetrators were from the United States, but significant numbers were also from the United Kingdom, Nigeria, Canada, etc. Males comprised 54 % of the complainants, about two-third were between the ages of 30 and 50. Apart from the United States, IC3 also received numerous complaints from Canada, United Kingdom, Australia, India and Puerto Rico (Internet Crime Report, 2009; Ndubueze, 2012).

In 2010, IC3 received the second-highest number of complaints since its inception (303,809). IC3 also reached a major milestone in 2013 when it received its two-millionth complaint. On average, IC3 received and processed 25,000 complaints per month. The 2010 Internet Crime Report demonstrated how pervasive online crime has become, affecting people in all demographic groups (Internet Crime Report, 2010, p. 5).

In 2011, 314,246 complaints were received, which represents 3.4 % increase over the 2010, and $485.3 million adjusted dollar loss of complaint. The most common victim complaints included FBI-related scams, identity theft and advance fee fraud. IC3 received and processed more than 26,000 complaints per month. There was little change between 2010 and 2011 in the age groups that filed complaints. The highest percentage of complainants was between ages 40 to 59, which represented 44 percent in 2010 and 43 percent in 2011. In 2012, total complaints received were 289,874; complaints reporting loss was 114,908. A total loss was $525,441,110.00; median dollar loss for those reporting a loss was $600.00. Average dollar loss overall was $1,813.00; and average dollar loss for those reporting loss was $4,573.00 (Internet Crime Report, 2012).

It is estimated that 90% of the software, DVDs, and CDs sold in some countries are counterfeit, and that the total global trade in counterfeit goods is more than $600 billion a year. In 2009, the majority of malware connects to host Web sites registered in the U.S.A. (51.4%), with China second (17.2%), and Spain third (15.7%). A primary means of malware dissemination is email. By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time. Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime (Gercke, 2012; IBM Survey, 2006).

In Africa, Nigeria, Ghana, Cameroon and South Africa have prominently and consistently featured in the list of the world perpetrating and complaint demography (Internet Crime Report, 2009; 2010; Kozlovski, 2005; Smith, 2016). In the same token, some other geographic areas in Africa- including Nigeria, Cameroon, South Africa, Kenya and other sub-Saharan African countries like Zambia and Botswana- have been delimited the cybercrime "capital" of the world (Akuta et al., 2011). What is more, Nigeria has been at the spot light from the international community for its involvement in cybercrime.

In the same vein, high prevalence of such cybercrime categories like pornography, debit/credit card fraud, spam mail, phishing, cyber terrorism, cyber stalking, e-fraud, advance fee fraud, (419), fake copy-cat website, software piracy, hacking, and others have been witnessed in Nigeria (Adeleke, Ibiwoye & Olowokudejo, 2007; Wada & Odulaja, 2012).

1.2. Categorization of Cybercrime

In the light of pitfalls associated with the definition of cybercrime, some scholars have attempted to rather define it in terms of category (Ashaolu, 2011; Finnie et al., 2010; Gercke, 2012; Malby et al., 2013; O'Shea et al. 2007). For instance, the Council of Europe Convention on Cybercrime (2005) categorized cybercrime into four different types of offences; namely: offences against the confidentiality, integrity and availability of computer data and systems; content-related offences; copyright-related offences; and computer-related offences. What is more, Yar, (2005, p. 407), supported by other scholars like Ashaolu (2011), and Gordon and Ford (2006), prefer broader categorization of cybercrime victimization into two: computer-assisted/associated and computer focused. For the purpose of this study, categorization of cybercrime was adopted. The reason is that it appears to pose less analytical challenge in comparison to other categorizations. What is more, it is allusively supported by other scholars like Ashaolu (2011), and Gordon and Ford (2006).

1.2.1. Computer-Assisted (related) Crimes

These refer to those crimes that pre-date the Internet but take on a new life in cyber space. They include the following: Cyber Terrorism; E-Forgery/Data Diddling; E-Fraud; Identity Theft; Erotic/Pornographic Material; Racism, Hate Speech, Glorification of Violence; Religious Offences; Illegal Gambling and Online Games; Libel and False Information; Cyber Bullying; Cyber Stalking; etc. (Malby et al., 2013).

1.2.2. Computer Focused Crimes

These refer to those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it. They include the followings: Email Bombing; Denial-of-Service Attack (DoS); Spam and Related Threats; Trojan; Key-loggers; Hacking; Data Espionage; Illegal Interception; Data/System Interference; Viral Attacks; Phishing; Email/Web Spoofing; Web Jacking; etc. (Gercke, 2012).

1.3. Features of Cybercrime Awareness Campaign

The responsibility of carrying out anti-cybercrime campaign could be shouldered by both governmental and non-governmental agencies and individuals at any level- regional, national, and municipal. However, there should be government agencies and departments coordinating such campaigns (Malby et al., 2013, p. 31). Bringuel and Rich (2010, p. 312) indicated that there are really three areas the government could require warnings regarding Internet dangers. First, legislation could be passed requiring that all manufactures of computer equipment include a Personal Internet Security users learners' guide that would include warnings and an educational module before allowing the computer's web browser to operate.

Second, the government could also require that any software which allows access to the Internet to have a simple warning about the threat to personal privacy/security on the Internet. Thirdly, the government could require or encourage all Internet-based Services (IBS) to comply with a certification system wherein users see a familiar logo or trademark indicating approved membership in trade organizations sensitive to consumer privacy/security issues. Cybercrime awareness could also be carried out by other government agencies like the ministry of communication, and the police department (O'Dea & Rich, 2010, p. 236).

1.4. Cybercrime Awareness and Internet Users

Anyone connected to the Internet is at risk of being targeted and could become a victim of cybercrime. Some have suggested individuals are more likely to be threatened, bullied, assailed, or mugged online than on the local street corner (Lieber, 2013). With this in mind, individuals must make active steps to prevent themselves from getting injured, either emotionally, financially, or physically. As Hansen (2007, p: 263) put it: "The point is, with all the remarkable and amazing technological introductions over the past 30 years, both with personal computer systems and today with handheld devices, we (sic) are still vulnerable to the frailties of human behavior".

One question that usually comes to mind is: why would someone want to target another? In answering this question, Hansen (2007, p: 263), puts thus: "there are several instances where a disgruntled teenager has downloaded pornography and gotten 'Daddy' in trouble with 'Mommy' to deflect attention away from other situations. Instances have occurred where marital discord has led to divorce and an upset wife has downloaded 'kiddie porn', afterward alerting authorities about it to discredit her spouse in regards to custody and financial disputes. There are instances of a co-workers failing to log out or even lock an office computer; share their password".

Lastly, in regards to protecting one's identity: people do freely share their data with the world; post personal pictures, stories, and other details online. In this regard, one might also ask the question: who might the culprit be? Studies show that over 90 percent of cyber-attacks come from pals, relatives or associates. Often times, the attack is a result of some trivial or heated disagreement at work with a colleague, or at home with a spouse, child, or relative. Most computers that are randomly compromised are done so to utilize some zombie or peer-to-peer manipulation of your computer's processing power, not your personal data (Hansen, 2007).

However, cyber-attacks could come from a stranger when people leave much information about them on the trash than on the computer (lack of "digital hygiene"). Incidentally, one could also ask the question: what might be the target of the attacks*?* According to Hansen, it could be money, sensitive data on the system, or any other device.

More so, how is access to one's computer system, PDA, or cell phone possible? It could be possible when one is a careless user of the cyber space (i.e., when one fails to lock one's office or house; when one leaves his/her laptop in the backseat of car with the windows down on a warm sunny day, etc.,). Rich (2010, p: 45) reported that more and more of the senior population are entering the world of cyber space, drawn to it for various reasons. While a good number of seniors have the means, time, and capability to become cyber spacers, they have not inherently been nurtured regarding the pitfalls of cyber space. Seniors are no strangers to credit card fraud, identity theft, and scams traditionally committed by unscrupulous individuals contacting them via telephone and through elaborate schemes.

1.5. Cybercrime Awareness and Educational Institutions

O'Dea and Rich (2010, p. 51) called for the realization that technology is playing an ever-increasing role in children's lives as in their educations right from the elementary school. According to the authors, "as we (sic)continue to increase the use of technology in our (sic) lives, and our (sic)children's lives, we (sic) must increase our awareness and preparation for the increasing threats posed to our (sic) children by criminals familiar with the cyber world". Internet and other ICT facilities are no doubt wonderful educational devices, but experience also showed that putting these facilities into the hands of school-age children, or anyone unaware of personal security safety problems, can be a dangerous prospect

As in many other educational domains, the most evident place to begin helping the children to protect themselves against cybercrime is in the schools. Studies show that schools and counties across the countries (mostly in developed countries) are now encouraging students and parents to practice cyber safety (Finnie et al., 2010). This practice could be replicated in Nigeria. Colleges and universities provide an additional venue for the delivery of educational programs to enhance both individual and institutional levels of cyber security for a large cross-section of the younger population (O'Dea and Rich, 2010). Cyber security for incoming first-year students can easily be introduced through the new student orientations that are increasingly required by most large state universities prior to enrollment for courses.

1.6. Challenges of Cybercrime Awareness Campaign

Advice to individuals on cybercrime risks and mitigation is an important component of an overall cybercrime reduction strategy. However, studies show that despite a growing number of such campaigns, a number of countries reported the view that it will take a while for the public awareness campaigns to build up the public trust. In the same token, receipt of information about cybercrime did not necessarily translate into "feeling informed" about cybercrime (Malby et al., 2013, p: 236). It also highlighted challenges in developing appropriate and cost-effective campaigns, and noted that providing information to users without additional training and skills acquisition activities can have a limited impact on their online behaviour.

The review concluded that simple campaigns focused on a specific target group seemed to be most cost-effective. There are also limits as to how far users can be expected to learn complex security mechanisms, remember long and varied passwords for every online service they sign up to, and take other precautions that often directly interfere with the task at hand (Sasse, Brostoff and Weirich, 2001).

2. Methodology

2.1. Participants

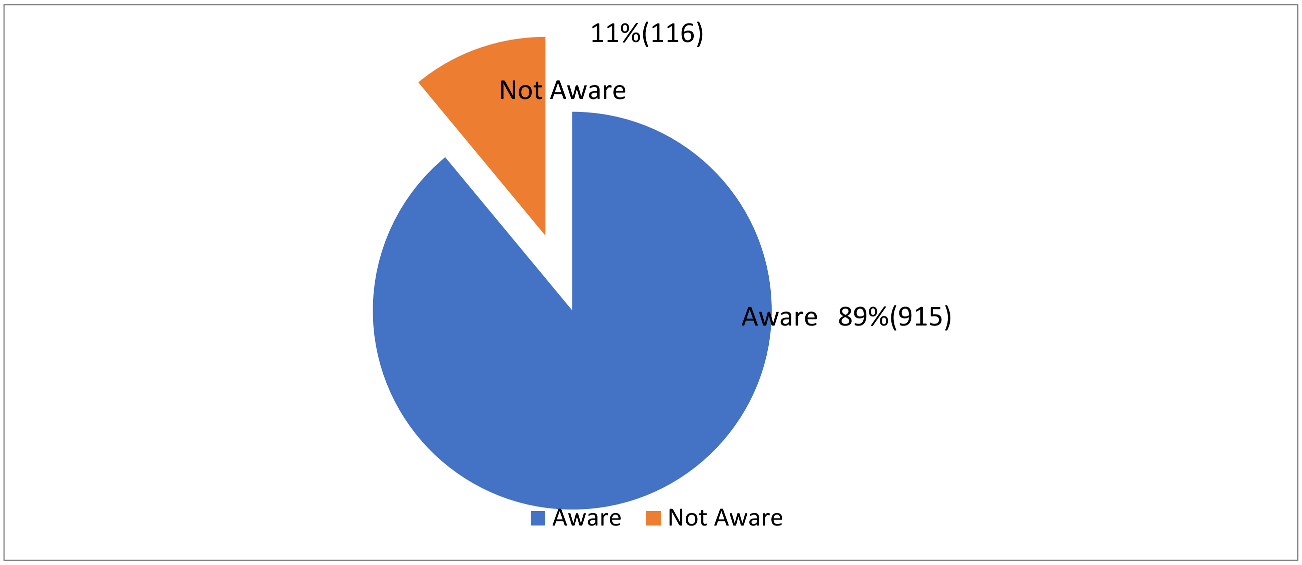
1031 participants were selected for the study (between July and August, 2015) using multistage clustering and random sampling methods. However, 1031 properly completed the questionnaire. In order to achieve methodological triangulation 8 key participants (4 academic staff and 4 students) were also purposefully selected to participate in the In-depth Interview section. Most respondents identified themselves as female (*N*= 650; 63%), while fewer respondents identified themselves as male (*N*= 381; 37%). Again, the modal age of the respondents was between 20-29 (*N*=574; 56%), followed by the age bracket of between 30–39 (N=293; 28%), the next is the age bracket of below 20 years (N=144; 14%), the least age bracket is that of 40-49 (N=15; 1.5%); and 50 and above (N=5; 0.5%) respectively. In terms of marital status, most respondents were single (N=866; 84%), followed by those who admitted they were married (N=158; 15.3%); next is those who admitted they were separated (N=5; 0.5%); only 2 persons (0.2%) admitted they were divorcee(s). In terms of religious affiliation, the majority (N=990; 96%) identified with Christianity; 3.5% (N=36) identified with Islam; while only 5 (0.5%) identified with African Religion. Regarding the educational level completed, majority completed SSCE/NECO (N=647; 62.8%); followed by those who completed NCE/OND (N=263; 25.5%); next are those who have Master's Degree and above (N=70; 6.8%); the least are those who were graduates (N=51; 4.9%). What is more, the majority of the respondents were students (N=938; 91%); while just 93 (9%) were staff.

3. Data Analysis and Presentation

3.1. Objective 1: To Ascertain the Level of Cybercrime Awareness in Imo State.

a. Level of Cybercrime Awareness in Imo State

Figure 1. Distribution of Respondents by the Percentage (%) of their Cybercrime Awareness

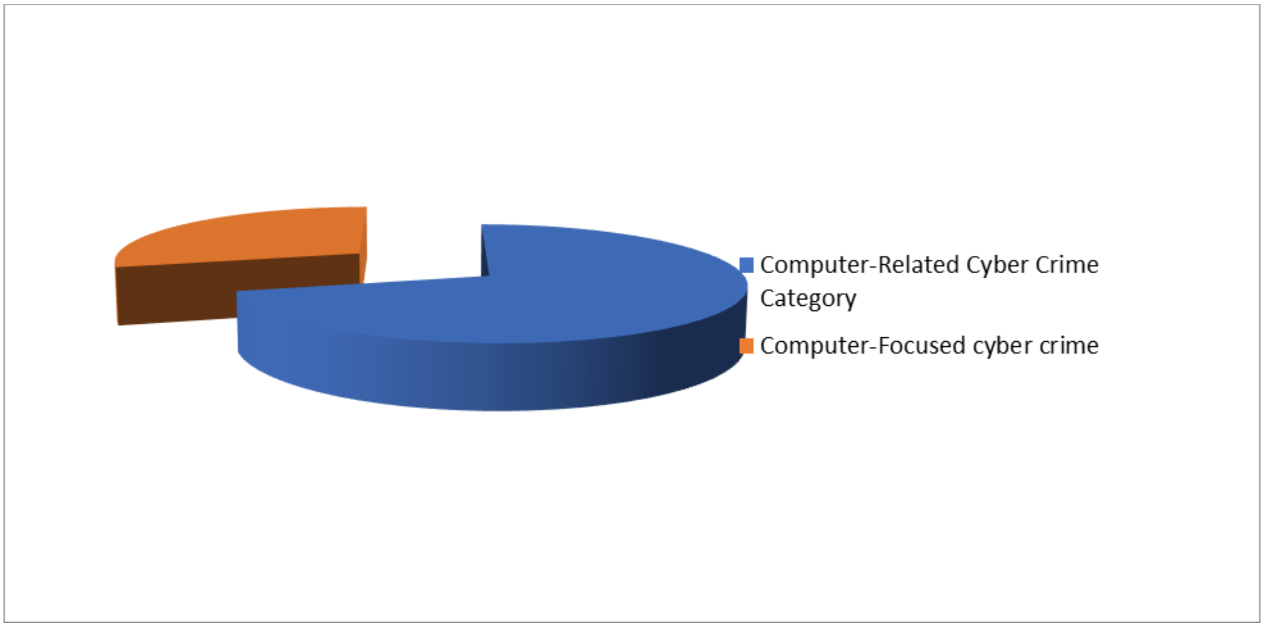


Respondents were asked: “Are you aware that people have been attacked, raped, or even lost money or lives through the Internet, phone, or ATM?” “If yes, please mention or describe the one(s) you are aware people have suffered on the Internet in last three years”. Awareness of cybercrime was therefore measured by not only circling “yes”, but by mentioning a given cybercrime category- say “spam mail”, “fraud”, etc. Level of cybercrime awareness was considered very low at ≤40%; moderate at 40-50%; high at 60-70%; and considered very high at 8-0-100%.

From figure 1, the overwhelming majority of the respondents (N=915; 89%) admitted that they were aware of cybercrime, while just few (N=116; 11%) respondents admitted not being aware of cybercrime. It was therefore concluded that the level of cybercrime awareness was very high. This position was also validated by the IDI data, where almost all the interviewed informants admitted being aware of cybercrime. For instance, an informant from Imo State University (IMSU) (student, female, single, 23years, and Christian) put it thus: “…well, of course everyone should know what is cybercrime”.

3.2. Objective 2: To Determine the Depth of Cybercrime Awareness by Ascertaining the Categories of Cybercrime to which Respondents are Actually Aware of.

Figure 2. The Depth of Respondents’ Cybercrime Awareness Status Using their Cybercrime Awareness Category



From the question: “If yes, please mention or describe the one(s) you are aware people have suffered on the Internet in last three years”; it was discovered that of the 915 respondents who admitted knowledge of cybercrime, greater majority (N=804; 78%) (see Figure 2 above) were only aware of computer-related/assisted category of cybercrime; while as low as 22% (227) were aware of computer-focused cybercrime.

Again, the information from IDI section corresponded with this- for instance, almost all the informants, who admitted being aware of cybercrime, were only aware of the computer-related/assisted category of cybercrime like e pornography e-fraud, identity theft, using ICT to facilitate kidnapping, and others. For instance, an informant at Federal Poly, Nekede (male, Muslim, 41 years, teaching staff, married) put it thus:

> about 6 years ago, the media was awash with the stories on the gruesome murder of 25-year old Cynthia Osokagu, daughter of a retired general, on the 23rd of July 2012, inside a hotel room in Amuwo Odofin L.G.A of Lagos State By friends she met on the Facebook...[Informant: IDI; Male Muslim, Academic Staff of Federal Poly Nekede, 41 years, Married.].

3.3. Objective 3: To Find out the relationship between socio-demographic characteristics of the respondents and cybercrime awareness.

3.3.1. Gender and Cybercrime Awareness

Table 1. Distribution of Respondents by Gender and Cybercrime Awareness

Awareness of Cyber Crime	Gender		
	Male	Female	Total (%)
Aware	346 (91%)	572 (88%)	918 (89%)
Not Aware	35 (9%)	78 (12%)	113 (11%)
Total	381 (100%)	650 (100%)	1031 (100%)

Source: Field Work (2015).

Table 1 indicates that out of the total of 381 male respondents, 91% (N=346) admitted that they were aware of cybercrime; while only a handful of them (N=35; 9%) admitted not being aware of cybercrime. On the other hand, of 650 female respondents, 88% (N=572) admitted being aware of cybercrime; while only 12% (N=78) admitted not being aware of cybercrime.

3.3.2. Level Education and cyber crime awareness

The questionnaire item on the level of education was collapsed into higher and lower levels of education. Higher level of education implied, in this regard, those respondents who have completed any of OND, NCE, B.sc, HND, and above; while lower level of education implied those respondents, who have completed SSCE/WASSE and below). From Table 2: 65% (N=670) of the respondents had low level of education, while just 37% (N=361) admitted being highly educated.

What is more, of 670 lowly educated respondents, 87% (N=583) of the respondents admitted being aware of cybercrime, while just 13% (N=87) admitted not being aware. On the other hand, of 361 highly educated respondents, majority (N=332; 92%) admitted being aware of cybercrime, while just few (N=8; 29%) admitted not being aware of cybercrime.

Table 2. Distribution of Respondents by Level Education and Cybercrime Awareness

Awareness of Cyber Crime	Level of Education Completed		
	Low Level	High Level	Total (%)
Aware	583 (87%)	332 (92%)	915 (89%)
Not Aware	87 (13%)	29 (8%)	116 (11%)
Total	670 (100%)	361 (100%)	1031 (100%)

Source: Field Work (2015).

3.3.3. Age and cybercrime awareness

Table 3. Distribution of Respondents by Age of Respondents and Cybercrime Awareness

Awareness of Cyber Crime	Age of Respondents		
	Younger	Older	Total (%)
Aware	613 (85%)	305 (97%)	918 (88%)
Not Aware	105 (15%)	8 (3%)	113 (12%)
Total	718 (100%)	313 (100%)	1031 (100%)

Source: Field Work (2015).

Here, age of respondents was collapsed into younger (i.e., Age < 30), and older (i.e. Age > 30) Internet Users. Table 3 shows that 70% (N=718) of the respondents were younger, while 30% (313) were older. What is more, of 718 younger respondents, 85% (N=613) admitted being aware of cybercrime, while just 15% (N=105) admitted not being aware. On the other hand, of 313 older respondents, 97% (N=305) admitted being aware of cybercrime, while just 3% (8) admitted not being aware of cybercrime. Put in another way, respondents tended to become more aware of cybercrime menace as they grew older; and vice versa.

3.4. Summary of Findings

1. It appears that there is very high level of cybercrime awareness given that the majority of respondents (N=915; 89%) admitted being aware of cybercrime, while just few (N=116; 11%) respondents admitted not being aware of cybercrime.

2. The study also found that the knowledge of cybercrime menace appeared to be very superficial because a greater majority (N=714; 78%) of the respondents were only aware of computer-related/assisted category of cybercrime like e-fraud; while as low as 22% (N=201) were aware of only computer-focused cybercrime categories like business email compromise; spam email; etc.

3. Another finding shows that cybercrime awareness was gender sensitive in the sense that more males (N=347; 91%) that females (N=572; 88%) were aware of cybercrime; while lesser males (N=34; 9%) that females (N=78; 12%) were not aware of cybercrime.

4. That there is a positive relationship between level of education and awareness of cybercrime- in the sense that the highly educated Internet users tend to be more informed (N=332; 92%) about online criminal activities that the lowly educated ones (N=583; 87%).

5. It also holds that there's a positive relationship between age and cybercrime awareness in the sense that the prevalence of cybercrime awareness increases (N=305; 97%) as Internet users get older.

4. Discussion

Given the conflicting positions on the pattern of, and trend in cybercrime awareness as a strategy of controlling and preventing cybercrime victimization, the study evaluated the pattern of public awareness of cybercrime in Imo State Nigeria. Several important findings emerged from this study as follows:

4.1. Level of Cybercrime Awareness in Imo State, Nigeria

From the finding, the majority of respondents (N=915; 89%) admitted being aware of cybercrime, while just few (N=116; 11%) respondents admitted not being aware of cybercrime. This implies a high level of cybercrime awareness in Imo State. This appears to be similar with the reality in Ghana, another West African country, as reported by Boateng, Isabalija, Olumide and Budu (2011). They found that cybercrime awareness is on the increase.

4.2. The Depth Respondents' Cybercrime Awareness Status

The study also found that the knowledge of cybercrime menace appeared to be very superficial because majority (N=714; 78%) of the respondents were only aware of computer-related/assisted category of cybercrime like e-fraud; while as low as 22% (N=201) were aware of only computer-focused cybercrime categories like business email compromise; spam email; denial-of-service attacks; spam and related threats; trojan; key-loggers; hacking; data espionage; illegal interception; data/system interference; viral attacks; phishing; email/web spoofing; web jacking; etc.

This finding can be explained more in the light of Ndubueze (2012)'s conclusion that there was high prevalence of such cybercrimes as pornography, debit card fraud, etc., in Nigeria, which are mostly computer-assisted cybercrime categories. It is noteworthy that these categories of cybercrime are still same conventional common crimes that just found new expression on the Internet- hence, easily identifiable. More so, the high prevalence of computer-related/assisted cybercrime may equally be attributed to the media hype on them; hence people tend to be more aware of them. For instance, about 6 years ago, the media was awash with the stories on the gruesome murder of 25-year old Cynthia Osokagu, daughter of a retired general, on the 23rd of July 2012, inside a hotel room in

Amuwo Odofin L.G.A of Lagos State by friends she met on the Facebook - as relayed by a respondent interviewed.

Stressing the point further, the finding, which shows a superficial or shallow awareness of cybercrime, tends to support the following studies: individual cybercrime victimization rates are higher in countries with lower levels of development (Malby et al., 2013); that most cybercrimes go unreported (probably due to lack of awareness on the side of victims) (Boateng et al., 2011); only 10% of cyber-crimes are reported and less than 2% reported cases resulted in successful prosecution (Jiow (2013); the first problem in detecting and investigating cybercrime lies in the fact that victims of cybercrime don't always notice that they are being victimized; and that the first bottleneck in the fight against cybercrime is the fact that significant part of cybercrimes will never enter or leave the criminal justice system as a result of lack of knowledge of cybercrime (Leukfeldt et al., 2013) with all the remarkable and amazing technological introductions over the past 30 years, both with personal computer systems and today with handheld devices, most people are still vulnerable to the frailties of human behavior (Hansen, 2007); that it will take a while for the public awareness campaigns to build up the public trust; and that most users' education or cybercrime campaign did not necessarily translate into "feeling informed" (Malby et al., 2013).

Very significantly, the finding beams more light on the probable factor (lack or superficial awareness of cybercrime) contributing to the increasing cybercrime victimization. This is because, contemporarily, it appears that the computer-focused category of cybercrime is more devastating and intricate than computer related/assisted cybercrime categories. For example, it was reported recently that cybercrime perpetrators have changed their method: In the past, for instance, they were using romance scams (computer-assisted cybercrime) through dating sites as well as phony email business propositions from infamous "Nigerian princes," but their current tactics involved scamming non-paranoid individuals using business email compromise (BEC). This method involves fraudsters using hacked corporate/business email accounts to convince businesses or individuals to make payments that are either bogus or similar to actual payments owed to legitimate companies. This was the case recently in the well publicized fraud case of a 252-count federal grand jury indictment unsealed on Thursday (August 23, 2019) named 80 defendants charged with defrauding victims of up to $10 million in one of the "largest cases of its kind in US history." The fraudsters utilized the BEC method in an attempt to steal $40 million in total from victims in 10 countries as well as the US (Kazeem, 2019).

4.3. Gender and Cybercrime Awareness

Another finding shows that cybercrime awareness was gender sensitive in the sense that more males (N=347; 91%) that females (N=572; 88%) were aware of cybercrime; while lesser males (N=34; 9%) that females (N=78; 12%) were not aware of cybercrime. This is incidentally not in line with the finding of Ndubueze, Igbo and Okoye (2013) which held that males are more likely to be victims of cybercrime. This is because, given the higher prevalence of cybercrime awareness among males, as found in the present study, it is more logical that more females than males should be victims of cybercrime. Given this logic, more inquiries are needful to unravel this.

4.4. Level Education and Cybercrime Awareness

This finding holds that there is a positive relationship between level of education and awareness of cybercrime- in the sense that the highly educated Internet users tend to be more informed (N=332; 92%) about online criminal activities that the lowly educated ones (N=583; 87%) and vise versa. This is again does not correspond with Ndubueze, Igbo and Okoye (2013) position that more highly educated than lowly educated were victimized of cybercrime. It also stands to reason that if more educated Internet users are more aware of cybercrime, as held in this study, they should be less victimized of cybercrime. More investigations are required in this case to ascertain the other factors than awareness of cybercrime that predispose people to cybercrime victimization.

4.5. Age and Cybercrime Awareness

This finding also holds there's a positive relationship between age and cybercrime awareness in the sense that the prevalence of cybercrime awareness increases (N=305; 97%) as Internet users get older; and vise versa. This seems to support Ndubueze, Igbo and Okoye (2013) finding that younger respondents are more likely to be victims of cybercrime than aged ones. This because it is logical hold that since the younger respondents, as held in this study, are less likely to be aware of cybercrime, the risk of cybercrime victimization should be higher amongst them.

Conclusion and Recommendations

The findings of this study have exposed the fact that most individuals, including the security personnel, basking on the euphoria of being well informed about the illegal activities online, are really not informed. At the best they appear to be shallowly informed. In this sense, most people tend to be more informed of computer-assisted/related cybercrime categories like e-forgery, e-fraud, e-pornography, etc., and less likely to be informed of computer-focused categories like business email compromise, spam mail, malware attacks, phishing, and others. This therefore calls for in-depth and holistic cybercrime awareness campaign to cover the computer-focused crimes that are more blight to human society.

The findings appear to have united the parallel or conflicting positions on the course or pattern of cybercrime awareness in the literature. The findings achieved this feat by deflecting the focus from the level of awareness to how deep, useful, and effective the awareness is. This therefore calls for more collaboration among the stakeholders for a deep, sustained, useful and effective cybercrime campaign.

The findings also expose some demographic pattern to awareness of cybercrime. In this sense, the fact that more males, the older, and highly educated Internet users than the females, younger, and lowly educated ones tend to be more informed about the illegal activities on the Internet. This therefore call for more deep, useful, and effective cybercrime awareness campaign targeted at the female, younger, and less educated internet users both in Nigeria, and the globe.

Strengths and Limitations of the Study

There are a number of strengths associated with the study that is worth highlighting. Firstly, the methodological triangulation that accommodated both questionnaire and in-depth interview is worth mentioning here. Each helped in cancelling each other's weakness(s). Furthermore, it gives insight into the fact that most individuals are not properly informed about the criminal activities going on the Internet. By this, it helped to pint to possible factors to increased cybercrime victimization in the world today. In the same token, the study appears to have united the parallel or conflicting positions on the course or pattern of cybercrime awareness in the literature. The findings achieved this feat by deflecting the focus from the level of awareness to the depth, effectiveness, and usefulness of cybercrime awareness. Again, the study exposes the demographic pattern of cybercrime awareness.

However, there are weaknesses inherent in the study. Firstly, the study wasn't wide enough in scope- it only explored theoretical and limited demographic aspects of the pattern of cybercrime awareness; it failed to expand the scope to geographical, campus, regional and other aspects. Secondly, the instruments of data collection adopted-questionnaire and in-depth interview- all belong to obtrusive measures-both are reactive measures with its inherent limitations. Again, the tools for data analysis employed in the study (as demanded by the departmental postgraduate board of examiners) failed short of international standard- strong statistical instruments like SPSS should have been employed. More so, the study was only a descriptive study, no attempt was made to undertake hypothesis testing, or causal analysis in an explanatory study. This would have availed the intellectual community the opportunity to have some insights into the nature, strength, and direction of the relationship; as well as the causal relationship that exist between cybercrime awareness and cybercrime victimization. It also failed to reveal factors that informed the patterns as obtained in the study.

Future Directions

From the developments from the current study regarding the pattern or trend in cybercrime awareness, it will be revealing for future studies on: other aspects of the pattern in cybercrime awareness; other factors, other than awareness of cybercrime, that predispose people to cybercrime victimization; factors predispose people to crime; more techniques in running effective anti-cybercrime campaign; and others.

References

Adeleke I.A., Ibiwoye, A., & Olowokudejo, F. F. (2007). *Cyber risk exposure in Nigerian business environment and prospect for cyber insurance.* Retrieved from http://www.unilag.edu.ng/opendoc.php%3Fsno.

Akuta E. A., Monari, I., & Jones, C. R. (2011). Combating cyber crime in Sub-Sahara Africa: A Discourse on law , policy and practice. *Journal of Peace, Gender and Developmental Studies, 1*, 129–137.

Aloul F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology 3*(3), 176–183. doi: 10.4304/jait.3.3.176-183

Ashaolu, D. (2011). *Combating cybercrimes in Nigeria*. Ibadan: Lifegate Publishers.

Babbie, E. (2008). *The basics of social research* (4th ed.). Belmont, USA: Thomson Wadsworth.

Boateng, R., Isabalija, R. S., Olumide, L., & Budu, J. (2001). Sakawa - Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact*, *11*(2), 85–100.

Bringuel, A., & Rich, W. (2010). What role and responsibility does the government have in protecting consumer's rights to privacy/security on the internet? In & J. J. (T. Finnie, T. Petee (Ed.), *Future challenges of cyber crime* (pp. 47–50). Virginia: Futures Working Group.

Finnie, T., Petee, T., & Jarvis, J. (Eds.). (2010). Future challenges of cyber crime. Virginia: Futures Working Group.

Gercke, M. (2012). *Understanding cybercrime: Phenomenon, challenge and legal response.* Geneva: International Telecommunication Union (ITU).

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, *2*, 13–20.

Hansen, J. R. (2007). Cybercrime prevention. In C. B. R. J. K. O'Shea, J. Steete, J. R. Hansen & T. Ralgh (Eds.), *Cybercrime investigations: Bridging the gaps between security Professionals,law enforcements and prosecutors* (pp. 261–283). New York: SynGressPublishing.

Haralambos, M., & Holborn, M. (2004). *Sociology: Themes and perspectives* (6th ed.). London: Harper Collins Publishers.

Hassan, A. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science 2*(7), 626–631. Retrieved from http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf.

IBM. (2006). *Survey.* Retrieved from http://www.ibm.com/press/us/en/pressrelease.

Igbo, E. U. . (2007). *Introduction to criminology* (2nd ed.). Nsukka: University of Nigeria Press.

Imo State. (n. d.). Population. Retrieved from http://www.nigerianstat.gov.ng/imo.

Internet crime complaint centre. (2009). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx

Internet crime complaint centre. (2010). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Internet crime complaint centre. (2012). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

Israel, G. D. (1992). *Sampling: The Evidence Of Extension Program Impact. Program Evaluation and Organizational Development, IFAS.* University of Florida.: PEOD-6.

Kazeem, Y. (2019). The FBI's Nigerian email scam ring bust shows how the billion-dollar global fraud has evolved. Retrieved from www.quartzAfrica.com

Kozlovski, N. (2005). A Paradigm Shift in Online Policing – Designing Accountable Policing, (0331548). Retrieved from http://crypto.stanford.edu/portia/papers/Kozlovski.pdf.

Lee, H. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, Vol.12 (1).*

Leukfeldt, R., Veenstra, S., & Wout. (2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, *7*(1), 1–17.

Liebel, D. (2013). The watch dog: Do you know the superagency that can best protect you from cybercrimes? Retrieved from http://www.dallasnews.com.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). Comprehensive Study on Cybercrime. *United Nations Office on Drugs and Crime*, (February), 1–320. doi: 10.1103/PhysRevLett.105.018904

Mali, P. (2008). *Cyber law consulting: Text book of cyber crime and penalties.* Retrieved from www.cyberlawconsulting.com.

McCrohan, K. F., Engel, K., & Harvey, W. J. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, *9*(1), 23–41. Retrieved from doi: 10.1080/15332861.2010.487415

Ndubueze, P. N. (2012). *Cyber crime and third party policing in Nigeria. A study of selected cyber-cafes in Lagos metropolis*. University of Nigeria, Nsukka.

O'Dea, M., & Rich, W. (2010). The not-so-distant average school day. In & In T. Finnie, T. Petee & J. Jarvis (Eds.), *Future challenges of cybercrime* (pp. 51–55). Virginia: Futures Working Group.

O'Shea, K., Steete, J., Hansen, J. R., Jean, C. B. R., & Ralgh, T. (2007). *Cyber crime investigations: Bridging the gaps between security professionals, law enforcements and prosecutors.* New York: SynGress Publishing.

Oji, M., Dike, M., & Bello, M. (2012, August 23). Facebook murder: Why we killed Cynthia. *Sun Newspaper [Daily News],* p.1

Population and housing census of the federal republic of nigeria. (2006). Retrieved from www.population.gov.ng

Reyes, A. (2007). The problem at hand. In *Cyber crime investigations: Bridging the gaps between security professionals, law enforcements and prosecutors* (pp. 1–20). New York: SynGress Publishing.

Rich, W. (2010). Seniors and cyber space. In T. Finnie, T. Petee, & J. Jarvis (Eds.), *Future challenges of cybercrime* (pp. 59-60). Virginia: Futures Working Group.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer Interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131.

Schools. (n. d.). *Schools and university in Imo State.* Retrieved from http://www.nijapals.com/%3FL%3Dresearch

Siegel, L. J. (2010). *Criminology: Theories, patterns, and typologies* (10th ed.). Belmont, USA: Wadsworth Cengage Learning.

Smith, S. (2016). Contents 2016 Internet Crime Report. *Federal Bureau of Investigation of USA*. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf.

Wada, F., & Odualaja, G. O. (2012). Assessing cybercrime and its impact on e-banking in Nigeria using social theories. *African Journal of Computing & ICT, 5*(1), 69-82.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427.