CYBERCRIME AWARENESS AND CYBERCRIME VICTIMIZATION IN IMO STATE, NIGERIA

Ogochukwu Favour Nzeakor
Peace & Conflict Unit, Michael Okpara University of Agriculture, Umudike, Nigeria

Nnamdi Green Onuoha
Peace & Conflict Unit, Michael Okpara University of Agriculture, Umudike, Nigeria

Chibuike Ndubuisi Nwoke
Department of Sociology and Anthropology, University of Nigeria, Nsukka, Nigeria

Abstract

Despite the increasing incidence of cyber-criminality in Imo State, Nigeria, there is still dearth of evidence expounding public awareness of the incidence and factors precipitating cybercrime vulnerability and victimization among residents of the State. Adopting a cross-sectional survey design rooted in Routine Activity Theory, this study examines the relationship between Internet users' cybercrime awareness status and their cybercrime victimization experiences. The study's sample consists of 1,031 respondents drawn from a population of 73,718 Internet users selected from Alvan Ikeoku College of Education, Owerri; Federal Polytechnic, Nekede; Federal University of Technology, Iheagwa; and Imo State University, Owerri. The study's results showed that cybercrime uninformed Internet users (67%) are more likely to experience cybercrime victimization than cybercrime informed users (19%). The study confirms a statistically significant but high negative relationship between Internet users' awareness status and their cybercrime victimization experiences, $X^2(1030) = 69.8$, $p < 0.05$, $r = .-9$. The study concludes that the volume and distribution of predatory crime such as e-fraud and cyber-bullying in Imo State closely relate to the availability of suitable targets (uninformed Internet users); the absence of capable guardians (lack of adequate cybercrime awareness); and the presence of motivated offenders (cybercrime perpetrators). Thus, the study recommends that increased and adequate public awareness of victimization risks and protective measures represent an important strategy in the prevention of cybercrime in Imo State, Nigeria.

Keywords: Cybercrime, Awareness, Victimization, Risks, Internet Users

Introduction

Information society or globalization brought about a new variant of crime known as cybercrime into the human society (Haralambos & Holborn, 2008; Ndubueze, 2017; Siegel, 2010). Extraterritorial nature of cybercrime, its speed of occurrence, and anonymity are some of the peculiar characteristics of cybercrime that make it ambiguous and insurmountable, especially in the developing countries like Nigeria (Gercke, 2012; Malby, Mace, Holterhof, Brown, Kascherus & Ignatuschenko, 2013).

Consequently, cybercrime threats have literally overwhelmed the security formation, as well as the criminal justice system of most countries in the world (Malby et al., 2013; Warren & Streeter, 2005). More so, lack of cybercrime awareness on the part of most Internet users, lack of comprehensive statistics of cybercrime threats, rapid expansion of computer connectivity, and astronomical growth of the number of Internet users are some of the major factors that have contributed to the high prevalence and sophistication of cybercrime phenomenon (Akuta et al., 2011; The current state of cybercrime, 2013; Internet World Stats, 2013).

Consequently, the spate of cybercrime has assumed sinister dimensions with online fraud and forgery, hacking, botnet attacks, computer virus and worms, cyber terrorism and warfare, cyber pornography, and others constituting the most dangerous cybercrime attacks both in Nigeria and the globe (Finnie, Petee, & Jarvi, 2010; Gercke, 2012; Hollinger, 2000; Mali, 2008). Admittedly, a number of studies have advanced various interventions and strategies including: law enforcement, legal, public-private partnership, technical, institutional measure, international cooperation, and public awareness (Akuta, Ong'oa, & Jones, 2011; Ashaolu, 2011; Boateng, Olumide, Isabalija, & Budu, 2011; Cybercrime Bills, 2013; Dawson, 2009; EFCC, 2013; Fraizer, 2010; Hassan & Makinde, 2012; Jiow, 2013; Leukfeldt, Veenstra, & Stol, 2013; Malbyet al, 2013; Raed, 2010; Wada & Odualaja, 2012; Warren & Streeter, 2005) towards lowering the curve of cybercrime threats. However, most of the studies were done outside Nigeria; and few that were done in Nigeria failed to examine the factor of public awareness as a strategy in reducing the spate of cybercrime victimization experiences. And very few of such studies were done in the southeastern part of Nigeria, especially in Imo State (Ndubueze, 2012; Longe, Chiemeke, Fashola, Longe, & Omilabu, 2007; Boateng et al, 2011; Akuta et al, 2011; Wada & Odualaja, 2012; EFCC, 2013; Ashaolu, 2011; Hassan, Lass, & Makinde, 2012).

The focus of the current study was on public awareness as a factor of preventing cybercrime vulnerability and victimization experiences-collecting data from the southeastern part of Nigeria. This is because, as

Liebel (2013) put it "cybercrime will certainly continue, but those who work to be smarter, more paranoid and less trusting are more likely to avoid the threats of cybercrime. And none of the above mentioned skills can be acquired without adequate user education (public awareness). In the same token, the frailty of human behaviours constitutes the weakest point in the computer technology (Reyes, 2007). Stemming from the above, the objective of the current study was to examine the relationship between Users' cybercrime awareness status and their cybercrime victimization experiences in Imo State, Nigeria.

Information Security and Cybercrime Awareness in Nigeria

There is no consensus among scholars regarding the relationship between information security awareness and cybercrime victimization experience. While some scholars opined that there is no relationship at all; some advanced a negative and strong correlation between cybercrime awareness and cybercrime victimization in the sense that people who are aware of cybercrime scourge are less likely to experience cybercrime victimization (Boateng et al., 2011; Gercke, 2012; Hansen, 2007; Lee, 2018; Leukfeldt et al., 2013; Liebel, 2013; Malby et al., 2013). 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 behaviour. Liebel (2013), supporting a negative correlation between cybercrime awareness and cybercrime victimization, opined that 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.

From Middle East background, Saudi Arabia, Hadlington, Binder, and Stanulewicz (2020) found that participants who reported higher levels of 'Fear of Missing Out' (FoMO) had lower overall 'Information Security Awareness' (ISA), as well as having poorer knowledge, a more negative attitude, and engaged in riskier behaviors in relation to ISA. FoMO was also demonstrated to be the largest single negative predictor for information security or cybercrime awareness, above that of age, gender, and the key personality traits tested. However, this does not reveal much about the Nigerian scenario. Ndubueze, Igbo and Okoye (2013), in their study titled "the cybercrime victimization among Internet active Nigerians: An analysis of socio-demographic correlates, found that younger respondents, males, ever married respondents, respondents with higher level of education, unemployed respondents and Christians are more likely to fall victim of cybercrime. Though the study highlighted the correlation between socio-demographic variables and cybercrime victimization; it however did not

throw light on the correlation between public awareness and cybercrime victimization, nor collected data from Southeastern Nigeria.

A qualitative study by Boateng, Isabalija, Olumide and Budu (2011) examined the state of cybercrime in Ghana and measures being used to address it. A total of 40 respondents participated in the study. They comprised 10 bank staff, 10 internet café operators, 10 police investigators, 5 legal practitioners and 5 internet fraud victims. The researchers found that although cybercrime awareness is on the increase, 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. The study however failed to reveal the relationship between awareness and victimization, especially in Nigeria.

The data from a recent study titled: the impact of cybercrime individual (Impact of Cybercrime, 2013), conducted by cyber security experts at the University of Kent in UK, revealed that over 9 million adults in Britain have had online accounts hacked, and 8% of the UK citizens are revealed to have been victims of cybercrime. 2.3% of the population reported losing more than £10,000 to online fraudsters. The main crime suffered by UK online users is the hacking of their web services accounts. Those include online banking, email, and social media. In nearly 33% of the cases, the offense was repeated. The UK government documented in an official report that the overall cost of cybercrime economy was £27 billion a year. Identity theft was most common crime, accounting for £1.7 billion, and followed by online scams, with £1.4 billion. Cybercrime in the UK was most insidious for organizations, private businesses and government offices, suffering high levels of cyber espionage and intellectual property theft. Social media is a primary target for emerging cybercrime in the UK. Malicious code is used by criminal gangs to exploit social networks for banking fraud or for phishing campaigns. The same malicious code is used by criminals to hack victims' accounts, for the creation of bogus social network 'likes' that could be used to generate buzz for a company or individual (Impact of Cybercrime, 2013). However, the study failed to reveal any correlation between awareness of cybercrime and victimization experiences

Using a total questionnaire sample of 3,506, collected from four countries, Finland, US, Germany and UK, Näsi, Oksanen, Keipi, and Räsänen (2015), found that online crime victimization was relatively uncommon (aggregate 6.5% of participants were victims). Slander and threat of violence were the most common forms of victimization and sexual harassment the least common. Male gender, younger age, immigrant background, urban residence, not living with parents, unemployment and less active offline social life were significant predictors for cybercrime

victimization. However, the study was silent on the factor of awareness in cybercrime victimization.

Accounts of Cybercrime Victimization in South-Eastern Nigeria

Not quite much has been recorded on the pattern and volume of cybercrime in Southeastern part of Nigeria in general, and Imo State in particular. Though there are pockets of reports on cybercrime, but empirical studies on this regard is arguably very scanty. For instance, the alarming incidence of cybercrime in the Southeastern part of Nigeria was brought to the fore in 2019 (News Agency of Nigeria, 2019). In that report, the Economic and Financial Crimes Commission said it was worried over the frightening dimension which cybercrime had assumed in the country, especially the South East. The South East Zonal Head of the commission, Mr Usman Imam, was reported to have accused some parents of not only being aware of their children's involvements but even abetted such terrible crime. This is related to another report in the Nigerian Tribune of May 24, 2021, where it was reported that the operatives from the Tactical Units of the Imo State Police Command busted a syndicate of notorious Internet fraudsters in the state (Uzoma, 2021). As it was reported, the syndicate had been on the run for series of cybercrimes they had committed within Imo and neighbouring states.

One of the few empirical studies on the volume and pattern of cybercrime was done by Udelue and Mathias (2019), who investigated the prevalence of cybercrime among youths in Onitsha, a commercial city in Anambra State. The authors found among others that cybercrime was prevalent among the youths in the area. They equally found that hacking, advance fee fraud, identity theft and cyber terrorism were among the most prevalent cybercrime categories among the youths in the area. Though the study agrees with the existing reports of the increasing incidence of cybercrime, it however did not reveal much about the pattern of cybercrime victimization in Southeastern Nigeria in general, and Imo State in particular. In a seemingly attempt to fill the gap, Nzeakor, Nwokeoma, and Ezeh (2020) evaluated the pattern of public awareness of cybercrime. The authors found that though the level of cybercrime awareness was very high, the knowledge of cybercrime menace appeared very superficial because majority of the Internet users tend to be only informed of computer-related/assisted category of cybercrime; while very few of them were aware of only computer-focused cybercrime categories. The authors equally reported that cybercrime awareness appeared to be gender sensitive in the sense that more males than females Internet users tend to be aware of cybercrime. They equally reported 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 about online criminal activities that the lowly educated ones. It was also discovered that the level of cybercrime awareness increases as Internet users get older. However, their study appeared to have provoked another research question: the correlation between awareness of cybercrime and victimization status of Internet users. This is what the current intervention is poised to investigate.

Theoretical Framework

A number of theoretical choices available in the study of cybercrime include: intergroup emotion theory (Jones, Manstead & Livingstone, 2011); broken windows theory (Wilson & Kelling, 1982); choice theory (Verecio, 2017); social dominance theory (Sidanius, Liu, Shaw & Pratto, 1994); and routine activities theory (Cohen & Felson, 1979). Meanwhile, Routine Activities Theory (RAT) has been applied to cyber aggressive research more often than most frameworks (Beran & Li, 2005; Holt & Bossler, 2008; Arntfield, 2015; Oblad, 2020). In this respect, Frye, Ompad, Chan & Vlahov (2011) applied RAT in examining the situational factors that predict bystander intervention behaviors in inter-personal violence. Leili (2019) equally utilized RAT in exploring three different types of online victimization involving women: stalking, dating violence and sexual violence. It has also been used to explain motivation for cyber-stalking (Reyns, Henson, Fisher, 2011); and importance of parental influence (Dehue, Bolmon & Vollink, 2008). It has equally been utilized to identify where victims are being targeted, methods used by cyber victims as well as to help find risk factors among victims, patterns that prevention specialists can identify and warn others with (Oblad, 2020).

RAT would therefore be adopted as the theoretical orientation in this study. This is because its central schema that emphasizes the necessity for a motivated perpetrator, an identified target and lack of surrounding safeguards (e.g., lack of appropriate users' education) helps to explain the rising incidence of cybercrime).

The major premise of Routine Activity Theory as propounded by Lawrence Cohen and Marcus Felson (1979) holds that the volume and distribution of predatory crime (like e-fruad, cyberbullying) are closely related to the interaction of three variables: the availability of suitable targets (uninformed Internet users); the absence of capable guardians (lack of adequate cybercrime awareness); and the presence of motivated offenders (cybercrime perpetrators). The theory places a rationally motivated offender within an environmental context and explains how these two link up and lead to cybercrime occurrence. This approach to understanding crime was the result of an observation by Cohen and Felson that a crime rise following World War II may in fact have been resulting from a societal transformation

whereby the patterns of daily life were being fundamentally altered triggering new opportunities for crimes to be committed. Cohen and Felson opined that crime was an offshoot of the convergence in space and time of offenders and targets in the absence of a capable guardian (proper awareness campaign) (Cohen & Felson, 1979; Tench, 2019). In this regard, information society, where information and communication technology is a norm, has fundamentally altered daily life, and therefore created opportunities for increased cybercrime victimization experiences.

Methodology

Cross-sectional variant of survey design was adopted. Questionnaire was the main instrument of data collection, while interview guide was used as a supplementary instrument. The area of the study was Imo State, Nigeria. Imo State is one of the 5 states in the eastern part of Nigeria. It has Owerri as its capital and largest city. Imo State lies within latitudes 4º45'N and 70º15'N, and longitude 65º᾽E and 7º25'E with an area around 5,100 sq km. It is bordered by Abia State on the east, by Rivers Niger and Delta on the west, by Anambra State to the north and Rivers State to the south. According to the 2006 population census, Imo State population was put at 3,927, 563; and the population density varies from 230-1,400 people per square kilo-meter. Imo State houses several public and private institutions of higher learning, among them are nine tertiary institutions (National Population Commission, 2006). Imo State was justified as the area of the study based on the fact that it houses about nine tertiary institutions, and other federal and state establishments that attract both cyber offenders and victims alike (National Population Commission, 2006).

The scope of the study covered students and staff of four randomly selected tertiary institutions in Imo State; including: Alvan Ikeoku College of Education, Owerri; Federal Polytechnic, Nekede; Federal University of Technology, Iheagwa; and Imo State University, Owerri. The general population of this study comprised all the Internet users in Imo State which was put at 3,927, 563. The target population comprised of students and academic staff in the 4 selected tertiary institutions in Imo State which was put at 73,718. The details showed that: Alvan Ikeoku College of Education has 13,000 students and 600 academic staff; Federal Polytechnic, Nekede has 21,000 students, and 570 academic staff; Federal University of Technology has 21,039 students and 926 staff; and Imo State University, Owerri has 15,900 and 683 staff (Imo State, n.d.).

Sample size of 1,099 was initially selected based on published tables of sample; however 1,088 was later sampled as per the sampling technique below (see appendix). According to Israel (1992, p.2), there are several approaches to determining sample size. These include using a census for

small populations; imitating a sample size of similar studies; using published tables; and applying formulas to calculate a sample size. In this study, published table approach was adopted (see appendix). According this approach, under the error margin or desired level of precision of ± 3, any population size between 60,000 and 100,000 attracts the sample size of 1,099. Recall that the population size of the selected tertiary institutions was put at 73,718. To supplement the quantitative data, a total of 8 participants- 4 academic staff and 4 students- were selected for In-depth Interview.

To obtain the study sample, multistage clustering, probability proportionate to size (PPS), and random sampling methods were adopted. At the first stage, tertiary education institutions in Imo State were listed and 4 were randomly selected. At the second stage, faculties/schools in the 4 selected tertiary institutions were listed and 4 faculties/schools each were randomly selected- totaling 16 faculties/schools. At the third stage, departments in each of the selected faculties/schools were listed and 4 departments each were randomly selected- totaling 64 departments. The clustering could not be scaled down to the class level because academic staff needed to be accommodated. This is because staff are not categorized as academic class.

At the final stage, the ultimate sampling unit (USU), simple random sampling technique and probability proportionate to size were applied in selecting the respondents (students and academic staff) in each of the selected departments. In this sense, 16 students, and 1 staff were randomly selected from each of the selected department in the ratio of 0.96/0.4 students/staff- totaling 1,088 respondents per department. Meanwhile, only 1,031 respondents could complete their questionnaires appropriately. This represents 94.8% response rate. Furthermore, for the In-depth interviews (IDIs), the 4 students and 4 academic staff (a student and staff per Institution) were selected based on their availability and willingness.

The questionnaire was designed by the researcher, and validated by the Postgraduate Board of Examiners in the Department of Sociology and Anthropology, University of Nigeria. It was also self- administered to respondents for 2 weeks in each of the 4 selected educational institutions- employing the services of trained research assistants. The instrument was also tested in one of the selected institutions (IMSU) for 2 days in order to ensure its effectiveness in generating the responses intended in the research objectives. The field data were processed and analysed manually (as the Departmental tradition demanded) using tables and other descriptive statistical tools. And the hypotheses were tested with Chi-square (X^2) statistic at 0.05 level of significance. The IDI data were analyzed using thematic method. This consisted of quotes and illustrative expressions

under distinct themes. Some relevant descriptive statistics were also used, in addition to tables, and figures.

To guarantee the ethical considerations in research endeavor (i.e., principles of voluntary participation, no harm to the participants, anonymity and confidentiality, and no deception), introductory letters were attached to the questionnaire items, and the interview schedules informing the participants of the purpose of the research, and their right of participation. They were also assured of the confidentiality, anonymity, as well as the commitment to use their data strictly for research purposes (see the appendices). Of 1088 questionnaires administered on the Internet users in the selected tertiary institutions in Imo State, only 1031 respondents were validly completed and returned, and were used in the analysis. This figure, 1031, constitutes 94.8% response rate. The qualitative data collected through In-depth Interviews with 4 academic staff and 4 students were used to support and complement the quantitative data. Furthermore, the result shows that more females (63%), singles (84%), Christians (96%), lowly educated (63%), younger (89%), and students (96%) than males (37%), ever married (16%), other religions (4%), highly educated, older (11%), and academic staff (4%) participated in the survey.

Results and Discussions

Internet Users' Awareness Status and Cybercrime Victimization Experiences

To measure cybercrime awareness, respondents were asked: "Are you aware that people have been attacked, or even lost money or lives through the Internet or ICT devices?" "If yes, please mention or describe what you know have suffered on the Internet in last three years". Awareness of cybercrime was therefore measured by not only circling "yes", but by mentioning or describing a given cybercrime category- say "e-fraud". To measure cybercrime victimization experiences, participants were asked: Which of the following experience(s) they have had in the last 3 years? They were also asked to circle all that apply; with the following options given: a)My online account(s) (email, facebook, twitter, instagram, or bank mobile App) has been hacked; b)I have complied with strange email or call asking me to disclose my personal information, like password, or BVN; c)I have lost money to stranger I met online, or through phone/email; d)I have opened/replied spam mail(s); e)I have received email/text/call that threatened/insulted me; f)I have visited a stranger I met online and had an ugly experience; g)My computer/phone has been attacked by malware/virus; h)I have been contacted by criminal gangs to join them; i)My computer/phone/ICT gadget(s) has been stolen/damaged; and j)I have been

contacted for sexual related activities. Participants were regarded to have experienced cybercrime victimization if they checked or described any of the cybercrime victimization indexes above; and regarded as not victimized if they checked none.

Table 1: *Distribution of Users' awareness status and their cybercrime victimization experiences*

Victimization Status	Internet Users' Awareness Status		
	Aware	Not Aware	Total (%)
Victimized	174 (19%)	76 (67%)	247(24%)
Not Victimized	744 (81%)	37 (33%)	784 (76%)
Total	918 (100%)	113 (100%)	1031 (100%)

Table 1: shows that of 918 informed cybercrime users, as low as 1 in 5 (19%) of them had experienced cybercrime victimization; while as high as 4 in 5 of them (81%) did not experience victimization. On the other hand, of 113 uninformed Internet users, as high as 2 in 3 (67%) of them did experience cybercrime victimization, while as low as 1 in 3 (33%) of them did not experience cybercrime victimization. This therefore means that the cybercrime uninformed Internet users (67%) are more likely to experience cybercrime victimization than the informed users (19%).

The qualitative data equally revealed the possibility. For instance, a student from one of the institutions said:

> …there was this friend of mine that I usually asked to assist me to get money from the ATM for me, who later used my ATM to withdraw from my account without my authorization **[IDI: Nekede, Student, Christian, Female, 21years and single].**

Another victim of advance fee fraud put it thus:

> "I don't think it was greed, rather it was a sheer lack of awareness…I was innocently trying to help a young lady who was helpless in a refugee camp…without knowing I was being duped" **[IDI: Federal University of Technology, married, male, 52years, Assoc. Prof., and Christian].**

Another victim of cyber-bullying, a postgraduate student, from Imo State University equally narrated how her ex-boyfriend took over access of her Facebook account to post her nude pictures and other private information both shared in the past.

Table 2: *Chi-Square distribution of the relationship between Internet users' awareness status and their cybercrime victimization experiences*

Victimization Status	Internet Users' Awareness Status		
	Aware	Not Aware	Total (%)
Victimized	174 (19%)	76 (67%)	247(24%)
Not Victimized	744 (81%)	37 (33%)	784 (76%)
Total	918 (100%)	113 (100%)	1031 (100%)

Note: X^2 = 69.8, table value: 3.841, level of significance: $p \leq 0.05$, r = -.9, degree of freedom: 1.

Table 2 indicates that the calculated (x^2) value of 69.8 is greater than the table value of 3.841, we therefore reject the null hypothesis (H_0) and accept the alternative hypothesis; and conclude that there is a statistically significant but high negative relationship between Internet users' awareness status and their cybercrime victimization experiences, $X^2(1030) = 69.8$, $p< 0.05$, r =.-9. In this sense, cybercrime informed Internet users are less likely to experience cybercrime victimization than uninformed Internet users.

Once again, the objective of the study is to discover the relationship between Internet users' awareness status and their cybercrime victimization experiences. The result shows that while as low as 1 in 5 (19%) of cybercrime informed users had experienced cybercrime victimization; as high as 4 in 5 of them (81%) did not experience victimization. On the other hand, while as high as 2 in 3 (67%) of cybercrime uninformed users did experience cybercrime victimization, as low as 1 in 3 (33%) of them did not experience cybercrime victimization.

This therefore means that the cyber-security uninformed Internet users (67%) are more likely to experience cybercrime victimization than the informed users (19%). The test of hypothesis shows that the above result/relationship is statistically significant. In this regard, it was concluded that there is a statistically significant but high negative relationship between Internet users' awareness status and their cybercrime victimization experiences, $X^2(1030) = 69.8$, $p< 0.05$, r =.-9.

In revealing the possibility from the qualitative data, a student from one of the institutions narrated how her friend with whom she usually shared her ATM details stole money from her account. Another victim of advance fee fraud narrated how he was unaware that the poor girl he was innocently trying to help out in a refugee camp duped him of his hard earned money.

Another victim of cyber-bullying, a postgraduate student, from Imo State University equally narrated how her ex-boyfriend gained access of her Facebook account to post her nude pictures and other private information both shared in the past. The result is synch with other findings like Gercke (2012), Liebel (2013), McCrohan, Engel and Harvey (2010), and Siegel (2010) who found a negative relationship between awareness and victimization experiences. Siegel (2010), instance, posited that increased awareness campaign, as a strategy, has successfully controlled not only other crime variants, but also other societal scourges like HIV/AIDS and polio, sickle cell anemia, etc (p.83). McCrohan, Engel and Harvey (2010) reported that people tend to employ more online security measures when educated about cybercrime menace. In the same token, this lends support to the conclusions of Gercke (2012, p. 105) who posited that certain cybercrimes – especially those property cybercrime category (phishing, fraud, spoofing – do not generally depend on a lack of technical protection, but rather on a lack of awareness on the part of the victims. In the same vein, Liebel (2013), supporting a negative correlation between cybercrime awareness and cybercrime victimization, opined that 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.

However, the result contradicts other findings like Boateng et al. (2011), Hansen (2007), Malby et al. (2013); and others found otherwise. For instance, Boateng, Isabalija, Olumide and Budu (2011) found that although cybercrime awareness was on the increase, cybercrime victimization was still on the increase, with the crimes mostly go unreported. Malby et al. (2013), on their own, held 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. In the same token, Hansen (2007, p.263) concluded that with all the remarkable and amazing technological introductions over the past decades, both with personal computer systems and today with handheld devices, we are still vulnerable to the frailties of human behavior (p.263).

Appropriate Measures to Curb Cybercrime in Imo State, Nigeria

From the field data analysed, and in line with the theoretical orientation (RAT), the following measures were put in place to mitigate against cybercrime in the Imo State. Some Internet users keep their software and operating systems updated. This helps in increasing surveillance of the network system, and as such, providing the needed capable guardianship as RAT stipulates. Using strong, and unique passwords was another technique of protection. Some considered starting with a favorite sentence, and then just use the first letter of each word, or even using a popular site like river,

street, rock, in their locality, as well as inputting numerals like important dates or phone numbers in-between. Others adopted multi-factor authentication on their social media accounts. Multi-factor authentication makes it much harder for a hacker to break into online accounts. Others were weary of using public Wi-Fi. This is because when using public Wi-Fi, anyone nearby who is connected to the same network can listen in on what one's computer is sending and receiving across the internet. Others reported they avoided opening any unsolicited and strange emails, links, and attachments.

Conclusion and Recommendation

It was therefore concluded that there is a statistically significant but high negative relationship between Internet users' awareness status and their cybercrime victimization experiences in the sense that cyber-security uninformed Internet users are more likely to experience cybercrime victimization than the informed users. The finding, to a greater extent, has closed the gap created by the conflicting position in the criminological literature regarding the relationship between cybercrime awareness and cybercrime victimization. By finding that there is a statistically significant but high negative relationship between Internet users' awareness status and their cybercrime victimization experiences, the study has substantiated Routine Activity Theory which holds that the volume and distribution of predatory crime (like e-fraud, cyber-bullying) are closely related to the interaction of three variables: the availability of suitable targets (uninformed Internet users); the absence of capable guardians (lack of adequate cybercrime awareness); and the presence of motivated offenders (cybercrime perpetrators). From the standpoint of RAT, increased and adequate public awareness of victimization risks and protective measures that can be taken represent an important strategy in the prevention of cybercrime in particular, and crimes in general.

The study aimed at contributing to a better understanding of the relationship between awareness and victimization experiences Internet users go through so as to recommend interventions towards reducing the spate of cybercrime victimization experiences. It is my belief that by discovering that more cybercrime informed Internet users than uninformed users are less likely to experience cybercrime victimization, interventions can be implemented to increasing adequate awareness campaign in Nigeria. Therefore, the study has not only enriched cyber-criminological literature, especially in the South-Eastern Nigeria, it has shown that information security or cybercrime awareness of victimization risks and protective measures that can be taken represent an important strategy in reducing

cybercrime scourge both in Nigeria and globally. Increased and adequate information security/cybercrime awareness campaign is therefore recommended. Both state and non-state actors are implored to design and carry out holistic and effective cybercrime awareness campaign. Such awareness campaign must accommodate the current trends on cybercrime victimization. More so, government at all levels should establish cybercrime complain center at every strategic point that will be saddled with the responsibility of collating, processing and disseminating cybercrime related complaints.

References

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.*

Arntfield, M. (2015). Towards a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication, 40*:371-388.

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

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

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*.

Boateng, R., Isabalija, R. S., Olumide, L., & Budu, J. (2011). Sakawa - Cybercrime and criminality in Ghana. *Journal of Information Technology Impact, 11(2), 85–100*.

Cohen, L. E, Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*:588-608.

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activities approach. *American Sociological Review (44), 588–608*.

Computer Security Institute. (2005). CSI/FBI Computer Crime and Security Survey. Retrieved from www.gocsi.com.

Dehue, F., Bolmon, C., & Vollink, T. (2008). Cyberbullying: youngsters' experiences and parental perception. *Cyber Psychology & Behavior, 11,* 217-223.

EFCC develops software to combat cybercrime in Nigeria (2013, September 18). Daily Trust News, p. 1.

Finnie, T., Petee, T., & Jarvis, J. (Eds.).(2010). *Future challenges of cybercrime*. Virginia: Futures WorkingGroup.

Fitzgerald, J. D., & Cox, S. M. (2002). Research methods and statistics in criminal justice: An introduction (3rd ed.). Belmont: Wadsworth Thomson Learning.

Frye, V., Ompad, D. C., Chan, C., & Vlahov, D. (2011). Intimate partner violence perpetration and condom use-related factors: Associations with heterosexual men's consistent condom use. *AIDS and Behavior 15(1):*153-62. DOI: 10.1007/s10461-009-9659-2.

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

Hansen, J. R. (2007). Cybercrime prevention. In K. O'Shea, J. Steete, J.R. Hansen, C. B. R. Jean & T. Ralgh (2007). Cyber crime investigations: Bridging the gaps between security professionals, law enforcements and prosecutors(112-118). New York: SynGress Publishing.

Hassan, A. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science, 2(7), 626–631*.

Holt T, Bossler A. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30:*1-25.

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

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

Impact of cybercrime.(2013). Retrieved from http://resources.infosecinsti tute.com/2013-impact-
cybercrime/.

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

Internet crime complaint centre. (2013). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx

Internet crime complaint centre. (2016).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.

Jones, S. E., Manstead, A. S. R., & Livingstone, A. G. (2011). Ganging up or sticking together?

Group processes and children's responses to text-message bullying. *American Psychological Association.* https://psycnet.apa.org/record/2011-19758-005.

Leili, J. A. (2019). Bystander intervention, victimization, and routine activities theory: An examination of feminist routine activities theory in cyber space. *Scholar Commons*, University of Southern Florida. Retrieved from https://scholarcommons.usf.edu/.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cybercrime and organization of the police: The results of two empirical studies in the Netherland. *International Journal of Cyber Criminology, 7(1).*

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

Longe, O. B., & Osofisan, O. A. (2011). On the origins of advance fee fraud electronic mails: A technical investigation using internet protocol address tracers. *The African Journal of Information Systems, 3 (1), 27-34.*

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. Retrieved from https://doi.org/10.1103/ PhysRevLett.105.018904.

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 https://doi.org/10.1080/15332861.2010.487415*.

Microsoft's estimate. (2014). About one half of all adults connected to the Internet were victims of cybercrime. Retrieved from https://news. microsft.com/stories/cybercrime/.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young

people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention.*

Ndubueze, P. N, Igbo E. U. M, & Okoye, U. O. (2013). Cybercrime victimization among internet active Nigerians: An analysis of socio-demographic correlates. *International Journal of Criminal Justice Sciences*, 8 (2).

News Agency of Nigeria (2019, May 17). Cases of cybercrime in South East very alarming —EFCC. https://punchng.com/cases-of-cybercrime-in-south-east-very-alarming-efcc/

Nigeria Communication Commission. (2013-2016). The final report on effects of cybercrime on foreign direct investment and national development. Department of New Media and Information Security.

Obikeze, D. S. (1990). *Methods of data analysis in the social and behavioral sciences*. Enugu: Auto-Century Publishing.

Oblad, T. (2020). A Holistic Overview of cyberbullying across the world: Review of Theories and Models. DOI: 10.5772/intechopen.91433.

Odiga, H. (2012, July 29). EFCC, Nigerians raise alarm on hacking. *Vanguard Newspaper* [Daily News], p. 5.

O'Dea, M., & Rich, W. (2010). The not-so-distant average school day. In T. Finnie, T. Petee &

J. Jarvis (Eds.). Future challenges of cybercrime (pp. 51–55). Virginia: Futures Working Group.

Olusola, M., Ogunlere, S., &Semiu, A. (2013).Impact of cybercrimes on Nigerian economy. Babcock University. Retrieved from https://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/

Okpa, T. J.,; Ajah, B. O., Shiotse, E & Abang, T. A. (2022). Business E-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*. https://doi.org/10.1057/s41284-022-00354-1.

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 K. O'Shea, J. Steete, J.R. Hansen, C. B. R. Jean & T.

Ralgh (2007). Cybercrime investigations: Bridging the gaps between security professionals, law enforcements and prosecutors (112-118). New York: SynGress Publishing.

Reyns, B. W., Henson, B., Fisher, B. S. (2011). Being pursued online: applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Crim. Justic. Behav., 38 (11),* pp. 1149-1169. 10.1177/0093854811421448.

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

Shiloh, J., & Fassassi, A. (2016). Cybercrime in Africa: Facts and figures. Retrieved from SciDev.Net Sub-Saharan Africa.html.

Sidanius J, Liu, J. H., Shaw, J.S, Pratto, F. (1994). Social dominance orientation, hierarchy attenuators and hierarchy enhancers: Social dominance theory and the criminal justice system. *Journal of Applied Social Psychology, 24:*338-366.

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_C3Report.pdf.

Steffensmier, D. (1987). The inventor of the new senior citizen criminal. In L. J. Siegel (Ed), Criminology: Theories, patterns, and typologies (10th ed.) (pp. 169-173). Belmont, USA: Wadsworth Cengage Learning.

Symantec. (2018). Cybercrimes: 23 million Germans fell victims in 2017, Norton study. Retrieved from https://www.guardian.ng/newsletters.

Tench, S. A., 2019. Space-time modelling of terrorism and counter-terrorism. A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy of the University College London.

The current state of cybercrime. (2013). An inside look at the changing threat landscape. http:// www.rsa.com.

Udelue, M. C., & Mathias, B. (2019). Prevalence of cybercrimes among youths In Onitsha South Local Government Area of Ananmbra State, Nigeria. *Journal of Health and Social Inquiry, Vol. 5(1).*

Umoru, H. (2017, May 24). $450m lost to cybercrime in Nigeria —Senate. Retrieved from https://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/.

Uzoma, J. (2021, May 24). Police bust cybercrime syndicate in Imo State. https://tribuneonlineng.com/police-bust-cyber-crime-syndicate-in-imo/

Verecio, R. L. (2017). Applications of latent Dirichlet allocation algorithm of published articles on cyberbullying. *International Journal of Applied Engineering Research;12(21)*:10878-10884.

Wall, D. S. (2010). Foreword. In K. Jaishankar (Ed.*). Cyber criminology: Exploring Internet crimes and criminal behavior*. London: CRC Press.

Wilson, C. (1996). Software piracy: Uncovering mutiny on the cyber. In L. J. Siegel (Ed),

Criminology: Theories, patterns, and typologies (10th ed.) (pp. 441-467). Belmont, USA: Wadsworth Cengage Learning.

Wilson, J. Q & Herrnstein, R. (1985). *Crime and Human Nature*. New York: Simon & Schuster.

Wilson, J. Q, Kelling, G. L. (1982). Broken windows: the police and neighborhood safety. *Atl Mon 211*:29–38.

Wolfgang, M. (1958). *Patterns in Criminal Homicide. Philadelphia*: University of Pennsylvania Press.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407–427. https://doi.org/10.1177/147737080556056.