Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

OPEN ACCESS Asian Journal of Scientific Research

ISSN 1992-1454
DOI: 10.3923/ajsr.2020.205.213

Research Article
Cybercrime and Socio-economic Development of Corporate Organizations in Cross River State, Nigeria

[1]John Thompson Okpa, [2]Ilupeju, A. Adebayo and [3]Eshiotse Emmanuel

[1]University of Nigeria, Nsukka, Nigeria
[2]University of Calabar, Nigeria
[3]Department of Sociology, University of Calabar, Nigeria

Abstract

Background and Objective: The e-commerce is evolving at bolt speed and with it, a new threat has emerged, alongside the economic and strategic hazard that go with it: this new threat is cybercrime. This study examined the effect of cybercrime on the socio-economic development of corporate organizations in Cross River State, Nigeria. Specifically, the study examines the major cyber-attacks and effect of phishing on the socio-economic development of corporate organizations. **Materials and Methods:** Cross-sectional survey research design that allows the triangulation of quantitative and qualitative methods was opted for. Questionnaires were distributed to 1074 respondents purposively selected from 18 financial institutions, 4 telecommunication network providers and 2 manufacturing companies while in-depth interview were administered on 13 respondents across the organizations studied. Elicited data were analyzed using Pearson chi-square and the qualitative data were analyzed using content analysis. **Results:** The study found that major cyber-attacks experienced by corporate organizations in Cross River State vary with phishing, spam messages and hacking. It was also established that corporate organizations with many cyber-platforms are more likely to suffer declined productivity as a result of phishing than organizations with fewer cyber-platforms. **Conclusion:** The study therefore recommends that Nigerian government in partnership with corporate organizations should establish a national cyber-security centre to coordinate and implement cyber regulations as well as engage in comprehensive research to determine the prevalence, nature and magnitude of cyber-attacks on corporate organizations in the country.

Key words: Cybercrime, organised crime, socio-economic, development, phishing, hacking, spam, corporate, organization

Citation: John Thompson Okpa, Ilupeju, A. Adebayo and Eshiotse Emmanuel, 2020. Cybercrime and socio-economic development of corporate organizations in Cross River State, Nigeria. Asian J. Sci. Res., 13: 205-213.

Corresponding Author: John Thompson Okpa, University of Nigeria, Nsukka, Nigeria

Copyright: © 2020 John Thompson Okpa *et al.* This is an open access article distributed under the terms of the creative commons attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Cybercrime is one of the greatest, generally perplexing and maybe the most convoluted issues in the digital world. The cyberspace has provided an internet platform, which has enabled geometric growth, productivity, efficiency and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by corporate organizations across the globe[1-3]. The internet has challenged the limits and has made geography insignificant in the operations of corporate organization in this day-and-age[4,5]. Organizations from various part of the world can now freely access and utilize the comfort, convenience, ease, productivity and efficiency offered by the internet platform in their daily interactions with one another[6]. A growing number of organizations depend on the services and resources provided via the internet to satisfy the demands of their numerous customers[7]. The advent of the internet and the adoption and evolution of new technologies and products have made it easier for organizations, businesses and consumers to operate on a larger dimension, while, also enabling groups and individuals to be active participants in the global economy (The International Cyber Security Protection Alliance[8]. Globally, a remarkable number of organizations have welcomed this new technology and used it to transact one form of business or another. There is no gainsaying that the internet has become one of the most efficient ways of doing business in the 21st century, despite the challenge of cybercrime[9-11].

Ironically, this technological revolution has evolved to become a smart instrument used by criminal elements for various forms of fraudulent and criminal activities. This has constituted a cog in the wheel of progress of corporate organizations globally[12,13]. Cyber threats is a major issue in the African continent as a large portion of the tricky electronic mails and different detestable practices related with cybercrime are commonly discernible to the African web-scape[14]. It is observed that, among the copious misdemeanours committed daily, using modern telecommunication networks, Nigeria and some other developing countries like South Africa, Tanzania, Ghana, Egypt, Kenya, Rwanda, Uganda, among others are alleged to be at the forefront, particularly, with reference to sending deceitful, deceptive and spurious financial proposals all over the world[15]. A lot of cybercrime emanates and are perpetrated from the African continent and threats spread easily because many servers and computers are not appropriately ensured[14]. Cybercrime offenders in the continent exploit the convenience, speed as well as, the anonymity offered by information and communication technology (ICT), for purposes of committing unlimited number of criminal activities that have made and continue to make, many businesses in the continent go moribund.

Perpetrators of this crime, usually, take advantage of e-commerce system available on the internet to defraud victims who are mostly foreigners, corporations, bank customers and corporate organizations of thousands and sometimes, millions of dollars[16]. Cybercrime in Nigeria is largely perpetrated by both young and old adults, however, most of the young adults are students in various higher institutions of learning in the country as well as, unemployed graduates and school dropouts. They explore the liberty offer by the cyberspace to defraud, steal and engage in mind-boggling atrocities that affect the socio-economic development of corporate organizations in Nigeria. The alarming rise in incidents of cybercrime and the resultant financial implications have resulted to more than eighty per cent (80%) of e-businesses in Nigeria are prone to cyber-attacks, which consequently, threaten their existence and survival[17,18]. Young fraudsters get involved in hacking, cyber terrorism, cloning and defrauding unsuspecting victims, illicit drug trafficking, using tools such as password cracker, key loggers, network sniffers, port scanners, vulnerability scanners, among others[12,19].

Cybercrime remains one of the major security challenges confronting corporate organizations in the Cross River State[20]. This has resulted to loss of sensitive company information and reduced the competitive strength of most corporate organizations in the state. Reliable data on the incidence of cybercrime and its' effect on socio-economic development of corporate organization in Cross River State is lacking but news reports and statements by police and government officials give credence to the likelihood that the problem is increasing. Thus, the study examines the effect of cybercrime on socio-economic development of corporate organizations in Cross River State, Nigeria.

The study aims to fill the gap in knowledge on this discourse and make policy relevant suggestions on how to improve cyber-security of corporate organizations. The following research questions were raised which was transform into objectives and research hypothesis, (i) What are the major types of cybercrime perpetrated against corporate organizations in Cross River State? (ii) To what extent does phishing affect the productivity of corporate organizations in Cross River State?

MATERIALS AND METHODS

Cross-sectional survey design was adopted for the study. This design was used to establish, determine and assess what respondents know, believe or their experiences with regards to cybercrime[21]. This research was conducted from March, 2019 to January, 2020. The study was conducted in Cross River State, Nigeria. Cross River state has 3 senatorial Districts namely: Southern, Central and Northern Senatorial Districts, with 18 Local Government Areas and one hundred and ninety three (193) wards[3]. The study population was limited to employees working in selected corporate organizations in Cross River State, Nigeria. These corporate organizations include: Eighteen financial institutions, 4 telecommunication network providers and 2 manufacturing companies, based in the three senatorial district of Cross River State. The eighteen (18) financial institutions, 4 telecommunication network providers and 2 manufacturing companies were delineated into strata. Respondents were purposively selected from each of the strata. A sample size of one thousand and seventy-four (1074) respondents was drawn using Survey Monkey Sample Size calculator. The details are highlighted in Table 1.

Qualitative data was elicited using the in-depth interview guide. The in-depth interview is rich and insightful and was used to support the findings of the quantitative data. The in-depth interview was conducted among 13 purposively selected participants from selected corporate organizations. The inclusion criteria were, that respondents must have a computer set connected to the internet attacked to their desks and that they must be ICT staff and staff of information security unit of the banks as well as, engineers of these selected organizations. IDI was thematically and contently analyzed. The use of both quantitative and qualitative methods ensured complementarities of data and triangulation, which is emphasised in modern research.

Table 1: Spread of sample size

	Organizations		
Sample of financial institutions (Banks)	Sample proportion of staff	Proportion of staff	Sample size (n)
Access Bank	37	0.03	20
Diamond Bank	54	0.05	30
Eco Bank	95	0.09	53
First city monument Bank	80	0.08	44
Fidelity Bank	41	0.04	23
First Bank	308	0.29	171
Guarantee Trust Bank	37	0.04	20
Heritage Bank	17	0.02	9
Keystone Bank	22	0.02	12
Skye Bank	19	0.02	11
Stanbic Bank	32	0.03	18
Standard Chartered Bank	15	0.01	8
Sterling Bank	16	0.01	9
United Bank of Africa	54	0.05	30
Union Bank of Nigeria Plc	44	0.04	24
Unity Bank	14	0.01	8
Wema Bank	23	0.02	13
Zenith Bank	148	0.14	82
Total	1056		585
Sample of manufacturing companies			
Flour mills	384	0.48	213
UniCem	409	0.52	226
Total	793		439
Sample of telecommunication network providers			
9Mobile	17	0.19	9
Airtel	15	0.16	8
Glo	19	0.21	11
MTN	40	0.44	22
Total	91		50

Source: Field survey, 2018

The study observed all known ethical principles guiding social research such as informed consent, specific permission required for audio or video recording, voluntary participation and no coercion, participant right to withdraw and cultural sensitivity. The instruments were exposing to a pre-test. The pre-test was conducted using (5%) of the sample size in from respondents working in different corporate organization from the ones studied. The essence is to ensure that the data and findings of the study reverberate their set target. These instruments were validated by three senior lecturers in the Department of Sociology and Anthropology, University of Nigeria, Nsukka. The reliability of the questionnaire was determined using Cronbach alpha and a reliability coefficient of 0.86 was obtained. The analyses of quantitative data were done with descriptive statistics and Pearson chi square statistics using SPSS version 20 software. The data were presented using tables, bar charts and pie charts.

RESULTS

In all, 1074 questionnaires were distributed, while, 1002 were adequately completed, retrieved and used for the analysis. This puts the questionnaire return rate at 93.3% and was, therefore, considered suitable to be used for the data analysis. Majority of respondents (64.7%) of the respondents were male, while, (35.3%) were female as shown in Table 2.

Data presented in Fig. 1 shows that 0.7% of the respondents were 51years and above, followed by 9.1% of the respondents that were within 41-50 years. Also, 47% of the respondents were within 31-40 years while 43.2% were below 31 years. This implies that respondents who were within 31-40 years were the most common, followed by those that were below 30 years. In all, it implies that majority of the respondents (90.2%) were below 41 years.

Figure 2 depicts the distinct educational backgrounds of the respondents. It can be deduced from the pie chart that 0.5% of the respondents had only First School Leaving Certificate (FSLC), followed by 9.1% of the respondents that had General Certificate of Education (GCE) or Secondary School Certificate of Education (SSCE). Also, 14.9% had National Certificate of Education (NCE) or Ordinary National Diploma (OND), while, 62.9% had First Degrees in the forms of Higher National Diploma (HND) or Bachelor's Degree. There were also 12.7% of the respondents with Master's Degree or Doctorate. It can therefore be deduced from Fig. 2 that majority of the respondents (62.9%) had Bachelor's degree or Higher National Diploma. This further provides an insight on the literate status of the respondents and their ability to respond to the questionnaire items without help.

Data presented in Fig. 3 shows that 41.8% of the respondents work in manufacturing companies such as Flour mills and UniCem. Also, 4.5% of the respondents work in Telecommunication organizations such as 9 mobile, Airtel, Glo and MTN. The remaining respondents (53.7%) work in financial institutions, which are basically 18 commercial banks that operate in Cross River State (Table 1). The implication of this finding is that more than half of the respondents (53.7%) were from financial institutions. Furthermore, this composition is considered favourable for the study as financial organizations are evidently more attractive to cybercrime offenders.

In Table 3, it was observed that 42.1% of the respondents identified the primary function of their organization as that of production, while, 53.3% of the respondents indicated that

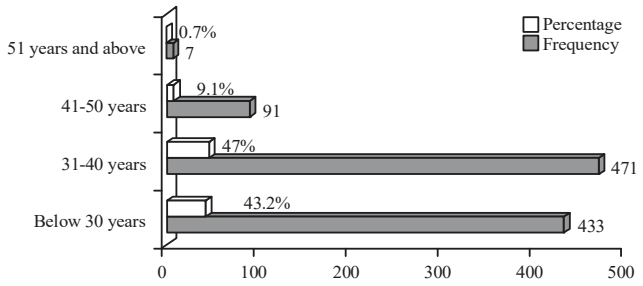

Fig. 1: Respondents' age distribution

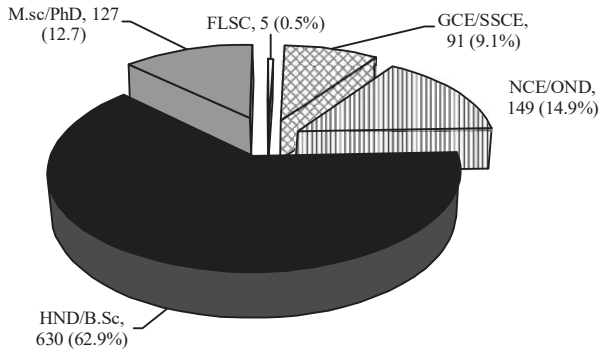

Fig. 2: Respondents' level of education

Table 2: Distribution of respondents by sex

Sex	Frequency	Percentage
Male	648	64.7
Female	354	35.3
Total	1002	100.0

Source: Field survey, 2019

Table 3: Distribution of respondents by the primary function performed by their organization

Primary function	Frequency	Percentage
Production	422	42.1
Financial services	534	53.3
Telecommunication services	43	4.3
Others	3	0.3
Total	1002	100.0

Source: Field survey, 2019

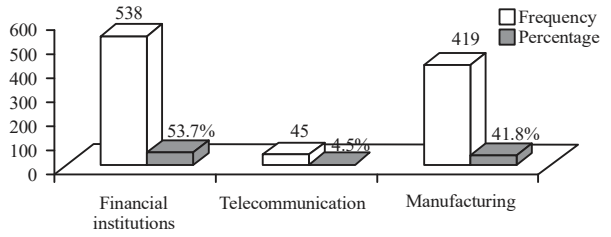

Fig. 3: Nature of organization

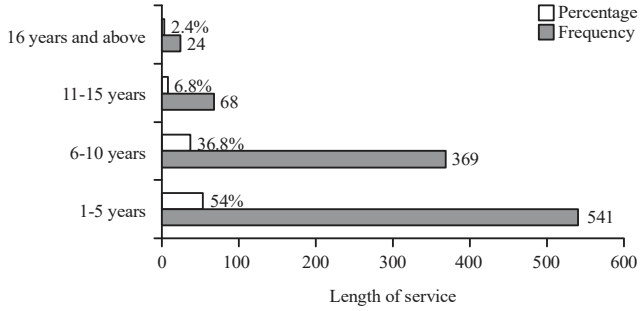

Fig. 4: Length of service

Table 4: Distribution of respondents on the most frequent cyber-attacks that is reported by their customer

Cyber-attacks on customers	Frequency	Percentage
Phishing	303	30.2
Virus dissemination	17	1.7
Spam messages	173	17.2
Denial of service	74	7.4
Identity theft	73	7.3
Cyber vandalism	83	8.3
Data modification	34	3.4
Theft of intellectual property	3	0.3
Hacking	159	15.9
No responses	83	8.3
Total	1002	100.0

Source: Field Survey, 2019

their organizations render financial services. Also, 4.3% of the respondents indicated that their organization's primary function is that of telecommunication services, while, 0.3% of the respondents gave other responses like procurement and distribution.

Data presented in Fig. 4 shows that 2.4% of the respondents have worked in their current organization for 16years and above. This was followed by 6.8% of the respondents that have worked in their organizations for 11-15 years. Also, 36.8% of the respondents indicated that they have worked in their organization for 6-10 years, while, 54% indicated that they have worked in their current organization for 1-6 years. This implies that more than half of the respondents (54%) have worked in their current organization for a period of 1-6 years.

Major cyber-attacks on corporate organizations: Aside the cyber-attack experienced by corporate organizations themselves, the cyber-attack experience of their customers was also considered in terms of reported incidence. As a result, the respondents were asked to indicate the most frequent cyber-attacks that are reported by their customer. The responses presented in Table 4 shows that 30.2% of the respondents indicated phishing as the most frequent cyber-attack suffered by their organizations reported by their customers. Also, 1.7% of the respondents indicated virus dissemination, 17.2% indicated spam messages, 7.4% indicated denial of services, while, 7.3% indicated identity theft. Other frequent cyber-attack reported by different proportions of the respondents includes cyber vandalism as indicated by 8.3% of the respondents, data modification (3.4%), theft of intellectual property (0.3%) and hacking (15.9%). The remaining 8.3% did not respond to the item. This further illustrate that phishing is the most frequent reported cyber-attack by customers of the sampled corporate organizations.

To further understand the dynamics of cybercrime in different organizations, its socio-economic development implications across organizations with distinct cybercrime reduction approaches, some variables were cross-tabulated. Data presented in Table 5 shows that the proportion of financial organizations that have been victims of phishing (46.1%) is comparatively more than the percentage of other organizations (12.5%) that have been victims of phishing. This was also the case with other forms of cyber-attacks like denial of services, spam messages and identity theft. However, with reference to cyber-attacks like hacking, only 1.7% of the respondents in financial institutions indicated hacking as the major cyber-attacks they have experienced, while, 27.4% of respondents in other organizations like manufacturing corporations and telecommunication organizations identified hacking as the major cyber-attack experienced in their organization. Cyber-attacks like theft of intellectual property, data modification, cyber vandalism and virus dissemination was also found to be comparatively higher in other organizations than was the case in financial institutions.

Test of hypothesis

Null hypothesis (H_0):

- Corporate organizations with many cyber-platforms are less likely to suffer financial loss as a result of phishing than organizations with fewer cyber-platforms

Table 5: Types of organizations and major cyber-attacks experienced

	Nature of organizations		
Major cyber attacks	Financial organization	Other organization	Total
Denial of services	35 (6.5%)	19 (4.1%)	54 (5.4%)
Spam messages	103 (19.1%)	50 (10.8%)	153 (15.3%)
Phishing	248 (46.1%)	58 (12.5%)	306 (30.5%)
Virus dissemination	5 (0.9%)	11 (2.4%)	16 (1.6%)
Identity theft	42 (7.8%)	13 (2.8%)	55 (5.5%)
Cyber vandalism	15 (2.8%)	79 (17.0%)	94 (9.4%)
Data modification	1 (0.2%)	37 (8.0%)	38 (3.7%)
Theft of intellectual property	2 (0.4%)	3 (0.6%)	5 (0.5%)
Hacking	9 (1.7%)	127 (27.4%)	136 (13.6%)
No response	78 (14.5%)	67 (14.4%)	145 (14.5%)
Total	538 (100.0%)	464 (100.0%)	1002 (100.0%)

Source: Field survey, 2019

Table 6: Organizations number of cyber-platforms and phishing induced declined financial gains

	Number of cyber-platforms		
Declined financial gain as a result of phishing	Fewer cyber-platforms	Many cyber-platforms	Total
Low	212 (50.5%)	220 (37.8%)	432 (43.1%)
High	208 (49.5%)	362 (62.2%)	570 (56.9%)
Total	420 (100.0%)	582 (100.0%)	1002 (100.0%)

$\chi^2 = 15.98^a$, df = 1, p = 0.000, N/B: Critical $\chi^2 = 3.841$, Source: Field survey, 2019

Substantive hypothesis (H_1):

- Corporate organizations with many cyber-platforms are more likely to suffer financial loss as a result of phishing than organizations with fewer cyber-platforms

This hypothesis was tested using with Pearson's chi-square statistics using question 18 on number of cyber-platforms operated by the organization and question 35, which measured the financial implication of phishing on the organizations was reworded as declined financial gains as a result of phishing. Organizations with less than three cyber platforms were coded as "fewer cyber-platforms", while, those with more than two cyber platforms were coded as "higher cyber-platforms". On the other hand, declined financial gain scores above the mean were coded as "high", while, decline financial gains scores within and below the mean score were coded as "low".

Data presented in Table 6 shows that more than half of the respondents in organizations with fewer cyber-platforms (50.5%) indicated that phishing induced declined financial gains in their organization is low, while, only 37.8% of respondents in organizations with many cyber-platforms share similar view. On the other hand, greater proportion of respondents in organizations with many cyber-platforms regarded phishing as resulting to high rate of decline-financial gains in their organization, while, only 49.5% of respondents in organizations with fewer cyber platforms regarded phishing as leading to high declined in financial gains.

The Pearson's chi-Square result was $\chi^2 = 15.98$, df = 1, with a p = 0.000 which is less than the alpha level of 0.05 implies that there is a statistically significant relationship between number of cyber platforms in an organization and the extent to which phishing is seen as reducing the organization's financial gains. As such, the null hypothesis (H_o) is rejected, while, the substantive hypothesis (H_1) is retained. The study, therefore, concludes that corporate organizations with many cyber-platforms are more likely to suffer declined financial gains as a result of phishing than organizations with fewer cyber-platforms.

The qualitative data indicated that phishing is the most common cyber-attack experienced by both corporate organizations and their customers. However, it might not be regarded as the attack with the most direct devastating econ-development impact on the organization. But, it is the most reported and most talked about because it affects the customers a great deal. One of the participants who identified phishing as the form of cyber-attack their organization has suffered the most in the past 10 years said:

- I think it is phishing. The target of cybercriminals is usually bank customers. They impersonate the bank and sent bulk SMS to bank customers phone numbers and e-mails address requesting them to provide sensitive information

such as card number, passwords, ATM Pin etc. These fraudsters know very well that it is difficult to attack bank platforms and that the easiest way of having access to the bank platforms is through the customer's account (IDI: Male Banker, 48, First Bank Plc)

A distinct insight was created by a participant who explained the dual dimension of cybercrimes in financial institution. He noted that both forms are experienced simultaneously and that their organization has witnessed such in recent times. According to him, Cybercrime in the banking sector can assume two major forms. They are direct and indirect fraud. The direct fraud includes money laundering, credit and debit card fraud, internet banking fraud, while, the indirect fraud include phishing, lottery scams, hacking, virus, etc. we have experienced both the direct and indirect fraud in this bank (IDI: Male Banker, 39, GT Bank).

DISCUSSION

The study found that cybercrimes of different types are perpetrated against corporate organizations in Cross River State, with 85.5% of the respondents indicating that their organizations have experienced some form of cyber-attack in the past ten years. This supports the findings of previous studies that cybercrime is on the increase, although, most go unreported. Hierarchically, majority of these attacks include, phishing, spam messages, hacking, cyber vandalism, identity theft, denial of services and data modification, among others[22]. This, to a larger extent, corroborates with the types of cybercrimes reported in previous study which include, phishing, network traffic, cyber stalking, data modification, cyber vandalism, identity theft and email bombing[9]. Also, other scholars reported cybercrime activities in Nigeria to include, virus dissemination, hacking, phishing, cracking, software piracy and pornography[23]. In this study, it was further established that corporate organizations in Cross River State are, however, not evenly affected by these attacks as different cyber-attacks occur more is some corporation. For example, denial of services, spam messages, phishing and identity theft occurs more in financial organizations, while, virus dissemination, data modification, theft of intellectual property and hacking occur more in other organizations like telecommunication and manufacturing organizations. Some of the aspect of cyber-attacks found to be common in financial organizations corroborates with previous study of cybercrime as an emerging threat to financial sector in Zimbabwe which revealed that phishing, hacking, identity theft and malware are some of the frequent types of cybercrime in banks[24]. On the other hand, the findings that virus dissemination occurs more in telecommunication and manufacturing organizations contrast with previous findings that financial organizations, specifically, banks are at the receiving end of the loss of credibility that results from virus dissemination attacks[25].

While, the above indicate cybercrimes that are experienced directly by the organizations, there were also reports of cybercrime by the customers of the various organizations. This was the case with 30.2% of the respondents who indicated phishing as the most frequent cyber-attack reported by their customers. Other forms of cyber-attacks reported by the customers, include, receiving of spam messages, hacking of their accounts, cyber vandalism, denial of services and identity theft. Acknowledging the fact of customers experiencing cybercrime, result from previous study noted that theft of information is among the key crimes perpetrated on cyber space that affects consumers and businesses alike[20].

Among the various types of cybercrimes observed in the current study, phishing stood out at 30.5% making it the most common cybercrime perpetrated against corporate organizations in Cross River State. It was also found to be the variant of cybercrime that is commonly reported by customers of these corporations. Previous studies revealed that deceitful electronic mails, which are an aspect of phishing, constitute one of the most prevailing aspects of cybercrimes in Africa's Internet landscape[14]. Phishing in the forms of sending deceitful, deceptive and spurious financial proposals all over the world is trending in most developing countries of the world of which Nigeria is an instance of Longe *et al.*[15]. Although, this relates with the position of the current study findings, it was, however, observed in this study that sending of fraudulent SMS is the most common mode of operation employed by phishers in the area, followed by false emails and calls. Similarly, previous study found that the nature of phishing in Amsterdam apart from involving fake e-mails and replication of websites, the perpetrators often goes as far as calling the victims using telephone to obtain transaction codes. Consequently and in line with one of the research objectives, the financial implication of phishing in corporate organizations was analysed[26]. It was shown that phishing has 5 key effects on the organizations' management and finances.

On the organization, generally, phishing affects brand reputation and image of the organization as indicated by majority of the respondents (92.1%). Again, the organization when exposed to phishing was also indicated by 94.9% to experience loss of trade and competitiveness. Other financial impact include that it decreases consumers' confidence in

online transactions, thereby, reducing patronage (93.6%) and also takes huge finances away from the organization as penalties and other compensatory payments may be required of the organization. This in some ways corroborates the position of extant studies which highlights various economic and other implications of phishing. Previous study for example, noted that phishing poses a huge threat to the e-commerce industry by shattering the confidence of customers from e-commerce activities and also causes huge financial loss to electronic service providers[27]. Additional study reported that phishing impact goes beyond the monetary loss experienced by the affected organizations as it also encompasses a destruction of the bond of trust built by organizations over the years[28]. Put differently, they found that phishing damages the organization's reputation and public confidence in the organization.

A related study observed the incidence of phishing among bank customers in the Netherlands, of which one-third of the respondents who have been victims of the fraud were aware of it before their victimization[29]. They, however, conclude that awareness and training on how to apply protective measures are critical factors in safeguarding online users from financial scams induced via phishing mechanism. In another study, respondents who are likely to fall victims of phishing were identified to include those with home users, persons with non-IT literacy background and people who are involved either directly or indirectly in the IT and computing industry[30]. The position of this study differs from the current study as number of cyber platform was among the major factors indicated to be associated with phishing induced financial loss[30]. Also, a related study concluded that the state of technical infrastructure in an organization affects the risk of victimization[31]. But such was not the case with the current study as ICT equipment maintenance did not significantly predict effect of cybercrime on socio-economic development corporation ($p>0.05$).

CONCLUSION AND RECOMMENDATIONS

Corporate organizations in Cross River State experience high level of cyber-attack as 85.5% have in the past ten years experienced significant cyber-attack of which phishing, Spam messages, hacking and cyber vandalism were the most prevalent. Apart from the corporate organizations, their customers have equally reported similar experience with phishing as the topmost in the list of cyber-attacks reported. Organizations with higher exposure to phishing experience more damages to their organizations' brand image and reputation, loss of trade and competitiveness and loss of consumers' confidence in the organizations product/services.

SIGNIFICANCE STATEMENT

This study discover that corporate organizations in the 21th century can only maximize the large business opportunities offered in the cyberspace as well as, reap from its ease of doing businesses by being connected to the cyberspace. The study will help the researcher to identify benefits associated with sound knowledge on the socio-economic implications of cyber-attacks on corporate organizations as well as measures to address specific attacks with more devastating effects that many researchers have ignored. Thus, a new theory on cyber security for corporate organization may be arrived at.

REFERENCES

1. Ndubueze, P.N. and E.U.M. Igbo, 2014. Third parties and cyber-crime policing in Nigeria: Some reflections. Policing: J. Policy Pract., 8: 59-68.
2. Odo, C.R. and A.I. Odo, 2015. The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. Global J. Comput. Sci. Technol., 15: 1-5.
3. Ipole, P.A. and J.T. Okpa, 2019. Working conditions and employees' productivity in Cross River state Civil Service, Nigeria. Eur. Scient. J., 15: 132-143.
4. Jaishankar, K., 2010. The future of cyber criminology: Challenges and opportunities. Int. J. Cyber Criminol., 1: 26-31.
5. Ndubueze, P.N., E.U.M. Igbo and U.O. Okoye, 2013. Cyber crime victimization among internet active Nigerians: An analysis of socio-demographic correlates. Int. J. Criminal Justice Sci., 8: 225-234.
6. Abdul-Rasheed, S.L., I. Lateef, M.A. Yinusa and R. Abdullateef, 2016. Cybercrime and Nigeria's external image: A critical assessment. J. Pan Afr. Stud., 9: 119-132.
7. Adewole, K.S., R.M. Isiaka and R.T. Olayemi, 2011. An inquiry into the awareness level of cyber security policy and measures in Nigeria. J. Sci. Adv. Technol., 1: 91-96.
8. ICSPA., 2016. A study on the impact of cyber crime on businesses in Canada. The International Cyber Security Protection Alliance (ICSPA), Buckinghamshire, UK. https://www.icspa.org/wp-content/uploads/2014/12/ICSPA-Canada-Cyber-Crime-Study-Report.pdf
9. Fanawopo, S., 2004. FG moves to enforce cybercrime laws. Daily Sun News, Johannesburg, South Africa, https://www.dailysun.co.za/

10. Das, S. and T. Nayak, 2013. Impact of cyber crime: Issues and challenges. Int. J. Eng. Sci. Emerg. Technol., 6: 142-153.
11. Okpa, J.T. and J.K. Ukwayi, 2017. Drug suspects perception of factors responsible for illicit drug trade in Cross River State, Nigeria. IOSR J. Humanit. Social Sci., 22: 80-87.
12. Okeshola, F.B. and A.K. Adeta, 2013. The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. Am. Int. J. Contemp. Res., 3: 98-114.
13. Ukwayi, J.K. and J.T. Okpa, 2017. The effect of electoral and economic crimes on sustainable development in Cross River State, Nigeria. Int. J. Social Sci. Res., 5: 32-42.
14. Quarshie, H.O. and A. Martin-Odoom, 2012. Fighting cybercrime in Africa. Comput. Sci. Eng., 2: 98-100.
15. Longe, B.O., V. Mbarika, M. Kourouma, F. Wada and R. Isabalija, 2009. Seeing beyond the surface: Understanding and tracking fraudulent cyber activities. Int. J. Comput. Sci. Inform. Secur., 6: 124-135.
16. Adomi, E. and S. Igun, 2008. Combating cyber crime in Nigeria. Electron. Library, 26: 716-725.
17. Akinsehinde, E., 2011. 80% of Nigerian businesses risk cyber-attacks. The Punch Newspaper, Nigeria, October 11, 2011, pp: 19.
18. Olayemi, O.J., 2014. A socio-technological analysis of cybercrime and cyber security in Nigeria. Int. J. Sociol. Anthropol., 6: 116-125.
19. Okpa, J.T. and I.D. Ekong, 2017. Global and national terrorism: Implications for sustainable development in Nigeria. IOSR J. Humanit. Social Sci., 22: 49-56.
20. Omodunbi, B.A., P.O. Odiase, O.M. Olaniyan and A.O. Esan, 2016. Cybercrimes in Nigeria: Analysis, detection and prevention. FUOYE J. Eng. Technol., 1: 37-42.
21. Ukwayi, J.K., J.T. Okpa, S.A. Adewoyin, P.U. Angioha and H.T. Udom, 2017. Security equipment and policing in central senatorial district of Cross River State, Nigeria. IOSR J. Humanit. Social Sci., 22: 6-14.
22. Boateng, R., L. Olumide, R.S. Isabalija and J. Budu, 2011. Sakawa-cybercrime and criminality in Ghana. J. Inform. Technol. Impact, 11: 85-100.
23. Maitanmi, O., S. Ogunlere, S. Ayinde and Y. Adekunle, 2013. Impact of cyber crimes on Nigerian economy. Int. J. Eng. Sci., 2: 45-51.
24. Mugari, I., S. Gona, M. Maunga and R. Chiyambiro, 2016. Cybercrime-the emerging threat to the financial services sector in Zimbabwe. Mediterr. J. Social Sci., 7: 135-143.
25. Duah, F.A. and A.M. Kwabena, 2015. The impact of cyber crime on the development of electronic business in Ghana. Eur. J. Bus. Social Sci., 4: 22-34.
26. Leukfeldt, E.R., 2014. Cybercrime and social ties. Trends Organized Crime, 17: 231-249.
27. Damodaram, R., 2016. Study on phishing attacks and antiphishing tools. Int. Res. J. Eng. Technol., 3: 700-705.
28. Ragucci, J.W. and S.A. Robila, 2006. Societal aspects of phishing. ACM SIGSOFT Software Eng. Notes, 31: 6-16.
29. Jansen, J. and R. Leukfeldt, 2016. Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. Int. J. Cyber Criminol., 10: 79-91.
30. Saudi, M.M., S. Ismail, E.M. Tamil and M.Y.I. Idris, 2007. Phishing: Challenges and issues in Malaysia. Int. J. Learn.: Annu. Rev., 14: 79-88.
31. Leukfeldt, E.R., 2015. Comparing victims of phishing and malware attacks: Unravelling risk factors and possibilities for situational crime prevention. Proceedings of the International Conference on Cyber Security, May 16-17, 2015, Redlands, CA., USA.