EFFECTS OF CYBERCRIME ON SOCIOECONOMIC DEVELOPMENT OF SMALL AND MEDIUM SCALE BUSINESSES IN OGBETE MARKET OF ENUGU STATE

By

[1]**Uzoigwe, Christopher Okoro**
Department of Computer Science, Federal University Wukari,
Taraba State, Nigeria

[2]**Ezenwaji, Chisom Ogochukwu**
Department of Sociology and Anthropology,
University of Nigeria, Nsukka

[3]**Asadu, Ngozi**
Department of Sociology and Anthropology,
University of Nigeria, Nsukka

[4*]**Deborah O. Obi***
Social Sciences Unit, School of General Studies, University of Nigeria, Enugu Campus

Corresponding author
[5]**Joy Chikaodili Omaliko**
Department of Sociology and Anthropology,
University of Nigeria, Nsukka

Abstract

Socioeconomic benefits remain a key element in every business organization. With cybercrime in the clime, businesses always anchor their engagements with suspicion and cynicism in the guard to avoid being defrauded or manipulated by internet fraudsters. Previous studies on cybercrime and cyber-attack control have not been able to fully address the cyber-attacks on small and medium scale businesses in Nigeria. Deviating from the conventional focus, this study examines the effect of cybercrime in socioeconomic development of small and medium scale businesses in Ogbete market of Enugu State. Both qualitative and quantitative methods of data collection were used in this study. The methods were divided into two: primary and secondary methods. The primary methods used were questionnaire and in-depth interviews. The questionnaire was used to gather quantitative data from 320 statistically determined respondents. The questionnaire consists of closed-ended and few open-ended questions. For the purpose of triangulation, the In-depth Interview (IDI) guide was designed for the qualitative aspect of the study. This was used to complement the quantitative instruments of data collection. The study found that business organisations in Ogbete market have experienced hacking into their business accounts and online platforms. The study, therefore, recommends that businesses need to create security policies and practices. This includes establishing rules for password creation, access controls, and data sharing. It is also important to develop a data protection plan in case of a data breach. This should include procedures for notifying customers and authorities and containing the damage. Equally, since the employees play a crucial role in protecting businesses from cyber-attacks, educating business employees on best practices for cybersecurity is essential. This includes teaching them how to identify suspicious emails and links, how to create strong passwords, and how to recognize and report cyber threats.

Keywords: Business organizations, Cyber-attacks, Cyber-fraud, Internet, Socioeconomic development.

Introduction

In a modern global setting where people are more connected than ever in history, the epithet of corruption and fraud spreads swiftly and do not only apply to people jumping queues or giving privileges to cronies, it is mostly pronounced in the domains of fraudulent activities perpetrated through the internet. These kinds of activities constitute what is known as cybercrime. Cybercrime includes the regular crimes that are widely known, like forgery, cheating, falsification, fraudulent representation of facts or impersonation – only that they are now carried out through the use of computer and internet (Ajah & Onyejegbu, 2019). The alarming increase in incidents of cyber-attacks and the resultant socioeconomic implications have made the management and security of the cyberspace a paramount concern to multi-stakeholders, driving the process, from the public to the private corporate institutions (Agugoesi, 2014:8). Hacking is a complicated technical activity aimed at exploiting systems' vulnerabilities to subvert security checks, geared towards compromising digital devices such as computers, smartphones, tablets, and networks of organisations for financial gains, corporate espionage and for fun.

Estimating the global economic impact of hacking is difficult since most organisations do not report or publish their financial losses. However, The Council of Economic Advisers (2018:8) estimated that malicious cyber activities cost the U.S. economy between $57 billion and $109 billion in 2016. In Kenya, several government websites came under hackers' attacks, putting huge amounts of citizens' data and even government revenue collection systems at risk. In 2012, over one hundred (100) Kenyan government websites were defaced by an Indonesian hacker with an estimated loss of $22.4 million. In South Africa, ATMs were massively compromised and huge sums of funds lost to the activities of the hackers in South Africa (Tobiko, 2014:7).

Equally, every successful attack, no matter how insignificant, attracts disastrous consequences for business organisations. The abuses of the cyberspace by hackers portend danger and have stalled the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and utilisation by corporate organisations in Nigeria. This development has widened the digital divide, crumbled the information infrastructure and affected consumer's confidence in online transactions in Nigeria (Oumarou, 2007; Salifu, 2008; Longe, Ngwa, Wada, Mbarika & Kvasny, 2009).

The disturbing rise in incidents of hacking and the resultant economic implications have made Akinsehinde (2011) and Olayemi (2014) to argue that more than eighty per cent (80%) of e-commerce in Nigeria are prone to hacking, which consequently, threatens their existence and survival. These scholars argue that web portals and web-based applications of the Central Bank of Nigeria, Nigeria Stock Exchange, banks, shopping malls, pension fund administrators and switching/electronic payment companies are vulnerable to attacks due to inadequate security measures for safeguarding their platforms. The cost of hacking is expected to grow exponentially in the distant future, as reliance on networked technology increases.

With the current high unemployment rate ravaging the nation, more young people across the country live below the poverty line, thereby; forcing some of them into internet-assisted crimes like hacking, phishing and other related vices (Ibrahim, 2016). Notwithstanding, most of the young adults are students in various higher institutions of learning in the country, as well as, unemployed graduates and school dropouts (Hassan, Lass & Makinde, 2012:12). They explore the liberty offered by the cyberspace to defraud, steal and engage in mind-boggling atrocities that impact negatively on the economic sustainability of corporate organisations in Nigeria. This study onerously studied the effect of cybercrime in socioeconomic development of small and medium scale businesses in Ogbete market of Enugu State.

Cybercrime in Nigeria

The penetration of internet in Nigeria created new ways of seeking opportunities offered by the internet. It was at this time that local fraudsters embraced the opportunity of the internet to go global and created a new version of fraud called cyber fraud (Jaishankar, 2007). According to Jansen and Leukfeldt (2016) cyber fraud includes all use of falsehood on the internet to gain a dishonest advantage. It is a type of cybercrime and is less diverse than cybercrime. Cybercrime includes all forms of criminal activities carried out on the internet. This includes hacking, cyber espionage, SIM swap, cyber fraud, and many more. Africa is most vested in cyber fraud. More sophisticated cybercrime activities also exist in Africa especially cyber-hacking of all sorts. In 2017, 50 graduating students from Makerere University Uganda were removed from graduating list in accusation of hacking into the University's system to change their grades (Abdi, 2016).

The bank systems are also often hit through direct hacking, malware planting, and many other more sophisticated means. Experts have estimated that over 80% of personal computers in Africa are infected with viruses and other malicious software that aid hacking and data loss. There are also rumors of a very gigantic network of malware-infested laptops called "botnet" that has the capacity to take down the whole internet (FranzStefan, 2010). Some of these sophisticated methods of cybercrime are manufactured and carried out in Africa while some are manufactured outside the continent but used in Africa – nonetheless, they all threaten African and global cyber security from Africa.

Similarly, the patterns of cyber fraud have evolved over time to match the changing social narratives between Africa and the rest of the world. In the early 2000s, Africa was newly opened to the world and both businesses and individuals scouted for big opportunities in the continent. Because the Western and European businesses thrived on trust and agreements, foreigners from both regions easily placed faith in dealing with business opportunities from Africa (Chinweze, Chukwuemeka, & Egbegi, 2019). At the time, the model of cyber fraud was to forge documents and sell hypothetical or fake products to foreigners through the internet.

They would search, study and send messages to target victims, bearing news of "unique" opportunities to buy items or make investments with guaranteed profits (Prince, 2019). Some of these messages are often too good to be true or so fashionably constituted that red flags are hard to detect.

Methodology

Study design and location

Cross-sectional design that allows the use of quantitative data was adopted. This design is considered appropriate for this study because it provides a better and comprehensive understanding of the problem under study. The study location is Ogbete Market in Enugu State.

Sample size and procedures

The sample size for this study was 320 which was drawn using Yamane (1967) formula for sample size generation. The formula is shown below. A 95% confidence level and level of maximum variability (P = 0.05) were assumed. The formula for the sample size estimation is given as: $n= \frac{N}{1+N\,(e)^2}$

Where:

n = the sample size
N = the population size
e = the level of precision (allowable error) that is 5% or 0.05.
Therefore, the sample size estimation is given as:

$$n = \frac{1600}{1+\,1600\,(0.05)^2}$$

$$n = \frac{1600}{5}$$

n = 320

This sample size was therefore considered fair to represent the entire universe for this study.

Methods of data collection and Analysis

Data for this study were primarily collected through questionnaire and In-depth Interview (IDI) guide. On the other hand, data were secondarily sourced through the library and other documents dealing with the internet system. Accordingly, responses from respondents, as were generated through interviews, were subjected to content analysis while the quantitative components of data generated were presented using frequencies and percentages.

Results

Inferring from the sample size, a total of 320 questionnaire were distributed to business owners in Ogbete market of Enugu State. From this number that were distributed, 307 were correctly filled and returned. This formed the basis for this analysis.

Table 1: Distribution of the respondents by whether they had experienced cyber attacks

Experienced cyber attack	Frequency	Percentage (%)
Yes	262	85.3%
No	45	14.7%
Total	307	100%

Source: Field Survey, 2022

The responses presented in Table 1 shows that 85.5% of the respondents affirmed that their businesses in Ogbete market have experienced cyber-attackd while 14.5% indicated that their businesses have not experienced cyber-attacks. This implies that majority of the respondents were of the view that their businesses have experienced cyber-attacks.

Responding to whether his business has been attacked by cybercriminals a participant said:

> Yes, my business has been attacked and you see, POS operators are often at the biggest risk of hacking attacks because of the money at their disposal. This is contrary to the assumption that cyber threats are aimed only at bigger organisations.

His position was further corroborated by another participant who said

> The activities of cyber criminals are routinely experienced by small and medium scale businesses. According to him, some of his business neighbours do experience breaches on their business accounts.

Another participant noted:

> The inevitability of online financial transaction in the current era of information and communication technology makes possibility of cyber-attacks high while perceiving cyber-attacks as the negative side of the advancement with financial institutions as the most targeted organisations.

Information and communication technology has rapidly transformed all facets of businesses, making almost every business organisation to own at least one computer platform. Odo and Odo (2015) emphasized the relevance of communication technology for many businesses noting that it is central in growing and sustaining successful businesses. This development invariably has impacts on small and medium scale business organisations as information technology brought with it a new dimension of crime, known as cybercrime with its divergent types and dimension (Falashade & Abimbola, 2013; Ukwayi & Okpa, 2017). A study by Ilmudeen (2013) shows that 68% of the respondents reported that they had experienced virus infection on their personal computer, more than half of which was attributed to online related factors like harmful websites, absence of antivirus, lack of anti-virus update and too much internet surfing. However with the case of studies outside the African continent the current findings could be regarded as relatively low as in Singhal (2014) study, 94% of the respondents confirmed that they have experienced virus attack in the course of their daily work schedule.

Table 2: Distribution of the respondents by whether they reported their experienced cyber-attack to the police

Report to the police	Frequency	Percentage (%)
Yes	10	3.3%
No	294	95.7%
Not aware	3	1.0%
Total	**307**	**100.0**

Source: Field Survey, 2022

Aside the attacks, 3.3% of the respondents reported the cyber-attacks in their businesses to the police, 95.7% of the respondents did not report such attacks, while 1.0% of the respondents said they are not aware whether or not such attacks was reported. This implies that majority of the respondents (95.7%) did not report such attacks in their businesses to the police. Responding to the reason they failed to report to the police, an IDI respondent said:

> I have been badly treated by the police in the past and I still perceive them as part of the problem one should be mindful of. Is it not the same police that illegally stop and extort money from the people at will that you expect me to report my experience to?

Another respondent had this to say:

> Some of the victims were physically and emotionally traumatized to the extent that they even consider reporting to the police as part of the problems. They may be afraid the police would not find and punish the perpetrators.

This supports Boateng, Olumide, Isabalija and Budu (2011) findings 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. This to a larger extent corroborates with the types of cybercrimes contained in Fanawopo (2004) which include phishing, network traffic, cyber stalking, data modification, cyber vandalism identity theft and email bombing. Also, Olusola et al (2013) reported cybercrime activities in Nigeria to include virus dissemination, hacking, phishing, cracking, software piracy, and pornography.

Table 3: Distribution of the respondents by how they know their businesses have been attacked

How to identify virus attack	Frequency	Percentage (%)
System slowdown in performance	261	85.0%
Unwanted messages and alert messages	32	10.4%
Failure in application functionality	14	4.6%
Total	307	100.0

Source: Field Survey, 2022

Data presented in table 3 shows that 85.0% of the respondents indicated slow-down in system performance as the mechanism through which they know that their business has been attacked by virus. Also, 10.4% of the respondents indicated unwanted and alert messages as their own way of knowing when their business has been attacked by virus, while 4.6% indicated failures of business electronic applications to perform their designed functions. This implies that slowdown in system performance is the most common mechanism through which majority of the businesses have been attacked by virus.

E-commerce by its global nature offers endless opportunities for businesses to triumph as its market resides in all part of the world. This advantage can be regarded as one of the ground breaking aspect of ICT oriented businesses of the 21st century. However given the fluid nature and often difficult to trance nature of financial transactions carried out using internet platforms, cyber criminals have enormously taking undue advantages of such weakness to perpetrate numerous financial frauds against individuals and business organisations. This introduces a new dimension in the study of cybercrimes against business organisations as distinct from existing literature like that of Jaishankar (2010) which took cybercrime as externally perpetrated act that targets corporate organisations.

Table 4: Distribution of the respondents on the measures taking to prevent their businesses from being hacked

Measures	Frequency	Percentage (%)
Sensitization of their workers and staff	60	19.5%
Non-use of mobile apps	33	10.8%
Continuous monitoring and reporting of transactions in their banks	214	69.7%
Total	**307**	**100**

Field survey, 2022

Data presented in Table 4 shows that 19.5% of the respondents indicated that their organizations engage in sensitization of their workers and staff as a way of preventing their businesses from being hacked. Also, 10.85 indicated their non-use of mobile apps as a way of warding off hackers while 69.7% of the respondents indicated their continuous monitoring and reporting of transactions in their accounts to the bank as a way of preventing and controlling their businesses from being hacked.

Danguah and Longe (2011) emphasized the relevance of public awareness through what they tagged, "providing of insights to the public", yet went further to enlist legal action enforcement as also needed to curb cybercrimes. While reiterating the legal dimension, Boateng, Olumide, Isabalija and Budu (2011) observed the negative impact of inadequate legislation/legal framework in the fight against cybercrime activities and like Dzomira (2014) emphasized the need for all stakeholders to be involved in the attempt to put the activities of cyber criminals to check.

Conclusion and recommendations

Cyber-attacks have been a major concern of all internet users; especially those who rely on it for business and governments through relevant agencies in collaboration with business organisations have made attempts to safeguard businesses and clients from cyber-attacks. However, reports of cyber victimization persist with millions often lost to cyber criminals. This has necessitated series of studies on cybercrime. A common denominator in these studies is the acknowledgement of cybercrime as part of the larger technology fallout which has fostered a new dimension of crime and risk. Nonetheless, the pace at which business organisations subscribes to e-commerce irrespective of the dangers posed by cybercriminal activities led the current study to investigate the effect of cyber-attacks on the socioeconomic development of businesses in Ogbete market of Enugu State. The study calls for businesses to create security policies and practices. This includes establishing rules for password creation, access controls, and data sharing. It is also important to develop a data protection plan in case of a data breach. This should include procedures for notifying customers and authorities and containing the damage. Equally, since the employees play a crucial role in protecting businesses from cyber-attacks, educating business employees on best practices for cybersecurity is essential. This includes teaching them how to identify suspicious emails and links, how to create strong passwords, and how to recognize and report cyber threats.

References

Ajah, B. O. & Chukwuemeka, O. D. (2019). Neo-economy and militating effects of Africa's profile on cybercrime. International Journal of Cyber Criminology 13(2), 326-342.

Akinsehinde, E. (2011, October 11). 80% of Nigerian businesses risk cyber-attacks. The Punch Newspaper Tue, pp. 19.

Alsayed, A. O. & Bilgrami, A. L. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. International Journal of Emerging Technology and Advanced Engineering, 7(1), 109-115.

Ayofe, A. N. & Irwin, B. (2010). Cyber security: Challenges and the way forward. GESJ: Computer Science and Telecommunications, 6(29), 56-69.

Babbie, E. (2010). The practice of social research. London: Wadsworth Cengage Learning.

Barber, R. (2001). Hackers profiled—who are they and what are their motivations? Computer Fraud Security (2), 14-17.

Bratus, S. (2007). What hackers learn that the rest of us don't: notes on hacker curriculum. IEEE Secur Priv, 5(4), 72-75.

Das, S. & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142-153.

Duah, F. A. & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in Ghana. European Journal of Business and Social Sciences, 4(1), 22-34.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Governance & Control: Financial Markets & Institutions, 4(2), 3-26.

Fanawopo, S. (2004). FG moves to enforce cybercrime laws.

Folashade B. O. & Abimbola, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114.

Frank, I. & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education, 1(1), 1-11.

Hassan, A. B., Lass, F. D. & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology, 2(7), 626-631.

Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. In: Cybercrime and computer forensic (ICCCF), IEEE International Conference on (pp. 1-9). Vancouver: IEEE.

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. International Journal of Cyber Criminology (IJCC), 1(2), 26–31

Kamini, D. (2011). Cybercrime in the society: Problems and preventions. Journal of Alternative Perspectives in the Social Sciences, 3(1), 240-259.

Karim, S. S. (2016). Cyber-crime scenario in banking sector of Bangladesh: An overview. The Cost and Management, 44(2), 12-19.

Kubina, M. & Koman, G. (2016). Big data technology and its importance for decision-making in enterprises. Communications - Scientific Letters of the University of Zilina, 18(4), 129-133.

Lee, K. J. & Song, I. (2007). Investigating information structure of phishing emails based on persuasive communication perspective. Journal of Digital Forensics, Security and Law, 2(3), 29-44.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unravelling risk factors and possibilities for situational crime prevention. Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

Longe, B. O., Ngwa, O., Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal use of information and communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. Journal of Information Technology Impact, 9(3), 155-165.

Longe, B. O., Ngwa, O., Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal use of information and communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. Journal of Information Technology Impact, 9(3), 155-165.

Makeri, Y. A. (2017). Cyber security issues in Nigeria and challenges. International Journal of Advanced Research in Computer Science and Software Engineering, 7(4), 315-321.

Manne, K. (2020). Inside the mind of a hacker.http://www.buffalo.edu/ubnow/stories/2020/02/psych-profile-hackers.html

Manufacturing Association of Nigeria, Cross River State Chapter yearly bulletin (2018).

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), 225-234.

Nnam, M. U., Ajah, B. O., Arua, C. C., Okechukwu, G. P. & Okorie, C. O. (2019). The War must be Sustained: An integrated theoretical perspective of the Cyberspace-Boko Haram terrorism nexus in Nigeria. International Journal of Cyber Criminology 13(2), 379-395.

Odo, C. R. & Odo, A. I. (2015). The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. Global Journal of Computer Science and Technology: H Information & Technology, 15(3), 1-6.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116-125.

Olson, P. (2013). We are anonymous: inside the hacker world of LulzSec, anonymous, and the global cyber insurgency. Back Bay Books, New York.

Olusola, M., Samson, O., Semiu, A. & Yinka, A. (2013). Impact of cyber-crimes on Nigerian economy. The International Journal of Engineering and Science (IJES), 2(4), 45-51.

Oumarou, M. (2007) Brainstorming advanced fee fraud: 'Faymania'–the Cameroonian experience. In: N. Ribadu, I. Lamorde and D. Tukura (Eds), Current trends in advance fee fraud in West Africa. EFCC, Nigeria, 33-34.

Oyelere, S. S. & Oyelere, L. S. (2015). Users' perception of the effects of viruses on computer systems – An empirical research. African Journal of Computing & ICT, 8(1), 121-130.

Peters, A. & Jordan, A. (2019). Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime

Quarshie, H. O. & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. Computer Science and Engineering, 2(6), 98-100.

Ragucci, J. W. & Robila, S. A. (2006). Societal aspects of phishing. ACM SIGSOFT Software Engineering Notes, 31(7), 6-16.