MALWARE VICTIMISATION AND ORGANISATIONAL SURVIVAL: A MULTI-METHOD EXPLORATION OF EMERGING MARKET

James Ajor Ogar [*], John Thompson Okpa [**], Thelma Aya Abang [*], Fredrick Awhen Opoh [***], Francis Abul Uyang [*], Bassey Ballantyne Ikpeme [****], Rosemary Ine Eneji [*], Augustine Eze Bassey [*], Patrick Owan Bisong [*], Chukwudi Charles Ezikeudu [*], Edem Ebong [*****]

* Department of Sociology, University of Calabar, Calabar, Nigeria
** *Corresponding author*, Department of Sociology, University of Calabar, Calabar, Nigeria
Contact details: University of Calabar, Etagbor, PMB 1115 Calabar, Cross River State, Nigeria
*** Social Science Education, University of Calabar, Calabar, Nigeria
**** Department of Social Work, University of Calabar, Calabar, Nigeria
***** Institute of Public Policy and Administration, University of Calabar, Calabar, Nigeria

OPEN ACCESS

How to cite this paper: Ogar, J. A., Okpa, J. T., Abang, T. A., Opoh, F. A., Uyang, F. A., Ikpeme, B. B., Eneji, R. I., Bassey, A. E., Bisong, P. O., Ezikeudu, C. C., & Ebong, E. (2023). Malware victimisation and organisational survival: A multi-method exploration of emerging market [Special issue]. *Journal of Governance & Regulation, 12*(3), 377–388. https://doi.org/10.22495/jgrv12i3siart19

ISSN Online: 2306-6784
ISSN Print: 2220-9352

Received: 15.05.2023
Accepted: 26.09.2023

JEL Classification: O1, O3, O4, L4
DOI: 10.22495/jgrv12i3siart19

Abstract

The internet has gained widespread acceptance globally since its inception. However, the escalating threats associated with this acceptance are alarming, as cyber fraudsters continually imitate and execute grievous attacks on corporate entities. While much is known about the various dimensions of malware attacks and defense (Sharmeen et al., 2019), little attention has been given to how malware affects the socio-economic survival of organizations in Nigeria, particularly in Cross River State. This article aims to bridge this knowledge gap by presenting empirical evidence on how malware victimization impacts organizational survival in the study area. Through the use of questionnaires and in-depth interviews, a sample of 1,074 research participants, including bank staff, industrial workers, and telecommunication staff, was selected from Cross River State using a multi-stage sampling technique. The findings reveal a significant increase in malware victimization among corporate organizations in Cross River State, resulting in severe consequences for their socio-economic development. To mitigate these risks, the study recommends that organizations strengthen their network security, implement comprehensive cybersecurity awareness training programs for employees, adopt advanced detection and response technologies, and employ mobile security solutions or business internet traffic security measures to ensure their safety.

Keywords: Corporate Organisations, Development, Malware, Cybercrime, Socio-Economic & Victimisation, Nigeria

Authors' individual contribution: Conceptualization — J.A.O., J.T.O, and F.A.O.; Methodology — T.A.A., F.A.U., B.B.I., and C.C.E.; Validation — A.E.B.; Formal Analysis — R.I.E. and P.O.B.; Investigation — E.E.; Resources — T.A.A., R.I.E., and P.O.B.; Writing — Original Draft — J.A.O., J.T.O., and C.C.E.; Writing — Review & Editing — R.I.E.; Visualization — T.A.A., F.A.U., B.B.I., and P.O.B.; Supervision — T.A.A. and E.E.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgment: The Authors would like to express our utmost appreciation to Professor C. U. Ugwuoke and all the respondents who participated in this study.

1. INTRODUCTION

Internet expansion and widespread adoption have led to an upsurge of cyber risks. In Nigeria today, different forms of cybercrimes are committed on a daily basis, ranging from phishing, business email compromise (BEC), hacking, cyber vandalism, cyber espionage, and malware attacks (Okpa et al., 2020). Malware attacks — a variant of cybercrime — are increasing in frequency, dimension, and sophistication, thus posing a serious threat to the socio-economic development of corporate organizations, Internet users, and national security (Ajah & Chukwuemeka, 2019; Nnam et al., 2019). The destructive intention of malware is to overwhelm, manipulate, and damage computers, whether personal or corporate, without the knowledge of the user (Okpa, et al., 2022). For this reason, countries like Kenya, Angola, Nigeria, Rwanda, Botswana, Uganda, Tanzania, and South Africa lose billions of dollars annually to malware attacks and other cyber-related offenses (Infocyte, 2017).

While analyzing the effect of malware invasion on organizations' information and communications technology (ICT) equipment, Sharmeen et al. (2019) identified the loss of revenue, process breakdowns, and even an outright shutdown of industrial and system activities as possible outcomes of malware attacks on an organization. Similarly, Jennings et al. (2019) argue that malware attacks are on the rise, and their effects on businesses are debilitating, consequently affecting organizational productivity, financial performance, and brand. Gilbert-Knight (2012) defines malware as any malicious software, such as viruses, ransomware, scareware, and spyware, among others, that disrupts the proper functioning of a computer system. The malware can make the computer malfunction by erasing data or hijacking the operations of the hardware. It is usually used to frustrate the user and make it impossible for them to access their personal/official data. This explains why Vijayanand and Arunlal (2019) classify and categorize malwares according to their behavior patterns. Gábriš and Hamuľák (2021), categorized malware into two classifications: "*family*" and "*variant*". The term "*family*" denotes a unique or initial malware piece, whereas "*variant*" designates an altered version of the principal malevolent code or family with only slight modifications.

Reporting on the dynamic nature of malware attacks, Jennings et al. (2019) state that malicious actors leverage automated software and other ICT tools to target small businesses and large corporations. This shows that no organization, whether big or small, production companies, or service providers, is immune to malware attacks. More recently, scholars such as Lévesque et al. (2018) have employed a quantitative approach to explore the interactions between users, antivirus (AV) software, and malware as they occur on deployed systems. Another form of malware known as ransomware, in a bid to avoid being traced, demands that its ransom be paid through bitcoin. This makes their input low and their profit very high, in addition to their operational anonymity (Jennings et al., 2019). Literature from both developed and developing nations has highlighted operational methods deployed by malware writers, including *"code obfuscation and modification or inclusion of new behavior in the malware to improve strength and viability*" (Gounder & Farik, 2017, p. 318). Gounder and Farik (2017) explore innovative methods to combat malware. They posit that code obfuscation complicates and disguises malware code, making it more difficult for malware detectors to identify. This technique also minimizes the size of the code, thereby simplifying and accelerating the download and deployment process of malware. These strategies are typically categorized as either "*polymorphic*" or "*metamorphic*".

The corporate organizations' ICT components are often the major victims of malware attacks due to a failure to secure their operating system designs and other related software vulnerabilities (Shubbar, 2022). Software vulnerabilities, according to Organisation for Economic Co-operation and Development (OECD, 2008), are a function of faulty coding, software not properly configured, or used in a manner not compatible with the suggested uses or improperly configured with other software. These factors allow for loopholes that expose corporate entities to malware attacks. In the event that internet fraudsters find these flaws, malicious software is created to take advantage of them (Akrim & Dalle, 2021). Non-technological factors, such as bad user behaviors and ineffective security policies and processes, may put a company at risk of malware infection. Malwares such as viruses or Trojans must be triggered by some kind of user activity, such as clicking on a seemingly trustworthy file or link, opening a phishing email, or visiting a compromised website, as well as through physical media such as external drives. Shires (2022) observes that once the security of a system has been breached through an initial malware attack, it can often lead to the automatic installation of extra malicious features. These can include elements such as spyware (like keyloggers), backdoors, rootkits, or other types of malware, which are collectively referred to as the payload. The vulnerability of Nigerian businesses to malware attacks has been an issue of great concern and the subject of serious debate at various cyber security conferences. Despite frantic efforts being made to secure the Nigerian cyberspace, the country is still vulnerable to a wide range of malware attacks owing to an ineffective legal and regulatory cybersecurity framework (Abdul-Rasheed et al., 2016; Abdulhamza, 2022; Suanpang et al., 2022).

Despite the extensive study that has been done on the many ways that malware may be attacked and defended against (Baeewe, 2021, Okpa et al., 2020; Suanpang et al., 2021), much has not been achieved when it comes to how malware affects the socio-economic development of organisational survival, particularly in Nigeria. This article therefore seeks to contribute to the ongoing cyber security debate by analysing the socio-economic implications of malware attacks on the survival of organisations in Cross River State, Nigeria from an empirical standpoint. The specific objectives of this study are: 1) examine the incidence of malware attacks, 2) determine the nature of malware attacks experienced by corporate organisations, 3) identify the medium through which malwares gain access to organisation's ICT equipment, 4) analyse factors responsible for malware attack, 5) determine

the relationship between malware attacks and socio-economic development of corporate organisations. The following research questions were formulated to guide the study:

RQ1: What is the nature of malware attacks experienced by corporate organisations?

RQ2: What are the medium through which malwares gain access to organisation's ICT equipment?

RQ3: What are the factors responsible for malware attacks?

RQ4: How do malware attacks relate with socio-economic development of corporate organisations?

The study on malware victimization and its impact on organizational socio-economic development is significant for understanding the consequences of cyber threats, informing decision-making processes, enhancing organizational resilience, and contributing to academic knowledge. By addressing these issues, the study can ultimately contribute to the development of effective cybersecurity measures and promote socio-economic growth in the face of evolving cyber threats. The study employed a cross-sectional survey design, utilizing a combination of quantitative and qualitative methods to gather data. This study made a significant contribution to the understanding of malware victimization and its effects on the organizational survival of corporate organisations. By examining the impact of malware attacks on various aspects of organizational functioning, the study provided valuable insights into the broader implications of such cyber threats. Through the use of both quantitative and qualitative methods, the research was able to capture a comprehensive view of the issue, allowing for a deeper understanding of the challenges and potential solutions. Overall, this study expanded the knowledge base surrounding malware victimization and its implications for organizational survival in Cross River State.

The structure of this paper is as follows: Section 1 captures the introduction, Section 2 reviews the relevant literature, Section 3 analyzes the methodology, Section 4 focuses on the results and discussion of findings, while Sections 5 and 6 present the conclusion and recommendations.

2. LITERATURE REVIEW

The technology adoption theory, also known as the diffusion of innovations theory, was developed by sociologist Everett Rogers in 1962. Rogers (1962) proposed this theory to explain how, why, and at what rate new ideas and technologies spread within a social system. His work was based on extensive research and analysis of the adoption patterns of various innovations in different fields, including agriculture, healthcare, and communication. The technology adoption theory suggests that the adoption of a new technology follows a bell curve pattern, with different groups of individuals categorized based on their willingness to adopt new innovations. These groups include innovators, early adopters, early majority, late majority, and laggards. The theory is a framework that examines the factors influencing the adoption and effective use of technology within organizations (Rogers, 1962). It posits that malware attacks, which refer to malicious software or code designed to exploit vulnerabilities in computer systems, can significantly impede the adoption and utilization of technology in corporate settings (Okpa et al., 2021; Okpa et al., 2022). When an organization becomes a target of a malware attack, it can experience various detrimental consequences such as financial losses, reputation damage, and operational disruptions.

Financial losses resulting from malware attacks can be substantial. Organizations may incur expenses related to incident response, remediation, and recovery efforts. These financial burdens can strain the organization's resources and impede its ability to invest in new technologies or allocate funds for digital transformation initiatives (Ushie & Okpa., 2021; Okpa, et al., 2022). Moreover, the cost of cybersecurity measures, such as acquiring robust security systems and training personnel, further adds to the financial burden. The reputation of an organization is critical for its success and sustainability (Nzeakor et al., 2022). Malware attacks can tarnish the reputation of an organization, especially if customer data is compromised or if the attack receives media attention (Emmanuel et al., 2021). Stakeholders, including customers, partners, and investors, may lose trust in the organization's ability to protect sensitive information. The negative perception generated by such incidents can deter potential customers, limit business opportunities, and even lead to customer churn. Operational disruptions caused by malware attacks can significantly impact an organization's ability to function effectively. For example, ransomware attacks can encrypt critical data, rendering it inaccessible until a ransom is paid. This can disrupt essential operations, halt productivity, and lead to significant downtime. The resulting delays and inefficiencies can hinder an organization's ability to meet deadlines, deliver products or services, and maintain customer satisfaction (Ajah & Chukwuemeka, 2019).

These negative consequences collectively contribute to a sense of reluctance and fear among decision-makers within the organization. Executives and managers may become hesitant to invest in new technologies or embark on digital transformation initiatives due to concerns about potential vulnerabilities and the associated risks of malware attacks (Nzeakor et al., 2022). The fear of experiencing financial losses, reputation damage, and operational disruptions can create a risk-averse culture within the organization, slowing down its socio-economic development. The theory did not "*give existence*" to any specific technology. Instead, it provides a framework to understand and predict the adoption and diffusion of innovations within a social context.

3. METHODS

3.1. Data and sampling technique

The research sample consisted of 1,074 male and female employees selected from 18 financial institutions, 4 network providers, and 2 production companies within the study area. The sample size of 1,074 was determined using the Survey Monkey sample size determinant, with a confidence level of

95% and a maximum variability level of $P = 0.02$. Out of this sample, 1,002 respondents were used for analysis. This represents a return rate of 93.3%, which is considered satisfactory for conducting data analysis.

The study employed a stratified proportional and purposive sampling approach to select research participants and respondents. The use of stratified proportional sampling segmented the study elements into twenty-four distinct strata. A total of 18 financial institutions, 4 network providers, and 2 production companies situated within Cross River State were selected. Participants were selected conveniently from each stratum. The participants in this study were individuals working in the field of ICT and were employed by various organisations. They had consistent access to a computer connected to the internet at their workstations. Additionally, the study included engineers employed by the selected organisations.

3.2. Design, study description and scope

The study adopts a descriptive and cross-sectional research design. This design is deemed suitable for this research because it provides a deeper and more thorough grasp of the issue being investigated. The study was conducted in 18 financial institutions, 4 telecommunication companies, and 2 manufacturing industries in the study area. Eighteen (18) commercial banks are located across the state. While the presence of a first-generation bank like First Bank of Nigeria Plc is felt both in the urban and rural areas of the state, the same cannot be said for the new generation banks, whose presence is mostly visible in urban areas such as Calabar, Ugep, Obubra, Ikom, Ogoja, Etung, Biase, Obudu, and Odukpani.

3.3. Data collection

A blend of quantitative and qualitative procedures and methodologies for data collection was adopted to obtain an insightful view of respondents' experiences of malware victimisation in Cross River State, Nigeria. This included a comprehensive review of existing literature, statistics, and field research conducted on corporate organizations in Nigeria. A total of 1,074 questionnaires were administered to the staff of 18 financial institutions, 4 telecommunication companies, and 2 manufacturing industries. The research instruments were self-administered by five researchers. The distributed questionnaires were filled out and returned on site, except in cases where respondents expressly asked for the researchers to return at a later time for collection. This collection approach ensured that the appropriate participants filled out the questionnaires, resulting in a satisfactory return rate of 93.3%, which is considered adequate for data analysis.

All established ethical standards governing research were observed in this study, including obtaining informed consent, explicit authorization for audio or video recording, voluntary involvement, participants' freedom to withdraw, and cultural sensitivity. The Ethical Committee of the University of Nigeria Nsukka granted the necessary approval for the study. Prior to the study, the instruments used underwent a pre-test for validation. The pre-test involved 5% of the sample size, comprising respondents from business organizations not being investigated. Its purpose was to ensure that the study's results aligned with its objectives. Three renowned instructors in the field of Criminology from the Department of Sociology and Anthropology at the University of Nigeria, Nsukka, validated and approved the instruments.

A total of 13 in-depth interview sessions were carried out with conveniently selected participants from financial institutions (7) and manufacturing and telecommunication industries (3 each). The interviews were conducted during the daytime and at the participants' convenience. Permission from the participants was obtained before recording the interview sessions on audiotape. Participants were chosen based on the relevance of their official position or knowledge on cybercrime-related issues in their organization. All participants were informed of the purpose of the study, and their written consent was obtained. Each respondent's interview lasted between 40 and 65 minutes.

3.4. Data analysis

Quantitative data are analyzed using descriptive statistics, which involve frequency distributions, simple percentages, and cross-tabulation analysis. Qualitative data are retrieved from the tape recorder, transcribed, described, and interpreted. The content analysis method is used to report direct quotations of important and striking responses in the study.

4. RESULTS AND DISCUSSION

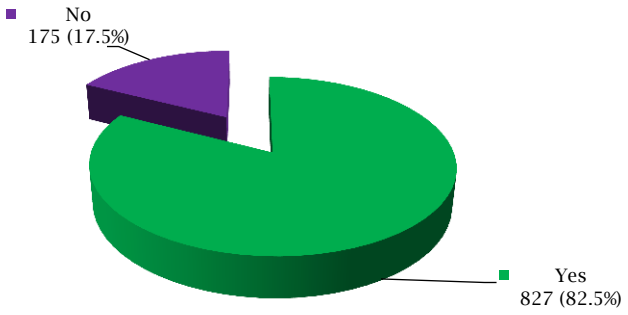
The data analysis was conducted with 1,002 retrieved questionnaires that were properly completed. The gender balance was 64.7% male and 35.3% female. The survey data were organized into four specific age groups. Nearly half (47%) of the respondents were aged between 31 and 40 years old, making this the largest demographic. The second largest age group, comprising 43.2% of the respondents, were 30 years old or below. The next age group consisted of those between 41 and 50 years old, with a significant 9.1% of respondents falling into this category. The smallest age group, at just 0.7%, was made up of individuals who were 51 years old and older. In terms of education, the lowest level of attainment among the respondents was the First School Leaving Certificate (FSLC), with only 0.5% holding this qualification. A larger proportion, 9.1%, held either a General Certificate of Education (GCE) or a Secondary School Certificate of Education (SSCE). The next level of qualification, held by 14.9% of respondents, was either a National Certificate of Education (NCE) or an Ordinary National Diploma (OND). The largest proportion of respondents, 62.9%, held First Degrees such as a Higher National Diploma (HND) or a Bachelor's Degree. Regarding the respondents' workplaces, the data showed that 41.8% worked in manufacturing companies, including Flourmills and Lafarge cement company. A smaller proportion, 4.5%, were employed by telecommunication corporations such as 9mobile, Airtel, Glo, and MTN. The largest workplace

category, however, was financial institutions, with 53.7% of respondents working in one of the 18 commercial banks operating within Cross River State. In terms of respondents' job descriptions, 5.8% of the respondents indicated that their job was in risk management, while 9.3% indicated that they worked in the ICT units of their organizations. Furthermore, 31.5% indicated that they worked as account officers in their organizations, while 55.4% worked as operational staff.

4.1. Incidence of malware attacks

Respondents are asked, *whether their organisations ICT equipment have suffered malware attack in the past*. From their responses, the majority (82.5%) of the respondents admitted that their organisations' ICT equipment have suffered malware attack in the past, while, 17.5% indicate that their organisations' ICT infrastructure have not suffered malware attack in the past. This implies that the majority of the respondents work in organisations whose ICT equipment have suffered malware attacks in the past. These findings can be generalised to mean that most corporate organisations in Cross River State have in the past experienced malware attacks on their ICT equipment. Previous studies including Chen and Bridges (2017) indicates that there is a high incident of malware attack being experienced by corporate organisations. They gave account of how ransomware (WannaCry) attack wreak havoc on the United Kingdom (UK) National Health Service hospitals data and another instance where Honda Motor Company in Japan was shut down as a result of ransomware (WannaCry) attack. In the same vein, Baeewe (2021) reveals in his study that 62% of respondents indicate that their computers have been attacked by malware more than 6 times in a space of three months. The findings of this study appear to be similar to the picture painted by Akrim and Dalle (2021) on malware attack in India. According to Akrim and Dalle (2021), virus attacks is one of the biggest challenge confronting personal computers owned by individuals and corporate organisations. Such attacks have a huge economic impact to the users especially when they were unable to perform their daily routine work.

Figure 1. Distribution of respondents by whether their organisation ICT equipment have suffered any malware attack in the past



Source: Field survey.

Qualitative responses on the incidence of malware attacks show that almost all the corporate organisations have experienced malware attacks in different ways. The dynamic nature of the attacks in financial organisations prompted constant changes within most of their ICT departments to enable them keep up with the challenge. Most respondents affirm that their organisations ICT equipment have been victims of malware attacks, this is not unconnected with the over reliance of modern organisations on big data and internet connectivity to interact with their customers. Based on the narrative above, a participant while responding to the question on whether their organisation has suffered malware attack said:

"*Actually, yes. Financial institutions are the major target of cyber fraudsters, cyber-attacks are a foremost, yet inescapable flip side of technological advancement. The fact that modern banking transactions heavily rely on big data and connectivity means that online criminals have a lot to steal, defraud or even hold for ransom*" (in-depth interview (IDI), male banker, 52 years old, bank 2, personal communication, 2019).

Corroborating the above submission, another participant when asked whether their organisation has experienced virus attacks in the past further explain the methods through which malware is often disseminated. He says:

"*Certainly, in most cases, viruses targeting banks are typically sent as harmful attachments within phishing emails or can be downloaded from suspicious spam websites. The actual infection occurs when a defiant employee of the bank opens the attachment with the intention of discovering its contents*" (IDI, male banker, 41 years old, bank 3, personal communication, 2019).

Another respondent from a reputable financial institution in the state while responding to the above question, simply said:

"*Yes. Attempts are being made on daily basis by online enemies to breach the security networks of commercial banks. This is simply because of the volume of cash at their disposal. The enemies (cybercriminals) are aware of what they stand to benefit if they succeed in defrauding a financial institution*" (IDI, male banker, 39 years old, bank 4, personal communication, 2019).

An individual from a separate banking institution outlined the types of malware attacks that their organization had faced. He explained that these malware intrusions operate in various

methods, which include eliminating the database, obstructing the removal of tainted software, and transmitting crucial bank information to the malevolent cybercriminal (IDI, male banker, 41 years old, bank 5, personal communication, 2019).

It is also evident that the online dissemination of malware contained in the responses of participants from financial organisations differ from the form of malware attacks reported by manufacturing organisation. For example, one of the participants from a manufacturing company notes that the malware attacks they often experience is minor. Responding to whether their organisation has experienced malware attacks in the past, he said:

"Yes, but a minor attack caused by the use of external drives like memory cards or flash drive" (IDI, male staff, 42 years old, manufacturing company 1, personal communication, 2019).

Similarly, another participant from a different manufacturing company corroborates the claim that malware attacks are minimal in manufacturing firms. He said:

"Not really, some of the malware attacks are not from the threat actors; they are caused by staff negligence" (IDI, male ICT staff, 39 years old, manufacturing company 2, personal communication, 2019).

An individual working with a telecommunications company has corroborated the fact that telecom enterprises face a high volume of malware threats because they serve as the portal through which other businesses connect to the internet. In her words:

"*The telecom industry faces a significant amount of malware attacks. This is primarily because telecom companies handle and oversee a vast database used for communication and storage of highly sensitive information. Additionally, they serve as the connecting platform for various organizations' networks. The extensive range of services provided by telecom companies, coupled with the substantial amount of data they possess, make them appealing targets for cybercriminals"* (IDI, female staff, 36 years old, telcommunication company 1, personal communication, 2019).

Triangulation of these responses reveal the reality of malware attacks on the ICT equipment of corporate organisations in Cross River State. Again, the above reports, coupled with the quantitative findings indicate that malware is one of the major mechanisms employed by cyber criminals to perpetrate cyber-attacks on corporate organisations. Although, the intensity is more in telecommunication and financial organisations, manufacturing firms are also at the risk of malware attacks on their ICT equipment.

4.2. Nature of malware attack experienced by corporate organisations

Respondents were asked *to identify the nature of malware that frequent plague their ICT equipment.* Data presented in Table 1 shows that 30.0% of the respondents identify viruses, 29.1% identify worms, while, 19.4% point to ransomware attack. Again, 17.5% of the respondents are of the view that trojan horse is the most frequently malware attack experienced by corporate organisations, while, 4.0% identify spyware. It is noted that 30.0% of the respondents identify viruses as the most common type of malware attack experienced by ICT equipment of corporate organisations in Cross River State, Nigeria. Despite a recent decline, worms and ransomware are also identified as a common type of malware that possess serious threat to organisations data. The data further shows that usually, viruses attack occurs more in financial institutions than any other corporate organisation in the state.

Table 1. Distribution of respondents on the nature of malware attacks in corporate organisations

Commonly used strategies	*Frequency*	*Percentage (%)*
Viruses	301	30.0
Worms	292	29.1
Ransomware	194	19.4
Trojan Horse	175	17.5
Spyware	40	4.0
Total	**1002**	**100**

Source: Field survey.

All participants during the qualitative study affirm the incidence of malware attack in their respective organisations. However, the frequency, nature, and extent to which the incidence occurs vary from one organisation to another. One of the participants responding to the question on the nature of malware attacks in their organisation says:

"In my organisation, viruses, ransomware and trojan horse are the common type of malware attacks they experience" (IDI, male banker, 52 years old, bank 2, personal communication, 2019).

Other participants acknowledge that their organisations ICT infrastructure have been attacked via ransomware, worms, viruses, and trojan horse. The findings of this study are consistent with Mariani and Zappalà (2014); they observe that a virus attack — a variant of malware attack is commonly used by fraudsters to attack small-scale business. However, they blame the success of such attacks on human behaviours, practices and errors, as the likely causes. The findings are in line with the research of Ernst & Young (2002). The result of Ernst & Young's (2002) study shows that over 61% of the organisations have suffered one or more virus incidents in the past that result in severe economic damage. The study further reveals that the incidence of virus attack is increasing exponentially yearly. This is also in line with the report of ICSA Labs (2005) which reveals that in 2004, virus encounter by organisations personal computers (PCs) increased by nearly 50% in comparison to 2003, with a rate of 400 encounters per 1,000 machines per month. Similarly, a survey by Richardson (2008) of organisations operating in the United States of America (USA), reveals that virus incidents are more frequent than expected confirmed by 49% of the workers in the affected organisations.

4.3. Medium through which malwares gain access to organisation's ICT equipment

Data presented in Table 2 shows that 41.1% of the respondents identify the phishing e-mails as the most widely used method of spreading malware infection, 27.0% identify online ads, while, 17.6%

point to visiting a website where malware is hosted. Again, 10.3% of the respondents are of the view that external devices are the most commonly method of spreading malware, while, 4.5% identify social media. This implies that majority of the respondents (41.1%) indicate that phishing e-mails are the most widely adopted method by fraudsters in spreading malware infection on ICT infrastructure of corporate organisations in Cross River State, Nigeria.

Table 2. Distribution of respondents on malware commonly used medium of penetration

Medium of penetration	*Frequency*	*Percentage (%)*
Online ads	271	27.0
Phishing e-mails attachment	412	41.1
External devices	103	10.3
Visiting a website where malware is hosted	176	17.6
Social media	40	4.5
Total	**1002**	**100**

Source: Field survey.

All participants during the qualitative study affirm that the e-mail attachments (phishing e-mails) is the commonly used method of disseminating malware infection. One of the participants responding to the question on the commonly used methods of distributing malware infection said:

"In my organisation, e-mails, online ads, and the use of external devices like external hard drive, flashes are the obvious and common methods of malware transmission" (IDI, male banker, 32 years old, bank 6, personal communication, 2019).

Other participants acknowledge that their organisations' ICT equipment have been attacked via e-mail attachments and online ads. The participants report that malwares simply exploit the vulnerability in the computer system to attack and infect organisations' files. Once malwares gain access into an organisation's ICT equipment, such malwares spread either by self-propagation or through user interaction. Malwares such as worms self-propagate itself without the help of any computer user while viruses depend on a user to move from one system to another. They maintained that there are several reasons why a system may get infected by a malware; moving forward, they recommend the use of effective antivirus software as the solution to tackling the present and future threats of malware.

4.4. Factors responsible for malware attack

Data presented in Table 3 shows that 4.9% of the respondents regard absence of antivirus software as responsible for malware attack on their organisations' ICT equipment. Also, 19.4% of the respondents indicate that the use of ICT equipment to visit harmful websites is responsible for malware attacks, 22.8% indicate lack of update to existing antivirus software, 2.2% indicate non-use of licensed antivirus, 19.2% indicate frequent use of internet, 12.5% indicated the use of flash drives on the system, while 1.5% give other responses. However, 17.5% do not respond to the question having indicated in figure 1 that their organizations' ICT equipment have not suffered any malware attacks in the past. The implication is that none of updating of antivirus software, visiting of harmful websites and frequent use of internet are the most common factors perceived by the respondents, as responsible for the malware attacks on their organisations' ICT equipment.

Table 3. Distribution of respondents on the factors responsible for virus attack on their organisation's ICT equipment

Factors responsible for virus attack	*Frequency*	*Percentage (%)*
Not having antivirus software	49	4.9
Visiting harmful sites	194	19.4
Non-updating of the antivirus software	229	22.8
None use of licensed antivirus	22	2.2
Frequent use of the internet	192	19.2
The use of flash drive on the system	126	12.5
Others	15	1.5
No response	175	17.5
Total	**1002**	**100.0**

Source: Field survey.

The state of computer software and their interface with other computer networks over the internet was also contained in the qualitative study as one of the factors responsible for the malware attacks on corporate organisations. For one of the participants:

"The bank's presence on the internet is largely responsible for the attacks" (IDI, male banker, 41 years old, bank 3, personal communication, 2019).

This was also corroborated by another participant who regarded their organisation's use of computers and data connected to the internet as the basis of their exposure to virus attack. He says:

"*Banks reliance on technology and use of data exposes them to different security challenges including virus attack. The sort of highly-sensitive personal and financial users' information that banks keep in their database and leverage on to provide personalised, predictive and seamless financial services makes them very attractive for malware attack"* (IDI, male banker, 41 years old, bank 5, personal communication, 2019).

The frequency at which the internet is relied upon for financial transactions was also pointed out by another participant, who said:

"*I may not be able to pinpoint a particular reason, but we cannot rule out the frequent use of the Internet. Many Internet fraudsters have exploited the vulnerabilities of most organisation ICT facilities to attack their computers and retrieve sensitive data for their malicious purposes. But all this can be averted with the use of updated anti-virus software"* (IDI, male banker, 48 years old, bank 1, personal communication, 2019).

Another participant believes that mere connection to the internet cannot be the only reason for the malware attack as the activities of the computer users on the internet is also responsible for the attacks. According to him, *"when staff download attachments from unverified sources, they expose the computer and other ones connected to it to virus attack"* (IDI, male banker, 52 years old, bank 2, personal communication, 2019). Another participant corroborating the assertion that opening malicious pop-up messages is one of the major ways through which organisations are exposed to virus attack, has this to say:

"*Computers are infected by malware when staff fail to yield to the warning that they should not download or install unauthorised/illegitimate applications that are laced with malware, which often appears legitimate. Once the malware infects a staff computer and obtains privileged access rights, it can gain control over the computer to intercept messages and steal personal information"* (IDI, male banker, 46 years old, bank 7, personal communication, 2019).

4.5. How to identify malware attack

Data presented in Table 4 shows that 38.2% of the respondents indicate a slow-down in system performance as the mechanism through which they know that their ICT equipment has been attacked by malware. Also, 22.6% of the respondents indicate unwanted alert messages as their own way of knowing when their ICT equipment have been attacked by malware. Similarly, 22.8% of the respondents indicate continuous restarting of their computer system, while 16.4% indicated failure of systems applications to perform their designed functions. This implies that a slow-down in system performance is the most common manifestation through which more than one-third of organisations personnel identify that their ICT equipment has been attacked by malware.

Table 4. Distribution of respondents by how they know that virus has attacked their organisation's ICT equipment

How to identify malware attack	*Frequency*	*Percentage (%)*
System slow-down in performance	384	38.2
Unwanted messages and alert messages	226	22.6
Continuous restarting	228	22.8
Failure in application functionality	164	16.4
Total	**1002**	**100.0**

Source: Field survey.

The position of the quantitative data was also corroborated by the qualitative responses as most participants indicate the various ways malware attacks manifest when it infects an organisation's computer system. These ranges from continuous system restarting to system failure. However, most financial institutions report that when their organisation's computer system is infected the system's performance is negatively affected. Correspondingly, some of the participants restrict their responses to duplication of documents, damage of important documents and unwanted messages and alert messages as some of the ways to identify a computer system that is infected with malware. By indicating the visible manifestation of malware attack on an organisation's ICT infrastructure, Joshi and Patil (2013) reached some conclusions that corroborates with the above findings that malware has the potential to compromise businesses and sensitive information but this depends on the type and scope of the infection which can manifest in lack of storage space, programs opening and closing automatically and slow-down in computer performance.

State of ICT equipment and their maintenance among corporate organisations in Cross River State.

Given the increasing rate of malware attacks, the study considers the rate at which organisations undergo regular system maintenance. The responses presented in Table 5 shows that 96.3% of the respondents affirm that their organisations undergo regular system maintenance, while 3.7% said no, which means that their organisations do not undergo regular system maintenance. It can therefore be deduced from the table that majority of the respondents work in organisations that carry out regular system maintenance.

Table 5. Distribution of respondents on whether their organisations undergo regular system maintenance

Regular system maintenance	*Frequency*	*Percentage (%)*
Yes	965	96.3
No	37	3.7
Total	1002	100.0

Source: Field survey.

Table 6. Distribution of respondents by how regular they carry out system maintenance

Regularity of system maintenance	*Frequency*	*Percentage (%)*
Never	37	3.7
Rarely	108	10.8
Always	585	58.4
Sometimes	272	27.1
Total	1002	100.0

Source: Field survey.

Data presented in Table 6 shows that 3.7% of the respondents indicate that their organisations have never carried out regular system maintenance. However, 10.8% of the respondents indicate that their own organisation rarely carries out regular system maintenance, 58.4% indicate always, while 21.7% indicate sometimes. The implication is that majority of the respondents (58.4%) are of the view that their organisations always carry out regular system maintenance.

4.6. Malware attack and socio-economic development of corporate organisations

To assess the impact of malware on organizational survival in Cross River State, respondents were surveyed to determine their agreement or disagreement with specific statements presented in Table 7. The table outlined six distinct impacts of malware attacks on corporate activities, and respondents were asked to indicate whether they *"agree", "strongly agree", "disagree",* or *"strongly disagree"* with each impact's relevance to their own organizations. To facilitate a meaningful analysis and interpretation, the responses of *"strongly agree"* and *"agree"* were combined and coded as *"agree",* while *"strongly disagree"* and *"disagree"* were merged and represented as *"disagree".* The results indicate that a significant majority of respondents (95.5%) agreed that malware attacks consume productive time for staff members who rely on computers, while only 4.5% disagreed. This suggests that in most corporate organizations, malware attacks have a negative impact on the productive time of computer-dependent staff. In the second row, 92.8% of respondents stated that malware

attacks affect their organizations by slowing down the performance of ICT equipment, rendering servers inaccessible, or causing network congestion. Conversely, 7.2% disagreed with this statement, implying that a majority of respondents recognize the economic consequences of malware attacks on their organizations, as it hampers ICT equipment performance, potentially leading to decreased overall output.

Similarly, in the third row, 91.4% of respondents agreed that malware attacks have a detrimental effect on organizational finances due to the costs associated with restoring damaged files and reinstalling networks. These substantial financial burdens impede the economic development of these organizations. However, 8.6% of respondents disagreed, indicating that such financial losses are not applicable in their organizations. Moving to the fourth row, 94% of respondents agreed that malware attacks cause system booting difficulties, resulting in hardware function failures, data loss, and operating system corruption, thereby disrupting organizational activities. Conversely, 6% of respondents disagreed, stating that this impact does not apply to their organizations. In the fifth row, 90.2% of respondents agreed that malware attacks in their organizations lead to an inability to access data from removable disks, jeopardizing the organization's reputation. Conversely, 9.8% of respondents disagreed, claiming that malware attacks in their organizations have not resulted in data inaccessibility from removable disks or reputation loss.

Finally, the sixth row indicates that a majority of respondents (88.6%) agreed that malware attacks on their organizations have led to the loss or alteration of programs or data, potentially compromising sensitive organizational information. Overall, the data presented in this section suggests that a majority of respondents believe that malware attacks have significant financial and organizational implications for affected corporate organizations, with the worst-case scenario potentially involving damage to the organization's reputation and substantial financial losses.

Table 7. Distribution of respondents by the various organisational and financial implications of malware attacks

Socio-economic implication of malware attack	*Agree*	*Disagree*	*Total*
It takes productive time away from staff who make use of these computers.	957 (95.5%)	45 (4.5%)	1002 (100.0%)
It slows down the performance of ICT equipment in organisations, making servers inaccessible and causes network jam.	930 (92.8%)	72 (7.2%)	1002 (100.0%)
Cost of restoring the damage files and the re-instalment of the networks involve huge finances, which affect the economic development of organisations.	916 (91.4%)	86 (8.6%)	1002 (100.0%)
Difficulty in system booting, hardware components failing to function, loss of data and corruption of the operating system.	942 (94.0%)	60 (6.0%)	1002 (100.0%)
Inability to access data from removable disks and loss of reputation.	904 (90.2%)	98 (9.8%)	1002 (100.0%)
Loss or alteration of programs or data, which can result to loss of sensitive organisation's data.	888 (88.6%)	114 (11.4%)	1002 (100.0%)

Source: Field survey.

A study by Akrim and Dalle (2021) on the economic impact of virus dissemination equally reports that a high rate of virus attacks amounts to a huge financial loss on the part of the organisations. They further note that some organisations attacked by viruses spend as much as $122,280 to clear up virus attacks. This was contained in Abroshan (2021) assessment of cybercrime and its impact on the Nigerian economy as a macro entity. They found that virus dissemination, as a strategy employed by cybercriminals, has an enormous negative impact of which loss of investors' confidence is rife. Abdulhamza (2022) has also indicated the negative impacts of virus dissemination on corporate organisations in a way that corroborates the findings of this study. These include difficulty in system booting, hardware components failure to function, loss of data and corruption of the operating system. The overall impact of cybercrime, which dwells on socio-economic development of the organisations, was also found in the study to be affected by virus dissemination. This is because virus attack is found to significantly predict a high negative effect of cybercrime on the socio-economic development of corporate organisations. Such negative impact is not limited to Nigeria's cyber landscape but is also applicable in other African business climates. For example, Baeewe (2021) reports that virus dissemination and credit card fraud, among other cybercrimes, are gaining ground in Ghana with wide negative implications on consumer and business owners' finances and the loss of credibility in the targeted institutions (financial institutions and state-owned businesses). Yusuf et al. (2017) have also found that virus dissemination and other cybercrime activities affect the productivity of the affected organisation, although such impact differs across organisations depending on the installation or un-installation of anti-virus software on a computer system. The extent to which malware attack affects corporate organisations varies depending on the ICT capabilities of the organisation and other factors. In the study, malware attack was found to constitute higher socio-economic development threats to organisations without regular system maintenance (73%), while at the same time, decreased to 71.5% for organisations with regular system maintenance. Regular system maintenance in the form of anti-virus updates has also been indicated by extant studies as reducing the extent of damage suffered via exposure to virus attacks (Suanpang et al., 2021).

4.7. Cross-tabulation of research variables

To further understand the dynamics of malware attacks in different organisations and its socio-economic development implications across organisations, some variables are cross-tabulated. In doing this, some variables are re-coded to create two groups. Again, the various organizations and the financial implications of malware attacks

presented in Table 7 are summed to obtain the malware impact score on organisations' socio-economic development. Scores above the mean are coded as *"higher malware impact",* while scores within and below the mean were coded as "*lower malware impact".*

Data presented in Table 8 shows that 84.6% of the respondents who work in financial organisations indicate that their organisations have suffered malware attacks in the past; this is also expressed by 80.2% of respondents who work in other organisations like manufacturing and telecommunication organisations. In addition, the percentage of respondents in financial organisations who indicate that their organisations have not suffered malware attacks in the past (15.4%) is less than the number of respondents from other organisations with similar views. This shows that financial organisations in Cross River State have more cases of malware attacks than telecommunication and manufacturing organisations put together.

Table 8. Types of organisations and experience of malware attacks in the past

Malware attack	*Nature of organisations*		*Total*
	Financial organisation	*Other organisations*	
Been attacked	455 (84.6%)	372 (80.2%)	827 (82.5%)
Not been attacked	83 (15.4%)	92 (19.8%)	175 (17.5%)
Total	538 (100.0%)	464 (100.0%)	1002 (100.0%)

Source: Field survey.

Data presented in Table 9 shows that 28.5% of respondents in organisations where regular system maintenance is carried out indicate a lower malware impact on the socio-economic development of their organisations. This is also expressed by 27% of respondents in organisations where system maintenance is not regular. Higher malware impact on socio-economic development is, however, indicated by 71.5% of respondents in organisations where regular system maintenance exists, while the figure increases to 73% for organisations without regular system maintenance. This shows that malware attacks negatively affect the socio-economic development of organisations without regular system maintenance more than organisations where regular system maintenance is applicable.

Table 9. Organisations regularity of system maintenance and extent of malware impact on its socio-economic development

Malware impact	*Regularity of systems maintenance*		*Total*
	Regular	*Not regular*	
Lower malware impact	275 (28.5%)	10 (27%)	285 (28.4%)
Higher malware impact	690 (71.5%)	27 (73.0%)	717 (71.6%)
Total	**965 (100.0%)**	**37 (100.0%)**	**1002 (100.0%)**

Source: Field survey.

5. CONCLUSION

Recent trends and cybersecurity reports suggest that malware attacks are on the increase, especially as it is mostly deployed innovatively by cyber fraudsters to steal personal data, conduct espionage, harm business operations, or deny user access to information and services. Globally, malware attacks remain one of the most notable strategies employed by highly sophisticated cybercrime syndicates in attacking and stealing information from large corporations and internet users. The study examines the effect of malware on the socio-economic development of corporate organisation in Cross River State, Nigeria. Based on the empirical evidence emanating from both descriptive and inferential statistics employed in the analysis of data, it has been observed that majority of the respondents (82.5%) report that they have experienced malware attacks on their personal computer, more than half of which is attributed to online related factors like harmful websites, absence of antivirus, lack of anti-virus update and too much internet surfing. However, the proportion of organisations that have suffered this attack varies as financial organisations are found to have experienced more of these attacks in the past than other organisations have. A development that has increased the demand for corporate user credentials among financial institutions. The extent to which malware affects corporate organisations varies depending on the ICT capabilities of the organisation and other factors. In the study, malware attack is found to constitute a higher socio-economic development threats to organisations without regular system maintenance (73%), while at the same time, decreased to 71.5% for organisations with regular system maintenance. The study therefore concludes that corporate organisations in Cross River State are connected to different forms of cyberspaces and as a result have significantly been exposed to various forms of malware attacks. The nature of malware attacks directed at these organisations were similar, although the intensity differs, as well as the effects it causes on their socio-economic development.

In order to arrest the vulnerability of an organisation to malware attacks, check the spread of malware throughout the organisation, and mitigate the impact of any further attack, it has therefore become imperative for corporate organisations to strengthen their network of security, engage in aggressive cybersecurity awareness training for staff, leverage advanced detection and response technologies, and use mobile protection solutions or corporate internet traffic protection to avoid the damaging effects of malware on their finances and reputation.

The cyber threat landscape is continuously evolving, with new and more complex types of malware emerging constantly. Research into malware victimization helps understand the trends, patterns, and techniques used by cybercriminals. This allows for the development of more effective prevention and mitigation strategies. Malware attacks can cause significant operational disruptions, which can threaten the survival of an organization, especially smaller ones. Research in this area can help organizations understand the potential risks and prepare for such scenarios,

minimizing the impact on business continuity. The major limitation of this study is that its scope is limited to selected corporate organizations in Cross River State, Nigeria. As a result, the data collected and analyzed in this study is based solely on information gathered from employees working in financial institutions, the manufacturing industry, and telecommunication service providers specifically in Cross River State, Nigeria. To support the research, secondary sources such as internet-based materials, textbooks, and journal articles have also been utilized. However, due to the focus on a specific region and industry, caution must be exercised when attempting to generalize the findings of this study to other corporate organizations in Nigeria and beyond. The sample size consists of respondents selected from only a few corporate organizations in Cross River State, which may not accurately represent the diversity and characteristics of all corporate organizations in Nigeria. Therefore, the findings of this study should be interpreted within the context of the specific organizations and industry under investigation and should not be indiscriminately applied to other organizational settings or geographical locations.

REFERENCES

1. Abdulhamza, S. M. (2022). The Iraqi legislative policy to protect national cyber security a study in the light of the principles of public international law. *Lark Journal for Philosophy, Linguistics and Social Sciences, 3*(46), 522–540. https://www.iasj.net/iasj/article/236956
2. Abdul-Rasheed, S. L., Lateef, I., Yinusa, M. A., & Abdullateef, R. (2016). Cybercrime and Nigeria's external image: A critical assessment. *Africology: The Journal of Pan African Studies, 9*(6), 119–132. http://jpanafrican.org/docs/vol9no6/9.6-9-Abdual-Rasheed.pdf
3. Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Computer Science and Applications, 12*(6), 31–37. https://doi.org/10.14569/IJACSA.2021.0120604
4. 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. http://surl.li/jijhw
5. Akrim, A., & Dalle, J. (2021). Mobile phone and family happiness, mediating role of marital communication: An attachment theory perspective. *International Journal of Interactive Mobile Technologies, 15*(21), 107–118. https://doi.org/10.3991/ijim.v15i21.17811
6. Baeewe, S. S. (2021). Cybercrime under the new Iraqi draft cybercrime law. *Journal of the College of Basic Education, 2*(SI), 123–141. https://cbej.uomustansiriyah.edu.iq/index.php/cbej/article/view/5724/5209
7. Beck, U. (2006). Living in the world risk society. *Economy and Society, 35*(3), 329–345. https://doi.org/10.1080/03085140600844902
8. Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of WannaCry ransomware. *Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 454–460). IEEE. https://doi.org/10.1109/ICMLA.2017.0-119
9. Computer Security Institute. (2010). *15th annual 2010/2011 computer crime and security survey.* https://urmh.edu.mx/15th-annual-2010-2011-computer-crime-and-security-survey_Yjo4OjEx.pdf
10. 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. http://surl.li/jilbm
11. Emmanuel, E., Okpa, J. T., & Iji, M. E. (2021). Corruption dynamics and the intractability of anti-graft war. In O. Àkànle & D. O. Nkpe (Eds.), *Corruption and Development in Nigeria* (1st ed., pp. 135–144). Routledge
12. Ernst & Young. (2002). *Global information security survey 2002.*
13. Gábriš, T., & Hamuľák, O. (2021). Pandemics in cyberspace — Empire in search of a sovereign? *Baltic Journal of Law & Politics, 14*(1), 103–123. https://doi.org/10.2478/bjlp-2021-0005
14. Gilbert-Knight, A. (2012, February 2). *Protecting your organization from spyware, viruses, and other malware: Learn how to keep your nonprofit or library computers safe*. TechSoup. https://www.techsoup.org/support/articles-and-how-tos/protecting-your-organization-from-spyware
15. Gounder, M. P., & Farik, M. (2017). New ways to fight malware. *International Journal of Scientific & Technology Research, 6*(6), 318–323. http://www.ijstr.org/final-print/june2017/New-Ways-To-Fight-Malware.pdf
16. ICSA Labs. (2005). *ICSA Labs 10th annual computer virus prevalence survey.*
17. Infocyte. (2017). *The threat of malware in Africa.* https://www.infocyte.com/wp-content/uploads/security_brief-malware_in_africa.pdf
18. Jennings, C. R., Johnson, E. A., & Sood, S. R. (2019, November 7). Ransomware attacks — Why it should matter to your business. *National Law Review.* https://www.natlawreview.com/article/ransomware-attacks-why-it-should-matter-to-your-business
19. Joshi, M. J., & Patil, B. V. (2013). Computer virus: Their problems & major attacks in real life. *Journal of Advanced Computer Science and Technology, 1*(4), 316–324. https://doi.org/10.14419/jacst.v1i4.318
20. Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and human factors of malware attacks: A computer security clinical trial approach. *ACM Transactions on Privacy and Security, 21*(4), Article 18. https://doi.org/10.1145/3210311
21. Mariani, M. G., & Zappalà, S. (2014). PC virus attacks in small firms: Effects of risk perceptions and information technology competence on preventive behaviors. *TPM, 21*(1), 51–65. https://doi.org/10.4473/TPM21.1.4
22. 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. https://doi.org/10.5281/zenodo.3707556
23. Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, O. B., & Okpa, J. T. (2022). Emerging trends in cybercrime awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*(3), 41–67. https://vc.bridgew.edu/ijcic/vol5/iss3/4
24. Okpa, J. T., Ajah, B. O., & Igbe, J. E. (2021). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology, 14*(2), 460–478. https://doi.org/10.5281/zenodo.4770111

25. Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimisation and economic sustainability of corporate organisations in Nigeria. *Security Journal, 36*, 350–372. https://doi.org/10.1057/s41284-022-00342-5
26. Okpa, J. T., Ilupeju, A. A., & Eshiotse, E. (2020). Cybercrime and socio-economic development of corporate organisations in Cross River State, Nigeria. *Journal Asian Journal of Scientific research, 13*(3), 205–213. https://doi.org/10.3923/ajsr.2020.205.213
27. Okpa, J. T., Ugwuoke, C. U., Ajah, B. O., Eshioste, E., Igbe, J. E., Ajor, O. J., Ofem, N. O., Eteng, M. J., & Nnamani, R. G. (2022). Cyberspace, black-hat hacking and economic sustainability of corporate organizations in Cross-River State, Nigeria. *SAGE Open, 12*(3). https://doi.org/10.1177/21582440221122739
28. Organisation for Economic Co-operation and Development (OECD). (2008). *Malicious software (Malware): A security threat to the internet economy.* https://one.oecd.org/document/DSTI/ICCP/REG(2007)5/FINAL/en/pdf
29. Pan, J. J. Y., & Fung, C. C. (2009). Malware's impact on e-business & m-commerce: They mean business! In *Proceedings of the 8th International Conference on e-Business (iNCEB2009)* (pp. 82–86). http://surl.li/jiqtq
30. Richardson, R. (2008). *CSI computer crime & security survey: The latest results from the longest-running project of its kind.* Computer Security Institute. http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf
31. Rogers, E. M. (1962). *Diffusion of innovations* (1st ed.). Free Press of Glencoe.
32. Sharmeen, S., Huda, S., & Abawajy, J. (2019). Identifying malware on cyber physical systems by incorporating semi-supervised approach and deep learning. *Proceedings of the IOP Conference Series: Earth and Environmental Science, 322*, Article 012012. https://doi.org/10.1088/1755-1315/322/1/012012
33. Shires, J. (2022). *The politics of cybersecurity in the Middle East.* Oxford University Press. https://doi.org/10.1093/oso/9780197619964.001.0001
34. Shubbar, H. (2022). *Constructing an Inter institutional and interministerial effort on cyber security in Iraq.* Al-Bayan Center Studies Series. http://www.bayancenter.org/en/wp-content/uploads/2022/03/87tr6tdf.pdf
35. Suanpang, P., Dongjit, J., Netwong, T., & Pothipasa, P. (2022). LGBTQ cyberbullying on online learning platforms among university students. *International Journal of Cyber Criminology, 15*(2), 60–76. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/15
36. Suanpang, P., Pothipasa, P., & Netwrong, T. (2021). Policies and platforms for fake news filtering on cybercrime in smart city using artificial intelligence and blockchain technology. *International Journal of Cyber Criminology, 15*(1), 143–157. https://cybercrimejournal.com/pdf/IJCC-11-2021.pdf
37. Ushie, E. M., & Okpa, J. T. (2021). Corruption and the development debacle in the Niger Delta region. In O. Àkànle & D. O. Nkpe (Eds.), *Corruption and development in Nigeria* (1st ed., pp. 120–132). Routledge
38. Vijayanand. C. D., & Arunlal, K. S. (2019). Impact of malware in modern society. *International Journal of Scientific Research and Engineering Development, 2*(3), 593–600. http://surl.li/jixla
39. Yusuf, M. S., Onotehinwa, T. O., & Okon, E. O. (2017). Productivity of business enterprises: Effect of computer virus infection on files. *International Journal of Computer Science and Mobile Computing, 6*(2), 179–193. http://surl.li/jixlt