Cyberspace, Black-Hat Hacking and Economic Sustainability of Corporate Organizations in Cross-River State, Nigeria

John Thompson Okpa1, Christopher Uchechukwu Ugwuoke2, Benjamin Okorie Ajah2, Emmanuel Eshioste1, Joseph Egidii Igbe1, Ogar James Ajor1, Ofem, Nnana Okoi1, Mary Juachi Eteng3, and Rebecca Ginikanwa Nnamani2

Abstract
Globally, e-commerce offers unlimited opportunities for corporate organizations to flourish as its customers reside in all parts of the universe. However, given the fluid nature of the cyberspace, black-hat hackers have enormously taken undue advantages of such mobility to perpetrate numerous financial frauds against individuals and corporate organizations. The impact of their attacks on the economic sustainability of corporate organizations is of obvious policy relevance, but little is empirically known about it. This study examined the role cyberspace plays in aiding the criminal activities of black-hat hackers and the impact of such malicious attacks on the economic sustainability of corporate organizations in Cross River State, Nigeria. An exploratory cross-sectional survey research design that allows the triangulation of quantitative and qualitative methods was adopted. Questionnaires were distributed to 1,074 respondents purposively selected from 18 financial institutions, 4 telecommunication network providers, and 2 manufacturing companies, while an in-depth interview was conducted on 13 participants across the selected corporate organizations. The presentation of data was done using frequency distribution tables, charts and relevant narratives. Chi-square was used to test the hypothesis, and content analyzing was adopted to analyze the qualitative data. The study found that corporate organizations with previous hacking experience are more likely to perceive black-hat hacking as affecting the productivity of their organization. The study, therefore, recommends that corporate organizations should strengthen their firewalls; educate their staff on the dangers of visiting unsafe websites, and downloading unverified attachments or clicking on links in unfamiliar emails.

Keywords
corporate-data, cybercriminals, cyberspace, digital-opportunists, malicious-codes

Introduction
Cybercrime is one of the most complex, widespread, and persistent social problems ravaging the cyberspace, and Africa is not immune from the ensuing treachery because of her weak legal and regulatory cyber policies (Abdul-Rasheed Ishowo et al., 2016; Ajah & Onyejegbu, 2019; Jaishankar, 2010; Ndubueze et al., 2013; Odo & Odo, 2015; Quarshie & Martin-Odoom, 2012). The cyberspace is driving business innovations and growth globally, and at the same time, exposing corporate organizations to new and emerging internet-assisted crimes (Longe et al., 2009; Makeri, 2017; Quarshie & Martin-Odoom, 2012). Today, the negative frontiers of the cyberspace that corporate organizations are contending with include: hacking, malware attacks, cyber-terrorism, spoofing, phishing, spam, virus attacks, child pornography, cyber vandalism, cyberstalking, data modification, email bombing, and cybersquatting (Fanawopo, 2004). The alarming increase in “incidents of cyber-attacks and the resultant economic 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, p. 8).

1University of Calabar, Cross River State, Nigeria
2University of Nigeria, Nsukka, Enugu, Nigeria
3Alex Ekwueme Federal University, Ndufu-Alike, Ikwo, Ebonyi State, Nigeria

Corresponding Author:
Benjamin Okorie Ajah, Department of Sociology and Anthropology, University of Nigeria, Nsukka, Enugu 000222, Nigeria.
Email: ajahokoriebenjamin@gmail.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
Hacking is a complicated technical activity aimed at exploiting systems’ vulnerabilities to subvert security checks, geared toward compromising digital devices such as computers, smartphones, tablets, and networks of organizations for financial gains, corporate espionage, and for fun. Hackers are broadly classified into the Black Hat, White Hat and Gray Hat hackers. The Black-hatters are the malicious hackers who hack for economic reasons. The White hatters are the “good guys” in the cyberspace who hack for ethical reasons, while, the Gray hatters hack for ideological reasons (Manne, 2020). The Black-hat hackers sometimes known as crackers are criminals, who use their skills to modify computer hardware or software for malicious intents. These groups of individuals use their programming skills to exploit target systems’ weaknesses and invade the networks of organizations, steal personal and corporate data for personal aggrandizement.

Black-hat hacking is committed by a diverse spectrum of actors (lone actors and organized crime syndicates), with different motivations and affiliations (Peters & Jordan, 2019). Their motivations range from economic gains to stealing and damaging sensitive data, disabling networks, establishing a command and control server, or using the system as a base to wreak future havoc. “Attacks can be active, such as a brute-force attack that determines a user’s password, or passive, such as a web-based attack that waits for a user to visit a malicious webpage in an attempt to infect the user’s computer with malicious codes through which they gain access into the target organisations’ networks” (Peters & Jordan, 2019, p. 6). These groups of digital opportunists usually cause mayhem in organizations by engaging in Distributed Denial-of-Service (DDoS), identity theft, vandalizing networks and creating worms to damage institutional and personal files. Studies have shown that fraudulent emails remain the most widely-used strategy by black hatters to attack corporate organizations. Most such attacks begin with phishing emails, which exploit staff vulnerabilities in order to infect computers with malware. Once the malware is downloaded into the network, black-hat hackers through this medium gain access to the user’s database to forge personal data with which they exploit an organization. The malware ignorantly downloaded into the network by staff could maliciously delete or transfer information, download destructive programs, providing hackers with unauthorized access to the computer, and more. Black-hat hackers also use psychology to trick staff into clicking on a malicious attachment or providing personal data. Despite differences in hackers’ profiles and drives, the majority of the attacks by these groups of cybercriminals have been found to be trans-national in nature (Peters & Jordan, 2019). This suggests that a single hacking attack can hit countless victims in different countries independent of the location of the source of the attack.

Estimating the global economic impact of black-hat hacking is difficult since most organisations do not report or publish their financial losses. However, The Council of Economic Advisers (2018, p. 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, p. 7).

Similarly, every successful attack, no matter how insignificant, attracts disastrous consequences for corporate organizations. The abuses of the cyberspace by black hatters portend danger and have stalled the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and utilization by corporate organizations in Nigeria. This development has widened the digital divide, crumbled the information infrastructure and affected consumer’s confidence in online transactions in Nigeria (Longe et al., 2009; Oumarou, 2007; Salifu, 2008). Corporate organizations in Cross River State that are victims of black-hat hacking frequently report substantial losses among previously loyal clientele, loss of revenues, massive loss of quality production time, overhead loss, as well as, immeasurable damages to their brand corporate image and reputation. These attacks have become worrisome due to their destructive nature and ability to affect the networks of high-profile corporate organizations in the State with relative ease.

The disturbing rise in incidents of black-hat hacking and the resultant economic implications have caused Akinehinde (2011) and Odumesi (2014) to argue that “more than 80 percent (80%) of organisations in Nigeria are prone to black-hat 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 black-hat hacking is expected to grow exponentially in the distant future, as reliance on networked technology increases.

Black-hat hacking in Nigeria is “largely perpetrated by both young and old adults; however, most of the young adults are students in various institutions of higher learning in the country, as well as, unemployed graduates and school drop-outs” (Hassan et al., 2012, p. 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 organizations in Nigeria. With the current high unemployment rate ravaging the nation, more young people across the country live below the poverty line, thereby; pushing them into internet-assisted crimes like hacking, phishing and other related vices (Ibrahim, 2016).
Several attempts have been put in place by corporate organizations to check the menace of black-hat hacking in Nigeria over the past few years, with minimal effect. Some of such attempts are the adoption of multi-factor authentication, role-based access control and hardware-based password management to keep sensitive data safe (Fanawopo, 2004; Frank & Odunayo, 2013; Gercke, 2013). With more than 80% of organizations in Nigeria prone to black-hat hacking attacks, the impact of these attacks on corporate organizations is of obvious policy relevance, but little is empirically known about it. Similarly, much has been written about the threats posed by hacking generally in literature (Ajah & Chukwuemeka, 2019; Barber, 2001; Bratus, 2007; Das & Nayak, 2013; Duah & Kwaweba, 2015; Dzomira, 2014; Jaishankar, 2007; Kamini, 2011; Karim, 2016; Kubina & Koman, 2016; Leukfeldt, 2015; Mohurle & Manisha, 2017; Ndubueze et al., 2013; Nnam et al., 2019; Okeshola & Adeta, 2013; Olson, 2013; Ragucci & Robila, 2006), but there has been comparatively fewer discussions on the extent black-hat hacking affect the economic sustainability of corporate organizations. A common denominator in these studies is the acknowledgment of black-hat hacking as part of the larger technological fallout, which has fostered a new dimension of crime and risks. Nonetheless, the pace at which corporate organizations subscribe to e-commerce, irrespective of the dangers posed by black hatters, provided the researchers with the motivation to examine the impact of black-hat hacking on the economic sustainability of corporate organizations in Cross River State, Nigeria. This was premised on the assumption that the financial loss often reported does not adequately account for the cost of black-hat hacking and without an insight on how corporate organizations’ overall economic development is impacted, empirical knowledge of the impact of black-hat hacking cannot be holistic. Thus, the study examines the impact of black-hat hacking on the economic sustainability of corporate organizations in Cross River State, Nigeria.

Methods

Study Design and Location

“The study adopted an exploratory cross-sectional design that allows the use of qualitative and quantitative data. This design is considered appropriate for this study because it provides a better and comprehensive understanding of the problem under study. The study area is Cross River State, Nigeria. Cross River State is a coastal State in the South-South region of Nigeria with its capital in Calabar. The area has three senatorial districts namely: Southern, Central and Northern Senatorial Districts, with eighteen Local Government Areas and one hundred and ninety-three (193) wards. The choice of Cross River State rests on the fact that reliable data on the incidence of cybercrime generally in the State is lacking, but news reports and statements by police and government officials give credence to the increase of the problem in the State” (Okpa et al., 2021, p. 463).

Participants and Procedures

“The target population for this study is 1,940 which were gleaned from financial institutions, telecommunication network providers, and manufacturing companies in the study area. Of this population, 1,056 (54%) are the staff of eighteen financial institutions (see Enukoha & Angioha, 2019), 91 (5%) are the staff of four telecommunication network providers (see www.ncc.gov.ng), and 793 (41%) are the staff of two manufacturing industries (see Manufacturers Association of Nigeria, Cross River State Chapter year bulletin, 2018). The study population was limited to permanent staff working in these selected corporate organisations in Cross River State, Nigeria. Using a Survey Monkey sample size determinant, with a 95% confidence level and level of maximum variability (P = 0.02), a sample of 1,074 was computed—out of which—1,002 respondents were finally used for analysis” (Okpa et al., 2021, p. 463).

The research adopted the stratified proportional and purposive sampling techniques in the selection of respondents. Stratified proportional sampling was used in delineating the study elements into 24 strata. “These are the eighteen (18) financial institutions, four (4) telecommunication network providers and two (2) manufacturing companies, based in the three senatorial districts of Cross River State (see Table A1 in the appendix for details). Respondents were purposively selected from each of the strata. The inclusion criteria were that respondents must have an internet enabled computer set attached to their desks and that they must be ICT staff, or engineers working in the selected organisations” (Okpa et al., 2021, p. 463).

Data Collection and Procedures

For triangulation, “the mixed methods of scientific investigation, consisting of quantitative and qualitative approaches of data collection were adopted. The instruments for data collection were a structured questionnaire and unstructured ‘In-Depth Interview (IDI)’. The research instruments were administered by four researchers. The questionnaire facilitates the collection of a large amount of information from a large number of people in a short time and in a relatively cost-effective way” (Okpa et al., 2021, p. 463). “The study observed all known ethical principles guiding social research such as informed consent, specific permission required for audio or video recording, voluntary participation, participants right to withdraw and cultural sensitivity. Ethical clearance was obtained from the ethical committee of the University of Nigeria Teaching Hospital; Ituku-Ozalla. The instruments were exposed to a pre-test. The pre-test was conducted using 5% of the sample size from respondents working in different corporate organizations from the ones studied.
The essence was to ensure that the data and findings of the study reflect their set target. The reliability of the questionnaire was determined using Cronbach alpha, and a reliability coefficient of 0.86 was obtained. The reliability coefficient was high enough for the instrument to be considered reliable for the study. Of the 1,074 questionnaires distributed, 1,002 copies were returned and used for analysis, while 72 copies were either not properly completed or not-returned" (Okpa et al., 2021, p. 463).

“The questionnaire return rate was put at 93.3% and was, therefore, considered suitable to be used for the data analysis. Qualitative data was elicited using the in-depth interview guide. The IDI provides valuable data far beyond the limit of the quantitative instrument and was used to support the findings of the quantitative data. The in-depth interview was conducted among thirteen (13) purposively selected participants from selected corporate organisations. The selection of these participants was based on two criteria which were the relevance of a participant’s official position and the reputation for being knowledgeable on cybercrime-related issues in the organisation in the study area. Again, participants were selected based on the principle of confidentiality of data, beneficence to participants and voluntariness. Each respondent’s interview lasted between 40 and 65 minutes” (Okpa et al., 2021, p. 463).

Data Analysis

“In analysing the data, a proper check was carried out on both the quantitative and qualitative components of the data collected to ensure that all items used for the analysis were properly responded to. Responses from the quantitative data were edited, coded and analysed using appropriate descriptive statistics like frequency distribution tables, bar charts, pie charts, and Chi-square through the Statistical Package for Social Sciences (SPSS). Qualitative data were analysed using content analysis after proper editing and transcription were done by the researchers. Catchy phrases and expressions gathered were identified and organised under distinct themes” (Okpa et al., 2021, p. 463).

Nature of Organization

Data presented in Figure 1 show that “41.8% of the respondents work in manufacturing companies such as Flourmills and Lafarge. Also, 4.5% of the respondents work in telecommunication organisations such as 9mobile, Airtel, Glo, and MTN. The remaining respondents (53.7%) work in financial institutions, which are the 18 commercial banks that operate in Cross River State (See Table 1). This finding implies that more than half of the respondents (53.7%) were from financial institutions. Furthermore, this composition is considered favourable for the study, as financial organisations are more attractive to cybercrime perpetrators” (Okpa et al., 2021, p. 464).

Length of Service

Data presented in Figure 2 show that “2.4% of the respondents have worked in their current organisations for 16 years and above. This was followed by 6.8% of the respondents that have worked in their organisations for 11–15 years. Also, 36.8% of the respondents indicated that they have worked in their organisations for 6–10 years, while, 54% indicated that they have worked in their current organisations for 1–5 years. This implies that more than half of the respondents (54%) have worked in their organisations for a period of 1-5 years” (Okpa et al., 2021, p. 464).

To enable deeper insight on the structure of the respondents in light of their distinct organizations, key aspects of their socio-demographic characteristics were cross-tabulated with the nature of the organizations they work with, as well as, the primary function of their organizations. Respondents’ age and level of education were re-coded into two categories. Respondents who were below 31 years were re-coded as “younger respondents,” while, those that were 31 years and above were re-coded as “older respondents.” Additionally, the respondents’ level of education was re-coded into two groups; Respondents who had B.Sc./HND or Masters/PhD were re-coded as “higher education,” while, those with First School Leaving Certificate, GCE/SSCE, and NCE/OND were classified as “lower education.” The outcome of the cross-tabulation is presented in Tables 1 to 3.

Table 1 shows that 52.2% of the male respondents work in financial institutions, which is 4.3% less than the proportion of female respondents that work in the same type of organization. This was not the case with telecommunication organizations, as 5.1% of male respondents indicated that they work with telecommunication organizations, while, only 3.4% of the female respondents work in the same organization. With regards to respondents in the manufacturing institutions, the finding shows that 42.7% of the male respondents work in manufacturing company, while, 40.1% of the female respondents work in the same organization. This implies that there were relatively more males in the telecommunication and manufacturing organizations than females.

Data presented in Table 2 show that a greater percentage of respondents with higher education (64.6%) work in financial institutions, while, 20% of respondents with lower education work with financial institutions. The reverse is the case with manufacturing companies, which shows that 77.1% of respondents with lower education work in manufacturing companies, while, 30.4% of respondents with higher education work in the same organizations. This further reiterates the fact that manufacturing organizations in Nigeria are largely labor intensive, and as a result rely more on personnel with lower educational qualifications.

Table 3 demonstrates the age disparity of respondents in different organizations. It shows that the majority of younger respondents (55.4%) are in organizations whose primary function is that of production, while, the majority of older
respondents (61.7%) are in organizations with financial services as their primary function. Also, a disparity was observed between younger respondents in organizations with telecommunication services as their primary function (1.8%), compared to older respondents in a similar organization (6.2%).
The majority (85.5%) of the respondents work in an organization that has been attacked by black-hat hackers in the past, while, 14.5% indicated that their organization has not been attacked by black-hat hackers in the past. This implies that majority of the respondents were of the view that their organizations have been attacked by black-hatters in the past. This goes further to suggest the high nature of black-hat attack on corporate organizations in Cross River State. However, it is possible that some of the respondents who claimed their organizations have not been attacked by black-hatters in the past could simply be unaware that the attacks occurred or existed. This is because, in some of the organizations, especially the financial institutions, a specialized unit exists that manages cyber-related attacks; consequently, an average staff in another department might not know that the various changes in the banks’ software or cyber platforms are in response to anticipated or real hacking attack. This was deduced from one of the participants in the qualitative interview. Responding to whether his organization has been hacked by black hatters, he said:

Sure, though banks have their hackers (ethical hackers), who identify vulnerabilities and patch them to forestall any attack from the bad guys. This effort has not prevented the black hatters from hitting our ICT equipment. In the bank, there is a specialised unit known as the Information Security Department that manages information relating to cyber-attacks on the bank. If there is a hacking attack, staff are usually not informed of the incident, but are directed and compel to take certain actions to mitigate future occurrence. Such actions include change of password in the middle of the month or deploying new software, which requires staff to log in afresh (IDI: Male Banker, 48, First Bank Plc).

Another participant from a different financial institution who claimed that the activities of black-hatters are routinely experienced by corporate organizations, especially the financial institutions, further corroborated the previous submission. According to him, “banks on daily basis experience breaches on their security networks by cybercriminals” (IDI: Male Banker, 39, GT Bank).

Other corporate organizations in the State are not exempted from the incessant attacks of black-hatters on their computers. Though there are variations, some of them perceived themselves as the most prone targets of black hatters as they stand a chance of losing their organizations’ biggest asset in the form of the intelligence on which the organization is founded. One of the participants from a manufacturing organization affirming that their organization has been attacked by black-hatters in recent time expressed his views thus:

Yes, we have been attacked and you see, manufacturing organisations like Lafarge are often at the biggest risk of hacking attacks because of the vast and easily transferable intellectual property they possess. This is contrary to the assumption that cyber threats are aimed only at financial institutions or organisations, where data could be monetized (IDI: Male ICT Staff, 39, Cement Manufacturing Company).

A participant from a telecom organization also confirmed that telecom corporations are exposed to a large number of cyber-attacks as they are the gateway to other organizations’ access to the internet. According to her:

Sure, though banks have their hackers (ethical hackers), who identify vulnerabilities and patch them to forestall any attack from the bad guys. This effort has not prevented the black hatters from hitting our ICT equipment. In the bank, there is a specialised unit known as the Information Security Department that manages information relating to cyber-attacks on the bank. If there is a hacking attack, staff are usually not informed of the incident, but are directed and compel to take certain actions to mitigate future occurrence. Such actions include change of password in the middle of the month or deploying new software, which requires staff to log in afresh (IDI: Male Banker, 48, First Bank Plc).
The qualitative data indicated that fraudulent emails and viruses/spyware/malware attacks are the most frequently applied approaches by black hatters in attacking corporate organizations in the State. One of the participants who identified fraudulent emails as the most commonly used medium of attack has this to say:

Fraudulent emails remain the most commonly used approach by the dark guys to attack financial institutions. They attack both

A participant from a manufacturing firm narrated how manufacturing industries have been hacked by black-hat hackers through fraudulent emails and *malvertising*. The participant has this to say:

From experience, I can say to you that the widely used methods by black-hat hackers are malvertising and fake email spread. These are not the only methods used by hackers in their operations. Through successful malvertising and fake email spread, hackers inject malicious contents that can damage and, most often, siphon off important organisational data (IDI: Male ICT Staff, 39, Lafarge Cement).

In some organizations, fraudulent emails and virus attacks were not much emphasized; rather other techniques of attacks like unauthorized access, botnets attacks, browser hijacks, ransom ware and denial-of-service attacks were evident. Some of the participants, while responding to the strategies used by black hatters in attacking corporate organizations said, “We have been attacked by a black-hat hacker via ransom ware and denial-of-service. Cyber robbers through denial-of-service gain a foothold on staff’s computers and consequently, the financial institution in which they work” (IDI: Male Banker, 41, UBA). Fraudulent emails and virus attacks were also indicated by participants from other corporate organizations, making both the most widely reported strategies adopted by black-hatters in attacking corporate organizations in Cross River State, Nigeria.

The Impacts of Black-Hat Hacking on the Organizational and Economic Sustainability of Corporate Organizations

The underlying objective of this study, aside from evaluating the hacking activities perpetrated against corporate organizations in Cross River State, is to ascertain the economic impacts that such sophisticated crime has on corporate organizations in the State. The black-hat hacking was evaluated against specific forms of organizational and economic implications on corporate organizations (Table 5).

Measuring the organizational and financial implications of black-hat hacking on corporate organization’s activities, six identifiable impacts were scaled to enable the respondents “agree” “strongly agree” “disagree” or “strongly disagree” on whether the impact is obtainable in their

| Methods of attacks              | Frequency | Percentage (%) |
|---------------------------------|-----------|----------------|
| Viruses/spyware/malware         | 271       | 27.0           |
| Fraudulent emails               | 412       | 41.1           |
| Browser hijacks                 | 103       | 10.3           |
| Ransom ware                     | 176       | 17.6           |
| Denial-of-service attacks       | 40        | 4.5            |
| Total                           | 1,002     | 100            |

Source: Field Survey, 2019.
organizations. In presenting the responses, “strongly agree” and “agree” options were merged and re-coded as “agree,” while, “strongly disagree” and “disagree” responses were merged and presented as “disagree.” The merging is to enable ease and meaningful descriptive interpretation and analysis. As can be deduced from the first row, 95.5% of the respondents agreed that black-hat hacking takes productive time away from staff that make use of these computers, while, 4.5% disagreed. It is, therefore, evident that in the majority of corporate organizations, black-hat hacking affects the productive time of staff that rely on computers to carry out their duties. In the second row, 92.8% pointed out that black-hatters attack affects their organizations’ activities by reducing the pace at which their ICT equipment perform, and also make their server to be inaccessible or cause network jam. This was, however, disagreed with by 7.2%, which implies that majority of the respondents acknowledged the economic impact of black-hat hacking in their organizations as it slows down the performance of ICT equipment, which could negatively affect performance and overall output.

This was also the case with data presented in the third row in which 91.4% of the respondents agreed that black-hat hacking affects the organizations’ finance negatively given the cost of restoring the damaged files or the re-installment of the networks. These huge financial losses affect the economic sustainability of these organizations. However, this was not upheld by 8.6% of the respondents who disagreed that such financial loss is not applicable in their organizations. In the fourth row, 94% of the respondents agreed that black-hat hacking creates difficulty in system booting, results in failure of hardware functions, leads to loss of data and corrupts the operating system, thereby, hampering their organizational activities. On the contrary, 6% of the respondents disagreed, noting that such is not applicable in their organizations.

In the fifth row, 90.2% of the respondents agreed that black-hat hacking in their organizations result to inability to access data from removable disks and as a result, the organization’s reputation is at stake. On the contrary, 9.8% of the respondents disagreed that black-hat hacking in their organizations has not resulted in the inability to access data from removable disks and consequently loss of an organization’s reputation. The sixth row equally shows that majority of the respondents (88.6%) agreed that black-hat hacking results in huge finances carted away from the organizations as penalties and other compensatory payments made to customers by the organizations, while, 11.4% of the respondents are of the contrary opinion on that viewpoint. A summation of all data presented in this section shows that majority of the respondents were of the view that black-hat hacking has serious economic and organizational impacts on affected corporate organizations, which in a worst-case scenario could cause the organizations’ reputation damage with attendant huge financial losses.

**Test of Hypothesis**

Corporate organizations with previous hacking experience are not likely to perceive black-hat hacking as affecting the productivity of their organizations more than those without previous hacking experience.

\( H_1 \) The productivity of corporate organizations will be affected by previous experience of black-hat hacking attack more than organizations without previous experience of black-hat hacking attack.

This hypothesis was tested with Chi-square statistics. The productivity implication of black-hat hacking scores was summed, and the mean score obtained. Scores that equaled to “disagree” and “strongly disagree” (<12) were coded as “do not affect productivity,” while, scores that equaled to “agree” or “strongly agree” (>12) were coded as “affects productivity.”

Table 6 shows that among respondents who have worked in organizations that have experienced hacking, 20.7% perceived black-hat hacking as not affecting productivity, while, the figure increased to 36.1% for respondents in organizations that have not experienced hacking. On the other hand, 79.3% of respondents in organizations where hacking has been experienced perceived black-hat hacking as affecting

---

**Table 5. Distribution of Respondents by the Various Organizational and Economic Implications of Black-Hat Hacking.**

| Organizational and economic implications of black-hat attack | Agree (%) | Disagree (%) | Total (%) |
|-------------------------------------------------------------|-----------|--------------|-----------|
| It takes productive time away from staff that make use of these computers. | 957 (95.5) | 45 (4.5) | 1,002 (100.0) |
| It slows down the performance of ICT equipment in organizations, making servers inaccessible and causes network jam. | 930 (92.8) | 72 (7.2) | 1,002 (100.0) |
| Cost of restoring the damaged files and the re-installment of the networks involve huge finances, which impact negatively on the economic sustainability of organizations. | 916 (91.4) | 86 (8.6) | 1,002 (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) | 1,002 (100.0) |
| Inability to access data from removable disks and loss of reputation. | 904 (90.2) | 98 (9.8) | 1,002 (100.0) |
| Huge finances carted away from the organizations as penalties and other compensatory payments made to customers by the organizations. | 888 (88.6) | 114 (11.4) | 1,002 (100.0) |

Source: Field Survey, 2019.
the productivity of their organizations, while, the figure
decreased to 63.9% for respondents in organizations that
have not experienced hacking. This suggests a form of rela-
tionship as dominant responses toed the hacking experience
line of the organizations’ productivity being impacted.

The chi-square value was $\chi^2 = 19.58; df = 1$; with a $p$-value
of .000. This is less than the alpha value of .05 adopted as the
study’s level of significance. Consequently, the null hypo-
thesis, which states that corporate organizations with previous
hacking experience are not likely to perceive black-hat hack-
ing as affecting the productivity of their organizations more
than those without previous hacking experience is rejected,
while, the substantive hypothesis is retained. The study,
therefore, concludes that corporate organizations with previ-
ous hacking experience are more likely to perceive black-hat
hacking as affecting the productivity of their organization
than those without previous hacking experience.

### Discussion of Findings

The findings from this study show that black-hat hacking
portends danger to the organizational and economic sustain-
bility of the corporate organizations in Cross River State,
Nigeria. These findings are consistent with the views of
Ayofe and Irwin (2010), as they submit that computer hack-
ing committed against a person, property, institution and
government claims huge sums of money and has affected up
to 56% of e-commerce globally. Again, the results show that corporate organizations lose unquantifiable amount of
resources, which range from loss of consumer confidence to
being held legally responsible for losses incurred by custom-
ners after such attack has occurred. Meanwhile, the real cost
of black-hat hacking cannot be ascertained because the
effects of such attacks can linger for years after the actual
incident. Consequently, and in line with the research objective,
the impact of black-hat hacking on the economic sus-
tainability of corporate organizations was analyzed to show
that black-hat hacking has six key impacts on the organiza-
tions’ management and finances.

On the organization, generally, black-hat hacking ham-
pers access to data from removable disk and affects the re-
putation and image of the organizations as indicated by the
majority of the respondents (90.2%). Again, 95.5% of the
respondents showed that organizations when attacked by
black hatters lose productive time. Such attacks also slow
down the performance of ICT equipment in organizations,
making servers inaccessible and causing network jam
(92.8%). Other financial impacts include the cost of restor-
ing the damaged files, and the re-installment of the networks
involves huge finances, which affect the economic sustain-
bility of organizations (91.4%). Also, the huge finances
carted away from the organizations as penalties and other
compensatory payments made to customers by the organiza-
tions are adverse (88.6%). This in some ways corroborates
the position of extant studies, which highlights various eco-

nomic and other implications of black-hat hacking to include
financial losses (Lee & Song, 2007), loss of data due to files
being deleted or changed (Alsayed & Bilgrami, 2017),
decreased privacy (Oyelere & Oyelere, 2015), and damaged
reputation (Olusola et al., 2013).

### Conclusion and Recommendations

Cyberspace plays a crucial role in building, promoting and
sustaining organizations’ brand and reputation. This is
because most customers rely on cyberspace like organiza-
tions’ websites, social media pages and applications (apps)
to interact directly with the organizations. However, when
these platforms are notably hacked by the dark guys in the
cyberspace, the brand and reputation of the organizations
become questionable, making customers lose trust and con-

fidence in them. The regularity of black-hat hacking is cur-
rently on the rise as almost all the respondents (85.5%) indi-
cated that they work in a corporate organization that has
been hacked by black-hatters. This confirms the argument of
Akinsehinde (2011) and Odumesi (2014) that “more than
eighty percent (80%) of organisations in Nigeria are prone to
black-hat hacking, which consequently, threatens their exist-
ence and survival”. And also verifies the report by Sophos,
a UK-based cyber security company that 86% of Nigerian
organizations surveyed said they suffered cyber attacks in
the last 12 months (Idris, 2020). Thus, the study recom-
mends that corporate organizations should spread their data
across smaller sub-networks to help contain attacks to only
a few endpoints instead of the entire ICT infrastructure. In
addition, corporate organizations should strengthen their
firewalls and educate their staff on the dangers of visiting
unsafe websites, and downloading unverified attachments.
or clicking on links in unfamiliar emails. Big corporations should hire ICT security experts to carry out a penetration test on their network, with the intent of identifying what vulnerabilities exist, and carry out necessary reparations to forestall possible forms of attack or breach on the organization’s ICT infrastructure.

APPENDIX A: Proportional Distribution of the Study Sample Size as Collated from Field Survey

Table A1. A Sample Breakdown of Banks and Their Branches.

| S/N | Bank     | Branch            | Bank branch population size (N) | Proportion of staff | Sample size (N) |
|-----|----------|-------------------|--------------------------------|---------------------|-----------------|
| 1   | FBN      | Calabar Main      | 75                             | 0.24                | 42              |
|     |          | Obudu             | 21                             | 0.07                | 12              |
|     |          | Ogoja             | 20                             | 0.06                | 11              |
|     |          | Ikom              | 30                             | 0.10                | 17              |
|     |          | Ugep              | 18                             | 0.06                | 10              |
|     |          | Akamkpa           | 18                             | 0.06                | 10              |
|     |          | Ekori             | 16                             | 0.05                | 9               |
|     |          | Ekorim            | 15                             | 0.05                | 8               |
|     |          | 8 miles           | 17                             | 0.05                | 9               |
|     |          | Main Avenue       | 20                             | 0.06                | 11              |
|     |          | NdidemUsang       | 31                             | 0.10                | 17              |
|     |          | EPZ               | 17                             | 0.05                | 9               |
|     |          | Iman              | 10                             | 0.03                | 6               |
|     | **Total**|                   | **308**                        |                     | **171**         |
| 2   | UBA      | Calabar Rd Main   | 18                             | 0.33                | 10              |
|     |          | Calabar Rd        | 14                             | 0.26                | 7               |
|     |          | Calabar Rd        | 12                             | 0.22                | 7               |
|     |          | Ikom              | 10                             | 0.19                | 6               |
|     | **Total**|                   | **54**                         |                     | **30**          |
| 3   | GTB      | Calabar           | 30                             | 0.8                 | 16              |
|     |          | Ikom              | 7                              | 0.19                | 4               |
|     | **Total**|                   | **37**                         |                     | **20**          |
| 4   | Access Bank | Calabar Rd     | 17                             | 0.46                | 9               |
|     |          | Calabar Bogobiri  | 13                             | 0.35                | 7               |
|     |          | Ogoja             | 7                              | 0.19                | 4               |
|     | **Total**|                   | **37**                         |                     | **20**          |
| 5   | FCMB     | Calabar Rd        | 40                             | 0.5                 | 22              |
|     |          | New Secretariat   | 25                             | 0.31                | 14              |
|     |          | Ikom              | 15                             | 0.19                | 8               |
|     | **Total**|                   | **80**                         |                     | **44**          |
| 6   | UBN      | Calabar           | 26                             | 0.59                | 14              |
|     |          | Akampka           | 8                              | 0.18                | 4               |
|     |          | Ogoja             | 10                             | 0.22                | 6               |
|     | **Total**|                   | **44**                         |                     | **24**          |
| 7   | Fidelity Bank | Unical       | 15                             | 0.37                | 8               |
|     |          | Calabar Main      | 16                             | 0.39                | 9               |
|     |          | Ikom              | 10                             | 0.24                | 6               |
|     | **Total**|                   | **41**                         |                     | **23**          |
| 8   | Zenith Bank | Mary Slessor    | 25                             | 0.17                | 14              |
|     |          | Calabar Main      | 52                             | 0.35                | 29              |
|     |          | Ikom              | 23                             | 0.16                | 13              |
|     |          | Ogoja             | 24                             | 0.16                | 13              |
|     |          | Chamley           | 24                             | 0.16                | 13              |
|     | **Total**|                   | **148**                        |                     | **82**          |

(continued)
Table A1. (continued)

| S/N | Bank            | Branch               | Bank branch population size (N) | Proportion of staff | Sample size (N) |
|-----|-----------------|----------------------|---------------------------------|---------------------|-----------------|
| 9   | Diamond         | Mary Slessor         | 21                              | 0.4                 | 12              |
|     |                 | Main Avenue          | 14                              | 0.26                | 8               |
|     |                 | Ogoja                | 8                               | 0.15                | 4               |
|     |                 | Ikom                 | 11                              | 0.20                | 6               |
|     | Total           |                      | 54                              |                     | 30              |
| 10  | EcoBank         | Mary Slessor         | 24                              | 0.25                | 13              |
|     |                 | Eta Agbor            | 17                              | 0.18                | 9               |
|     |                 | High Way             | 29                              | 0.31                | 17              |
|     |                 | Ikom                 | 14                              | 0.15                | 8               |
|     |                 | Ogoja                | 11                              | 0.12                | 6               |
|     | Total           |                      | 95                              |                     | 53              |
| 11  | Stanbic IBTC    | Marian               | 18                              | 0.56                | 10              |
|     |                 | IBB                  | 6                               | 0.19                | 3               |
|     |                 | Watt Market          | 8                               | 0.25                | 5               |
|     | Total           |                      | 32                              |                     | 18              |
| 12  | Skye Bank       | Ugep                 | 7                               | 0.37                | 4               |
|     |                 | Calabar              | 12                              | 0.63                | 7               |
|     | Total           |                      | 19                              |                     | 11              |
| 13  | Heritage Bank   | Calabar              | 17                              | 0.02                | 9               |
| 14  | Keystone Bank   | Calabar              | 22                              | 0.02                | 11              |
| 15  | Standard Chartered | Calabar          | 15                              | 0.01                | 8               |
| 16  | Wema Bank       | Calabar              | 23                              | 0.02                | 13              |
| 17  | Sterling Bank   | Calabar              | 16                              | 0.01                | 9               |
| 18  | Unity Bank      | Calabar              | 14                              | 0.01                | 8               |
|     | Total           |                      | 107                             |                     | 58              |

Source. Enukoh and Angioha (2019).

Table A2. A Sample Breakdown of Telecommunication Network Providers.

| S/N | Tel. Com.       | Branch               | Tel. com. population size (N) | Proportion of staff | Sample size (N) |
|-----|-----------------|----------------------|--------------------------------|---------------------|-----------------|
| 1   | MTN             | Eta Agbor Main Office| 19                             | 0.48                | 10              |
|     |                 | Marian               | 9                              | 0.22                | 5               |
|     |                 | Army Junction        | 7                              | 0.18                | 4               |
|     |                 | Ikom                 | 5                              | 0.13                | 3               |
|     | Total           |                      | 40                              |                     | 22              |
| 2   | Global Com      | Calabar Rd Main      | 11                             | 0.58                | 6               |
|     |                 | Ogoja                | 8                              | 0.42                | 5               |
|     | Total           |                      | 19                              |                     | 11              |
| 3   | 9mobile         | Calabar              | 17                             | 0.19                | 9               |
| 4   | Airtel          | Calabar              | 15                             | 0.16                | 8               |

Source. Authors’ compilation.

Table A3. A Sample Breakdown of Manufacturing Industries.

| S/N | Manufacturing   | Branch | Manufacturing company population size (N) | Proportion of staff | Sample size (N) |
|-----|-----------------|--------|------------------------------------------|---------------------|-----------------|
| 1   | Flour Mills     | Calabar| 384                                      | 0.48                | 213             |
| 2   | Lafarge         | Calabar| 409                                      | 0.52                | 226             |
|     | Total           |        | 793                                       |                     | 439             |

Source. Authors’ compilation.
Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID ID
Benjamin Okorie Ajah https://orcid.org/0000-0002-5942-1809

References
Abdul-Rasheed Ishowo, S. L., Muhammed, L. A., & Abdullateef, Y. R. (2016). Cybercrime and Nigeria’s external image: A critical assessment. Africology: The Journal of Pan African Studies, 9(6), 119–132.
Agugoesi, C. (2014). Surmounting the Africa cybersecurity challenge. Africa Telecom & IT: Expanding frontiers of Africa ICT, 7(2), 1.
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.
Ajah, B. O., & Onyjeegbhu, D. C. (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, p. 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.
Barber, R. (2001). Hackers profiled — Who are they and what are their motivations? Computer Fraud & Security, 2001(2), 14–17.
Bratus, S. (2007). What hackers learn that the rest of us don’t: Notes on hacker curriculum. IEEE Security & Privacy Magazine, 5(4), 72–75.
Council of Economic Advisers. (2018). The cost of malicious cyber activity to the U.S. Economy. CEA Report. https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyberactivity-u-s-economy/
Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International Journal of Engineering Sciences and 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 and Control Financial Markets & Institutions, 4(2), 17–27.
Emuoha, C. U., & Angioha, P. U. (2019). Management support for the use of information communication technology in commercial banks in Cross River State, Nigeria: Examining its relationship with the productivity of workers. Journal of Banking and Finance Management, 2(3), 1–7.
Fanawopo, S. (2004). FG moves to enforce cybercrime laws.
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.
Gercke, M. (2013). Training on cybercrime and discussion of the draft bill, special training on cybercrime. 2nd Workshop on Transposition of SADC Cyber Security. Model Laws in National Laws for Namibia Windhoek, Namibia. Retrieved March 10, 2018, from http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HPSSA/ Documents/Special%20Training%20on%20Cybercrime%20%281%29.pdf
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. https://www.ncc.gov.ng/technology/internet/internet-public-consultations/ongoing-consultations/60-spectrum-standard/cybersecurity
Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. In: Cybercrime and computer forensic (ICCCF), IEEE International Conference on (pp. 1–9). IEEE.
Idris, A. (2020). Why some of Nigeria’s worst cyberattacks are not reported. Cyberattacks in Nigeria. Business Day. https://businessday.ng/news/article/nigeria-is-experiencing-unprecedented-cyber-attacks/
Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1(1), 1–6.
Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. International Journal of Cyber Criminology (IJCC), 2(2), 26–31.
Kamini, D. (2011). Cybercrime in the society: Problems and prevention. 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., & Song, I. Y. (2007). Investigating information structure of phishing emails based on persuasive communication perspective. Journal of Digital Forensics, Security and Law, 3(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.
Makri, 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/manne/stories/2020/02/psych-profile-hackers.html
Mohurle, S., & Manisha, P. (2017). A brief study of Wannacry threat: Ransomware attack. International Journal of Advanced Research in Engineering & Technology, 8(5), 1938–1940.
Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cybercrime victimization among internet active Nigerians:

SAGE Open
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.

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

Okeshola, F. B., & Adeta, A. K. (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.

Okpa, J. T., Ajah, B. O., & Igbe, J. (2021). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, 14, 2.

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

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, & D. Tukura (Eds.), *Current trends in advance fee fraud in West Africa* (pp. 33–34). EFCC.

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*, 2(4), 45–51.

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

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime*, 15(4), 432–443.

Tobiko, K. (2014). The challenge in Africa. *Africa Telecom & IT: Expanding frontiers of African ICT*, 5(7), 11.