International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

Cybersecurity Threats and the Credibility of Digital Media Platforms in Ebonyi State, Nigeria

Leo Ekene Oketa

Research Fellow, Department of Mass Communication, Ebonyi State University, Abakaliki, Nigeria

***Corresponding author:** leoekeneoketa@gmail.com

ABSTRACT

Background: The rapid adoption of digital media platforms in Nigeria has significantly enhanced communication, information dissemination, and public engagement. However, the increasing prevalence of cyberattacks poses serious threats to the reliability, security, and credibility of these platforms, particularly in emerging digital environments such as Ebonyi State. Meanwhile, existing studies have paid limited attention to how cybersecurity threats affect the credibility of digital media platforms and public trust in emerging digital environments such as Ebonyi State, Nigeria.
Objective: This study examined the relationship between cybersecurity and credibility of digital media platforms in Ebonyi State, Nigeria.
Method: A mixed-methods research design was adopted. Quantitative data were collected from 317 active Internet users through structured questionnaire, while qualitative insights were obtained through in-depth interviews with media practitioners and cybersecurity experts. Data were analysed using descriptive statistics and thematic analysis.
Results: Findings reveal that phishing, malware, and hacking are the most prevalent cyber threats affecting digital media platforms. The study further shows that cyberattacks significantly disrupt media operations, including content production and distribution. This contributes to a noticeable decline in public trust in digital information sources. Despite awareness of cybersecurity risks, many media organisations lack adequate protective measures.
Conclusion: The study concludes that cyberattacks constitute a major challenge to the efficiency and credibility of digital media platforms in Ebonyi State. The persistence of these threats continues to undermine public confidence and highlights the vulnerability of digital communication systems in developing contexts.
Unique Contribution: This study provides empirical insight into the relationship between cyber threats, media operations, and audience trust within a sub-national context. It contributes to the growing body of knowledge on cybersecurity challenges in developing societies and offers practical perspectives for strengthening digital media resilience.
Key Recommendation: The study recommends the adoption of advanced cybersecurity technologies, continuous training for media personnel, and sustained public awareness campaigns on safe digital practices. Additionally, stronger collaboration among media organizations, government agencies, and cybersecurity experts is essential to ensure a secure and trustworthy digital media environment.

Keywords: Cyberattacks, Digital Media, Public Trust, Cybersecurity, Nigeria, Ebonyi State

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

INTRODUCTION

Digital technologies have fundamentally transformed communication, information dissemination, and social interaction across the globe. The rise of Internet-enabled platforms such as Facebook, WhatsApp, YouTube, X, TikTok, etc, has facilitated real-time access to information, enhanced civic engagement, and redefined the structure of media production and consumption (Ezike, et al. 2016). In contemporary societies, digital media platforms, including online news portals, social networking sites, and blogs serve as important channels for information exchange and public discourse. In Nigeria, this transformation has been particularly pronounced, as increasing internet penetration and smartphone usage have accelerated the adoption of digital communication tools across both urban and semi-urban areas.

In Ebonyi State, digital media platforms have become central to information sharing, governance communication, and socio-political engagement. Citizens increasingly rely on these platforms for news updates, public announcements, and interactive discourse. This growing dependence underscores the importance of ensuring the reliability, security, and credibility of digital media systems. However, the rapid expansion of digital platforms has also introduced significant vulnerabilities, particularly in the form of cyber threats. Cyberattacks - including phishing, malware, hacking, and Distributed Denial-of-Service (DDoS) attacks have emerged as persistent challenges capable of disrupting media operations, compromising sensitive data, and eroding public trust in digital information ecosystems (Nwafor, & Nwabuzor, 2021).

Meanwhile, existing literature has examined various dimensions of cybersecurity and digital media. For instance, Oladipo and Akintoye (2021) explored the prevalence of cyber threats in Nigerian digital environments, highlighting the increasing sophistication of attacks but focusing primarily on technical vulnerabilities rather than their broader societal implications. Similarly, Sule, et al (2021) investigated cyber risks within online communication systems, emphasizing security breaches but offering limited insight into how such threats influence public perception and trust and Adetunji (2020) examined digital media usage in Nigeria, noting the growing role of online platforms in information dissemination. While these studies provide valuable insights into cybersecurity challenges and digital media dynamics, they exhibit notable limitations. First, many focus predominantly on national-level analyses, thereby overlooking sub-national contexts such as Ebonyi State, where digital media adoption patterns and vulnerabilities may differ. Second, existing research tends to emphasise technical aspects of cyber threats without adequately examining their impact on media operations, including content production, distribution, and audience engagement. Third, there is limited empirical investigation into how cyberattacks shape public trust in digital media platforms, particularly within emerging digital societies.

This gap in the literature necessitates a context-specific investigation that integrates both operational and perceptual dimensions of cyber threats. Therefore, this study seeks to examine the impact of cyberattacks on digital media operations and public trust in Ebonyi State. By adopting a mixed-methods approach, the study provides a comprehensive understanding of how cyber threats affect the efficiency, credibility, and security practices of digital media platforms, as well as the extent to which these threats influence audience confidence in online information. In doing so, the research contributes to the broader discourse on cybersecurity and digital communication in developing contexts and offers practical insights for media practitioners, policymakers, and cybersecurity stakeholders.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

STATEMENT OF THE PROBLEM

The Internet has become an essential tool for communication, business, and social interaction (Erkomashvili, 2023). However, it has also created opportunities for cybercrime, which poses serious challenges to digital security. In Nigeria, including Ebonyi State, cyberattacks have become increasingly common, threatening the safety and reliability of digital platforms. As media organisations and individuals increasingly rely on digital platforms for information dissemination and consumption, the risk of cyberattacks continues to grow. These attacks can disrupt media operations, compromise sensitive information, and reduce public trust in digital media platforms. Despite the increasing importance of digital media in Ebonyi State, limited research has examined how cyberattacks affect the digital media environment in the State. This study therefore seeks to investigate the impact of cyberattacks on the digital media space in Ebonyi State, with the aim of understanding their effects on media operations, information security, and public trust.

RESEARCH OBJECTIVES

The general objective of this study is to investigate the impact of cyberattacks on the digital media space in Ebonyi State. Specifically, the study was meant to:

1. Examine the nature and frequency of cyberattacks affecting digital media platforms in Ebonyi State.
2. Analyze the impact of cyberattacks on media operations, particularly in content production, distribution, and audience engagement.
3. Assess the effects of cyberattacks on public trust and perception of digital media outlets in Ebonyi State.
4. Examine the measures adopted by digital media organizations in Ebonyi State to mitigate the impact of cyberattacks.

RESEARCH QUESTIONS

This study seeks to answer the following research questions:

1. What types of cyberattacks are most prevalent in the digital media space in Ebonyi State?
2. How do cyberattacks affect the operational efficiency of digital media platforms in the State?
3. What impact do cyberattacks have on public trust and perception of digital media outlets in Ebonyi State?
4. What measures have digital media organizations in Ebonyi State adopted to address the growing threat of cyberattacks?

HYPOTHESES

The study tests the following hypotheses:

H01: Cyberattacks do not significantly affect the operational efficiency of digital media platforms in Ebonyi State.

H02: Cyberattacks do not significantly influence public trust in digital media outlets in Ebonyi State.

H03: Digital media organizations in Ebonyi State have not implemented adequate cybersecurity measures to protect their platforms from cyber threats.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

SIGNIFICANCE OF STUDY

This study is significant in several ways. First, it will contribute to the growing body of knowledge on cybersecurity and digital media, particularly within the context of developing societies such as Nigeria. The findings will help scholars and researchers better understand the relationship between cyber threats and the performance of digital media platforms. Second, the study will be useful to media organizations in Ebonyi State by highlighting the nature and impact of cyberattacks on their operations. This will enable them to adopt stronger cybersecurity strategies and preventive measures to safeguard their digital platforms. Third, policymakers and government agencies responsible for information technology and cybersecurity will benefit from the findings of this study, as it will provide insights that can guide the development of effective policies and regulatory frameworks aimed at improving digital security. Finally, the study will also create awareness among digital media users about the risks associated with cyberattacks and the importance of adopting safe online practices when accessing or sharing information on digital platforms.

LITERATURE REVIEW

Advent of Internet Revolution and Transformation of Communication

The advent of the internet revolution has fundamentally transformed the nature, structure, and dynamics of communication in contemporary society. The emergence of digital technologies has shifted communication from traditional, linear, and centralized systems to decentralized, interactive, and network-driven processes. Early communication systems relied heavily on print and broadcast media, which were characterised by limited audience participation and delayed feedback mechanisms. However, the proliferation of Internet technologies has enabled instantaneous, real-time communication across geographical boundaries, thereby redefining the concept of global connectivity (Castells, 2010; Manovich, 2021).

Scholars such as Boyd (2014) argue that digital media platforms have facilitated participatory culture, where users are no longer passive consumers but active producers of content. This transformation has democratised information dissemination, allowing individuals and groups to contribute to public discourse without reliance on traditional media gatekeepers. Jenkins (2006) further highlights that convergence culture has blurred the boundaries between producers and consumers, fostering collaborative communication ecosystems. In the Nigerian context, the internet revolution has significantly influenced communication practices, particularly with the rise of mobile internet usage and social media platforms. According to Adetunji (2020), digital media has become a primary source of information for many Nigerians, especially among younger populations. In Ebonyi State, this transformation is evident in the increasing reliance on online platforms for news dissemination, governance communication, and civic engagement.

Despite these advancements, scholars caution that the internet revolution also introduces challenges related to information overload, misinformation, and digital inequality (van Dijk, 2020). Furthermore, while digital media enhances accessibility and speed, it simultaneously raises concerns about content credibility and system vulnerability. These concerns underscore the need to examine not only the benefits of digital transformation but also the risks associated with increased dependence on internet-based communication systems.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

Challenges of Cyberattacks

The rapid expansion of digital communication infrastructures has been accompanied by a corresponding rise in cyber threats. Cyberattacks, defined as deliberate attempts to compromise digital systems, networks, or data, represent one of the most pressing challenges in the digital age. These attacks threaten the confidentiality, integrity, and availability of information systems, thereby undermining the reliability of digital communication platforms (Whitman & Mattord, 2018). Common forms of cyberattacks include phishing, malware, ransomware, and Distributed Denial-of-Service (DDoS) attacks. Phishing involves deceptive attempts to obtain sensitive information, while malware refers to malicious software designed to disrupt or damage systems. Ransomware attacks, on the other hand, encrypt data and demand payment for its release, while DDoS attacks overwhelm systems to render them inaccessible (Kshetri, 2019).

Studies indicate that cyberattacks have increased in both frequency and sophistication, driven by technological advancements and the growing value of digital data. According to Kshetri (2021), cybercriminals increasingly exploit vulnerabilities in digital infrastructures, particularly in developing countries where cybersecurity measures are often inadequate. In addition to financial losses, cyberattacks can result in reputational damage, operational disruptions, and erosion of public trust. However, much of the existing literature focuses on the technical aspects of cyber threats, with limited attention to their socio-communication implications. This gap highlights the need for research that examines how cyberattacks affect not only system functionality but also user perception and trust in digital platforms.

Cyberattacks in the Media

The media sector has emerged as a critical target for cyberattacks due to its role in shaping public opinion and disseminating information. Digital media platforms are particularly vulnerable because of their reliance on open networks and user-generated content. Cyberattacks on media organizations can disrupt content production; alter information, and compromise data security, thereby affecting both operational efficiency and credibility. Smith (2019) further observes that cyberattacks on media institutions can lead to misinformation, content manipulation, and loss of audience confidence. Similarly, Oladipo and Akintoye (2021) identify hacking and malware attacks as significant threats to digital media platforms in Nigeria, emphasizing their impact on service delivery and data integrity. Adetunji (2020) further observes that politically motivated cyberattacks can be used to influence public perception and manipulate information flows.

Despite these insights, existing studies often focus on national-level trends and technical vulnerabilities, with limited exploration of localized contexts such as Ebonyi State. Moreover, there is insufficient empirical evidence on how cyberattacks influence audience trust and perception of media credibility. This limitation underscores the need for context-specific studies that integrate operational and perceptual dimensions of cyber threats in the media sector.

Cybersecurity

Cybersecurity encompasses the strategies, technologies, and practices designed to protect digital systems from cyber threats. It involves safeguarding networks, devices, and data from unauthorised access, disruption, or destruction. Effective cybersecurity ensures the confidentiality, integrity, and availability of information, which are essential for maintaining trust in digital systems (Kruse et al., 2017). Also, Nwachukwu (2021) and Aligwe, et al,

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

(2016) agree that cybersecurity is not only a technical issue but also an organisational and behavioural challenge, requiring coordinated efforts across multiple stakeholders. Similarly, Maduagwu (2023) highlights the importance of cybersecurity awareness and training in mitigating cyber risks, particularly in environments with limited technical capacity. However, the implementation of cybersecurity measures remains uneven, especially in developing countries. Factors such as inadequate infrastructure, limited expertise, and low awareness contribute to vulnerabilities in digital systems. While existing studies emphasize technological solutions, there is a growing recognition of the need to address human and organizational factors in cybersecurity strategies.

Digital Media and Internet Security

Digital media platforms have become integral to modern communication, enabling the creation, distribution, and consumption of content through internet technologies. These platforms rely heavily on internet infrastructure, making them susceptible to security threats. Internet security involves measures such as encryption, firewalls, and antivirus systems designed to protect digital media from cyberattacks (Whitman & Mattord, 2018). In the same vein, Manovich (2021) argues that digital media systems are inherently vulnerable due to their interconnected nature, which increases exposure to cyber threats. Similarly, Boyd (2014) highlights that user behavior and platform design can influence the effectiveness of security measures, emphasizing the need for user awareness and responsible digital practices.
Despite the recognized importance of internet security, many digital media platforms lack adequate protection mechanisms, particularly in developing contexts. This creates opportunities for cyberattacks that can compromise content integrity and user trust. Existing literature, however, provides limited empirical analysis of how internet security challenges specifically affect digital media operations and audience perception.

Cybersecurity Challenges in Nigeria and Ebonyi State

Nigeria faces significant cybersecurity challenges despite the existence of regulatory frameworks such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015. Factors such as low cybersecurity awareness, inadequate technical infrastructure, and weak enforcement mechanisms contribute to the persistence of cyber threats (Otozi et al., 2024). Meanwhile studies such as Aligwe, et al. (2017); Onwe, et al (2017) and Ogbaeja, and Nwafor, (2017) indicate that cyberattacks in Nigeria are increasing in frequency, often targeting financial institutions, government agencies, and digital media platforms. According to Sule, Mat, and Sambo (2021), cyber threats in Nigeria are driven by both economic and political motivations, with implications for national security and public trust.

In sub-national contexts such as Ebonyi State, these challenges are further exacerbated by limited institutional capacity and growing dependence on digital media for communication. The rise of online platforms in the state has exposed users and organizations to cyber risks, including phishing, malware, and hacking. However, there is a notable lack of empirical studies focusing specifically on cybersecurity challenges in Ebonyi State. Most existing research adopts a national perspective, thereby overlooking local dynamics and contextual variations. This gap highlights the need for localized research that examines how cyber threats impact digital media operations and public trust within specific environments.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

THEORETICAL FRAMEWORK

This study is anchored on two theories: Protection Motivation Theory (PMT) and Communication Privacy Management Theory (CPM). These theories help explain how individuals and organizations respond to cyber threats and how they manage information in digital communication environments. Protection Motivation Theory was developed by Rogers, R. W. in 1975 to explain how individuals respond to perceived threats and how they adopt protective behaviours to reduce risks. The theory suggests that people are motivated to protect themselves based on their perception of a threat and their belief in their ability to prevent or reduce the impact of that threat. According to PMT, individuals evaluate threats through two major processes: threat appraisal and coping appraisal. Threat appraisal involves assessing the severity of a threat and the likelihood of being affected by it. Coping appraisal involves evaluating the effectiveness of protective measures and one's ability to implement them.

In the context of cybersecurity and digital media, Protection Motivation Theory explains how media organizations and digital media users respond to cyber threats such as hacking, phishing, and malware attacks. When media organizations perceive cyberattacks as serious threats, they are more likely to implement protective measures such as stronger cybersecurity systems, secure networks, and staff training to reduce their vulnerability. This theory is relevant to this study because it helps explain how awareness of cyber threats influences the actions taken by digital media organizations and users in Ebonyi State to protect their platforms and information systems.

Communication Privacy Management Theory was developed by Petronio, Sandra in 1991 to explain how individuals manage private information and decide when and how to disclose or protect such information. The theory suggests that individuals believe they own their private information and therefore create boundaries to regulate who can access it. These boundaries are managed through privacy rules that guide decisions about sharing or protecting information. When these boundaries are violated, privacy turbulence may occur, leading to mistrust and communication breakdown. In the digital media environment, CPM theory is particularly relevant because digital platforms often involve the sharing and management of sensitive information. Cyberattacks such as hacking and data breaches can violate privacy boundaries by exposing confidential data without authorization.

Applying this theory to the current study, cyberattacks on digital media platforms can disrupt the privacy management process by compromising the control that media organizations and users have over their information. When such breaches occur, public trust in digital media platforms may decline, as users may feel that their information is not adequately protected. Both theories provide a useful framework for understanding the impact of cyberattacks on digital media platforms. Protection Motivation Theory explains how media organizations respond to cybersecurity threats by adopting protective measures, while Communication Privacy Management Theory explains how cyberattacks can affect information control, privacy, and trust within digital communication systems. Together, these theories help to explain the relationship between cyber threats, digital media operations, and public trust in digital media platforms in Ebonyi State.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

RESEARCH METHODOLOGY

This study adopted a mixed-method approach comprising quantitative (descriptive survey) and qualitative (in-depth interview) methods to provide a comprehensive understanding of the impact of cyberattacks on the digital media space in Ebonyi State, Nigeria. Ebonyi State, located in South-East Nigeria and comprising thirteen Local Government Areas, was selected due to the increasing use of internet services, social media, online news platforms, blogs, and digital advertising channels among residents. The study population consisted of all active internet users in Ebonyi State, estimated at 1,401,626 by the National Bureau of Statistics (2025). Using the Wimmer and Dominick Mass Media Research Online Sample Size Calculator at a 95% confidence level and 5% margin of error, a sample size of 384 respondents was obtained. Simple random sampling was used to select survey respondents to ensure equal representation and minimise bias, while purposive sampling was adopted for selecting participants for the in-depth interviews, including media practitioners and cybersecurity experts with relevant knowledge of digital media and cybersecurity issues.

Data were collected using two instruments: a structured questionnaire and an interview guide. The questionnaire contained closed-ended questions covering demographic characteristics, awareness and experiences of cyberattacks, and perceptions of digital media credibility. The interview guide explored cyber threats faced by digital media platforms and mitigation measures adopted by stakeholders. The instruments were validated by experts in Mass Communication and Statistics at Ebonyi State University, Abakaliki. Their observations improved the clarity and relevance of the instruments. A pilot study involving 10 respondents in Obubra Local Government Area of Cross River State was conducted, and reliability was tested using Cronbach's Alpha, which yielded a coefficient of 0.70, indicating acceptable reliability. A total of 380 copies of the questionnaire were distributed to internet users in Ebonyi State, out of which 317 were properly completed and returned, while 63 were invalid or not returned. Additionally, four in-depth interviews were conducted through face-to-face and telephone interactions. Quantitative data were analyzed using the Statistical Package for the Social Sciences (SPSS), employing frequencies, percentages, and Chi-square tests to examine relationships between cyberattacks and public trust in digital media platforms. Qualitative data were analyzed thematically by identifying recurring themes relating to cyber threats, their effects on digital media operations, and mitigation strategies adopted by media organisations.

RESULT

Table 4.1: Response Rate

Response	Frequency	Percentage
Returned	317	83.4%
Not Returned	63	16.6%
Total	380	100%

The response rate of 83.4% is considered adequate for the analysis of the study.

Demographic Characteristics of Respondents

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

Table 4.2: Gender Distribution

Gender	Frequency	Percentage
Male	182	57.4%
Female	135	42.6%
Total	317	100%

The result shows that 57.4% of respondents were male, while 42.6% were female.

Table 4.3: Age Distribution

Age	Frequency	Percentage
18 - 25 years	98	30.9%
26 – 35 years	124	39.1%
36 – 45 years	61	19.2%
46 years and above	34	10.7%
Total	317	100%

The data indicates that the majority of respondents (39.1%) are between 26 – 35 years, suggesting that young adults dominate digital media usage in Ebonyi State.

Analysis of Research Questions

Research Question 1

What types of cyberattacks are most prevalent in the digital media space in Ebonyi State?

Table 4.4: Types of Cyberattacks Experienced

Cyberattack Type	Frequency	Percentage
Phishing	102	32.2%
Malware	76	24.0%
Hacking	64	20.2%
DDoS attacks	48	15.1%
Others	27	8.5%
Total	317	100%

The findings reveal that phishing (32.2%) is the most common cyberattack, followed by malware (24.0%) and hacking (20.2%).

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

Research Question 2

How do cyberattacks affect the operational efficiency of digital media platforms?

Table 4.5: Impact of Cyberattacks on Media Operations

Response	Frequency	Percentage
Strongly Agree	121	38.2%
Agree	136	42.9%
Disagree	42	13.2%
Strongly Disagree	18	5.7%
Total	317	100%

The result indicates that 81.1% of respondents agree that cyberattacks negatively affect the operations of digital media platforms.

Research Question 3

What is the impact of cyberattacks on public trust in digital media outlets?

Table 4.6: Effect of Cyberattacks on Public Trust

Response	Frequency	Percentage
Strongly Agree	118	37.2%
Agree	129	40.7%
Disagree	50	15.8%
Strongly Disagree	20	6.3%
Total	317	100%

The result shows that 77.9% of respondents believe cyberattacks reduce public trust in digital media platforms.

Hypothesis Testing

Hypothesis 1
H_0: Cyberattacks do not significantly affect the operational efficiency of digital media platforms in Ebonyi State. Using Chi-Square statistical test, the result showed that $\mathbf{p} < 0.05$, indicating that cyberattacks significantly affect digital media operations. Therefore, the null hypothesis was rejected.

Hypothesis 2
H_0: Cyberattacks do not significantly influence public trust in digital media outlets.
The Chi-square analysis showed a significant relationship between cyberattacks and public trust ($p < 0.05$). Therefore, the null hypothesis was rejected.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

DISCUSSION

The findings of this study reveal that cyberattacks constitute a major challenge within the digital media environment in Ebonyi State, Nigeria. The study identified phishing, malware, and hacking as the most common cyber threats affecting digital media platforms. These threats were found to disrupt online operations, compromise sensitive information, and weaken communication processes within media organisations. The findings further indicate that cyberattacks negatively influence public trust and confidence in digital media platforms, as audiences tend to question the credibility and reliability of information disseminated through platforms perceived to be vulnerable to security breaches. These findings align with the position of Nwafor, et al. (2025) in their study on artificial intelligence and journalism in Ebonyi State, which observed that technological changes within the digital communication environment continue to generate concerns among media professionals regarding security, stability, and the future of media operations. Although their study focused primarily on job security in the era of artificial intelligence, it similarly highlights the growing vulnerabilities associated with digital communication technologies and the need for media organizations to adapt to emerging technological threats.

The findings are also consistent with the study Nwafor, Ezema, and Igwebuike (2022), which demonstrated the powerful influence of digital and social media platforms on users in South-East Nigeria. While their research examined social media use and substance abuse among young people, both studies acknowledge the expanding role and influence of digital platforms in shaping public behaviour and perception. The present study extends this understanding by showing that cyber insecurity within these platforms can significantly undermine users' confidence and trust in digital communication channels. Similarly, the findings support the work of Nwafor and Onwubere (2019) on pirate broadcasting and separatist agitations in Nigeria. Their study emphasised how unregulated and technologically enabled communication channels can threaten information credibility and social stability. In the same vein, the current study demonstrates that cyberattacks create opportunities for misinformation, unauthorised access, and manipulation of digital media content, thereby reducing audience confidence in online platforms. The findings of the present study also agree with the study conducted by Aligwe, et al. (2017), which found that digital news media spaces during the 2015 Nigerian general elections were characterised by uncivil and problematic communication patterns capable of undermining journalistic standards and public confidence. Both studies suggest that weaknesses within digital media environments - whether through uncivil discourse or cybersecurity threats - can adversely affect media credibility and audience trust.

Furthermore, the findings corroborate the study by Okoro, et al. (2014), which highlighted the significant influence of digital media technologies on audience behaviour in South-East Nigeria. While their study focused on children's behavioural exposure to digital media content, the current study similarly demonstrates the broad societal impact of digital platforms, particularly how cybersecurity breaches can shape audience perception, trust, and engagement with digital information systems. However, unlike some earlier studies that focused mainly on the social, behavioural, and political implications of digital media usage, the present study specifically contributes to knowledge by examining cybersecurity threats as a critical factor affecting the credibility and sustainability of digital media platforms in Ebonyi State. This underscores the need for stronger cybersecurity frameworks, improved digital literacy, and enhanced protection mechanisms to safeguard digital communication systems and maintain public trust in online media platforms.

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

CONCLUSION

From the findings of the study, it can be concluded that cyberattacks pose a significant threat to the digital media environment in Ebonyi State. As digital media continues to grow as a primary source of information and communication, the vulnerability of digital platforms to cyber threats becomes a serious concern. Cyberattacks not only disrupt media operations but also weaken public confidence in digital communication platforms. Therefore, addressing cybersecurity challenges is essential for ensuring the reliability, credibility, and sustainability of digital media platforms. Effective cybersecurity strategies, improved digital infrastructure, and increased awareness among digital media practitioners and users are necessary to reduce the risks associated with cyber threats.

Ethical clearance

Ethical consent was sought and obtained from the participants used in this study. They were made to understand that the exercise was purely for academic purposes, and their participation was voluntary.

Acknowledgements

We acknowledge all those who assisted us with data collection. We equally appreciate the Ebonyi State University Library staff for their cooperation and support.

Sources of funding

The study was not funded.

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Authors' Contributions

Leo Ekene Oketa conceived and conducted the study, including the design, data collection and collation, analysis and interpretation. The author has critically reviewed and approved the final draft, and is responsible for the content and similarity index of the manuscript.

Data availability statement

The datasets on which conclusions were made for this study are available on reasonable request.

Citation

Leo Ekene Oketa, L. E., (2025). Cybersecurity Threats and the Credibility of Digital Media Platforms in Ebonyi State, Nigeria. *International Journal of Sub-Saharan African Research*, 4(1), *942-955*

International Journal of Sub-Saharan African Research (IJSSAR)
Vol. 4, Issue 1, pp. 942-955, March 2026, ISSN: 3043-4467 (Online), 3043-4459 (Print)
doi:10.5281/zenodo.20067586

REFERENCES

Adetunji, O. (2020). Cyber threats and media security in Nigeria: The need for effective policy responses. *Journal of Digital Media, 12*(3), 45–67.

Aligwe, H.N., Nwankwo, S. U. & Nwafor, K. A. (2017). Agricultural Communication and Food Security in Nigeria: The Mass Media Role. *World Applied Sciences Journal 35(5): 843-847.*

Aligwe, H. N., Nwafor, K.A. & Nwasum, C. J. (2017). Journalistic Concern about Uncivil Political Talks in Digital News Media during the Electioneering of the 2015 General Elections in Nigeria. *IDOSR Journal of Arts and Management 2(2): 69-90, 2017.*

Aligwe, H.N., Nwafor, K. A. Nweze, S. (2016). Youths, Social Media and the 2015 General Elections in South East Nigeria. World Applied Sciences Journal 34 (12): 1909-1914.

Asogwa, C. E. (2019). Public perception of the influence of digital media on cybersecurity in Nigeria. *Universal Journal of Electrical and Electronic Engineering, 6*(5), 366–372.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Castells, M. (2010). *The rise of the network society*. Wiley-Blackwell.

Erkomashvili, D. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security. *International Master Security and Intelligence and Strategic Studies, 2*(1), 298–312.

Ezike, M. O., Nwafor, K. A. & Imeazue, G. A. (2016). Facebook Political Campaign and Its Effects on the 2015 Governorship Election in Ebonyi State, *International Journal of Communication, 19(1), 17-27.*

Jenkins, H. (2006). *Convergence culture: Where old and new media collide*. NYU Press.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review. *Technology and Health Care, 25*(1), 1–10.

Kshetri, N. (2019). Cybercrime and cybersecurity in developing economies. *Computer, 52*(2), 22–29.

Kshetri, N. (2021). The evolution of cyber threats. *IT Professional, 23*(1), 10–15.

Maduagwu, E. (2023). Cybersecurity awareness and digital protection in Nigeria. *African Journal of Information Systems, 15*(2), 78–92.

National Bureau of Statistics. (2025). *Telecom data: Active voice and internet subscriptions, porting and tariff information*.

Nwachukwu, C. (2021). Cybersecurity frameworks and digital resilience in Nigeria. *Nigerian Journal of Technology, 40*(3), 512–520.

Nwafor, K. A., Alegu, C. J., Nsude, I., Oketa, C., Nweze, S., Ede, F. N., Imakwu, V. N., Ogbu, J. A., & Aleke, C. (2025). Perception Of Job Security In The Era Of Artificial Intelligence Among Journalists In Ebonyi State, Nigeria. *International Journal of Educational Research & Amp; Social Sciences*, *6*(1), 72–86. https://doi.org/10.51601/ijersc.v6i1.952

Nwafor, K. A.; Ezema, S.I. & Igwebuike, O. (2022). Social Media Use And Substance Abuse Among Young People in South-East, Nigeria. *SAU Journal of Management and Social Sciences*, 3(1) 7-14.

Nwafor, K. A. & Nwabuzor, M.N. (2021). Social Media and Youths Engagements and Mobilisation for the 2020 #EndSARS Protests in Nigeria. *EBSU Journal of Mass Communication, 8(1), 13-24.*

Nwafor, K. A. & Onwubere, C. H. (2019). Pirate Broadcasting and Separatist Agitations in Nigeria: A Case Study of IPOB and Radio Biafra. *The Nigerian Journal of Communication, 16(1), 2019.*

Ogbaeja, N.I. & Nwafor, K. A. (2017). Social Media and Learning Behaviour of University Undergraduates in South East Nigeria. EBSU *Journal of Mass Communication. Ebonyi State University, Abakaliki,* 4 (1), 188-207.

Okoro, M. N., Nwafor, K. A. & Odoemelam, C. C. (2014). Influence of Digital Media, Video Games, Toys and Cartoons on the Behaviourof Early School-Age Children in South-East Nigeria. *The Nigerian Journal of Communication, 12(1), 212-240.*

Oladipo, T., & Akintoye, K. (2021). The vulnerability of digital media in Africa: Case studies from Nigeria. *International Journal of Media Security*, *8*(2), 78–92.

Onwe, E.C.N., Nwafor, K. A. & Orji-Egwu, A. (2017). Framing of Terrorism in Africa Media: A Comparative Study of Frames Employed in Reporting Boko Haram in Nigeria and Al-Shabab in Kenya. *Middle East Journal of Scientific Research*, 25(6), 1225-1233.

Otozi, U. J., Ephraim, B., & Yinka, A. I. (2024). Cybercrime and its negative effects in developing countries. *Journal of Mobile Computing & Applications, 11*(4), 10–16.

Smith, J. (2019). The impact of cyber threats on media organizations: A global perspective. *Journal of Cybersecurity and Media*, *10*(1), 22–34.

Sule, B., Mat, N., & Sambo, U. (2021). Cyber security and cybercrime in Nigeria: Implications for national security and the digital economy. *Journal of Intelligence and Cyber Security*, *4*(1).

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security*. Cengage Learning.