Received: 27.04.2026| Accepted: 27.05.2026| Published: 01.06.2026
Citation: **UDO, U.M, IKOH, M., & UDO, T.M. (2026)** Cyber-hacking and Socio-economic activities in Uyo Urban, Akwa Ibom State, Nigeria**. GAIJIST Vol.2.1.2026 pp.1-11 DOI:** https://doi.org/10.5281/zenodo.21839916

CYBER-HACKING AND SOCIO-ECONOMIC ACTIVITIES IN UYO URBAN, AKWA IBOM STATE, NIGERIA

[1]Utibeima Monday UDO [2]Moses IKOH &[3]Torobong Monday UDO
[1-3]*Department of Sociology and Anthropology, University of Uyo, Nigeria*
[1]udomacin@gmail.com [2]mosesikoh@yahoo.com [3]torobongudo8@gmail.com

Abstract

Background: The increasing internet penetration and growing reliance on digital platforms for banking, commerce, and record-keeping in Uyo Urban, Akwa Ibom State, Nigeria, have exposed residents and business operators to a wide range of cyber-hacking threats, including account takeovers and large-scale data breaches.

Purpose: This study examined the effects of cyber-hacking on socio-economic activities in Uyo Urban.

Methods: Anchored on Routine Activity Theory and General Strain Theory, the study adopted a descriptive survey design. A sample of 400 respondents was selected from Uyo Urban using the Taro Yamane formula and a multi-stage sampling technique involving cluster, stratified, and simple random sampling. Data on cybercrime victimisation and socio-economic impact were collected using a structured questionnaire and analyzed with descriptive statistics and Simple Linear Regression in SPSS Version 25.

Results: Findings revealed that cyber-hacking had the strongest effect on financial transactions (Mean = 3.73), and the least effect on loss of customers, though still above average (Mean range = 2.53–2.96). Regression results indicated a strong and statistically significant negative relationship between cyber-hacking and socio-economic activities ($R = .955$; $R^2 = .912$; $F(1, 382) = 3952.9$; $p < .05$). A unit increase in hacking activities was associated with a 0.986 unit decrease in socio-economic activities.

Conclusion and Recommendations: The study concludes that cyber-hacking is not merely a criminal act but a structural impediment to digital and economic development in Uyo. It recommends a subsidized cybersecurity audit program for small and medium enterprises, mandatory security upgrades, and enhanced collaboration among tech hubs, universities, and government.

Keywords: *Cyber-hacking, Socio-economic activities, Victimisation, Uyo, Routine Activity Theory, General Strain Theory*

*Corresponding author(s). **UDO, U.M, IKOH, M., & UDO, T.M. (2026)**, agree that this article remain permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

1. INTRODUCTION

Cybercrime has emerged as a pervasive international menace, fundamentally altering the safety architecture of the contemporary digital world, and in Uyo urban this phenomenon is no longer an outlier but a central challenge to regional stability (Smith, 2020).The rapid introduction of the internet has changed how individuals carry out daily activities, effectively turning the world into a global village (Leukfeldt and Holt, 2020) yet this technological assimilation has also facilitated the rise of internet fraud (Wilson, 2020).

Sullivan (2020) accentuated that

cybercrime poses a significant threat to developing economies, as the vulnerability of new digital users could lead to a total erosion of the "digital dividend" intended to uplift marginalised socio-economic groups. Historically, cybercrime was viewed as a low-risk, high-benefit activity due to the anonymity provided by geographic distance (Jones and Brown, 2020), but the landscape has shifted toward high-tech methods that thwart detection, making the prosecution of offenders increasingly difficult (Jones, 2021). Among the various forms of cybercrime, hacking is one of the most widespread and financially destructive. Cybersecurity Ventures (2021) projected that the damages caused by cybercrime would reach US$10.5 trillion per year by 2025, up from US$3 trillion in 2015. High-profile incidents illustrate the scale of the threat: the 2017 WannaCry ransomware attack compromised more than 200,000 computers in 150 countries and cost between US$4 billion and US$8 billion (Europol, 2017); the 2014 Sony Pictures hack cost more than US$100 million in damages, legal expenses, and recovery (BBC, 2014); and the Equifax data breach exposed the personal details of 147 million Americans, leading to a US$700 million settlement (Federal Trade Commission, 2019). The global cybersecurity market itself was projected to expand to US$345.4 billion by 2026 as organisations increased spending to curb future breaches (Markets and Markets, 2020), following average global data-breach costs estimated at US$3.86 million in 2020 (IBM, 2020).

In Uyo, the concentration of people and businesses increases the reach and efficiency of cybercriminals (Adesanya and Akinyele, 2023), while victims face lost income and reduced productivity, and businesses suffer operational downtime (Anderson et al., 2019; Button et al., 2020). The city's rapid adoption of technology and its transition toward a cashless economy have created what may be described as a comfortable environment for cyber-predators, compounded by a "get-rich-quick" syndrome associated with the "Yahoo Boy" subculture (Adesina, 2021; Ibekwe and Okoro, 2021). Rural and peri-urban areas around Uyo possess significant agricultural and artisanal potential but often lack the robust cybersecurity infrastructure and digital literacy found in Uyo itself (Ekong, 2023) so when hacking siphons capital from the local economy, it erodes the financial base necessary for sustainable rural investment.

Despite growing awareness of cybercrime as a national economic threat, there remains a significant research gap regarding the specific effects of hacking victimisation on the stability of socioeconomic activities in Uyo Local Government Area. Existing literature has extensively explored the drivers of cybercrime, such as unemployment and the inability of the job market to absorb graduates but has paid comparatively little attention to how hacking interferes with business operations and revenue streams at the local level. The current legal and institutional framework, including the Cybercrime Act 2015, has proven insufficient in curbing the susceptibility of key institutions such as banks and fintech platforms (Ekong, 2023), while inconsistent enforcement and a shortage of technical expertise within law enforcement further complicate the security landscape (Alabi, 2021). This study

addresses this gap by examining the direct effect of cyber-hacking on socio-economic activities in Uyo urban.

2. LITERATURE REVIEW

2.1 Conceptual Clarification: Hacking

Hacking is on the rise and comprises one of the most widespread types of cybercrime. Cyber-hacking poses a major challenge to the world economy, where millions of dollars go down the drain every year. Financial institutions, businesses, and individuals are usually victims of cyberattacks whereby offenders steal money or other important financial data, as illustrated by the WannaCry ransomware attack, which severely affected the United Kingdom's National Health Service and forced the cancellation of surgeries (Europol, 2017). Organisations are often targeted by cyberhackers who steal sensitive information such as customer data, intellectual property, and trade secrets; annual losses to intellectual-property theft through cyber espionage are estimated in the billions of dollars (Accenture, 2019). Cyberattacks also cost businesses in terms of recovery, system repair, legal compliance, and victim compensation (U.S. Department of Homeland Security, 2018).

Cyberattacks on critical infrastructure can cause mass trade disruption, as demonstrated by the 2020 attack on the shipping giant Maersk, which paralysed operations and delayed supply chains globally at an estimated loss of US$300 million (BBC, 2017). The SolarWinds attack, which inserted malware into software updates affecting multiple United States government agencies, further underscores how vulnerable public and private institutions are to cyberattacks with far-reaching consequences for national security, economic stability, and public trust. Obinna and Nneka (2024) evaluated the types of cybercrimes committed by undergraduates in tertiary institutions in Anambra State using a mixed-method design with a Taro Yamane-derived sample of 1,083 students and found that hacking and credit card fraud were the most frequently committed offences, recommending awareness campaigns and parental guidance. Okpa (2022) analysed cyberspace, hacking, and the economic sustenance of corporate organisations in Cross River State, surveying 1,074 respondents across financial institutions, telecommunication providers, and manufacturing companies, and found that hacking-related fraudulent transactions, including unauthorised withdrawals, had cost organisations considerably, while existing cybersecurity laws were insufficient. Chioma *et al.* (2017), through interviews with 50 purposively sampled respondents, identified poor recruitment and training of cybersecurity professionals, weak policy implementation, and underfunding of security services as underlying causes of rising cyber insecurity in Nigeria. Pius *et al.* (2021) examined youth involvement in hacking and cyber identity theft ("Yahoo Yahoo") and found that economic hardship and the glamorisation of wealth sustained the practice despite government intervention. Kothari (2019) observed that hacking, once mainly the work of individual actors, has been organised into the activities of criminal syndicates, while Choi (2008) found that multinational corporations, government agencies, and financial institutions are targeted because of the value of their data, even as small businesses and individuals remain vulnerable due to weak security protocols.

2.2 Cyber-Hacking and Socioeconomic Activities in Uyo

Hacking, as a fundamental type of cybercrime, has a significant effect on socioeconomic activities, as it affects businesses, undermines consumer trust, and

leads to large financial losses. Ajayi (2016), focusing on Uyo, found that hacking-related events, especially account takeovers, directly affect small and medium-sized enterprises (SMEs) as sensitive data and financial accounts are compromised. Bassey and Inyang (2020), also studying Uyo, found that an increase in hacking incidents is associated with a reduction in online business transactions. Ainsworth (2017) and Nakashima (2015) outlined the extensive financial implications of business email compromise, a form of hacking, on global supply chains, while Abdullah, Karim, and Zhang (2023) explained that such attacks exploit human weaknesses to deceive employees into making fraudulent transactions at massive cost. Choo *et al.* (2023) measured this effect by showing that such attacks cause financial, operational, and reputational losses to organisations. The financial effects of hacking extend beyond direct monetary loss to inflated operational expenses and reduced productivity. Akpan and Ekong (2022) and Akpan and Ekanem (2024), , found that the continuous risk of hacking in Uyo forces SMEs to spend heavily on cybersecurity, a cost that, according to Nse (2023), diverts funds that would otherwise support expansion or innovation. Anderson and Bohme (2024) argued from an international perspective that cybersecurity outlay has become an inseparable part of doing business in the digital era, a burden experienced more acutely in developing economies, a view supported by Campbell and Nichols (2024), who described cybercrime as a significant obstacle to economic growth in developing countries.

Loss of consumer confidence is one of the most consequential intangible costs of hacking. Accenture (2019) found that consumers become more reluctant to use online services following high-profile data breaches. Akpan and Udoh (2024), focusing on Uyo, found that recurring information-system breaches reduce web-based purchases and the use of online payment systems, a finding corroborated by Okon (2023), who attributed the erosion of trust in Uyo's digital economy to the increased prevalence of cybercrime. Calo (2019) further noted that identity theft following data breaches, a frequent outcome of hacking, exposes consumers to a persistent feeling of vulnerability, a point substantiated by the Federal Trade Commission (2019) in its review of the Equifax breach. Sociological and criminological explanations help account for the persistence of hacking, particularly among young people. Agnew's (1992) General Strain Theory and Berkowitz's (1989) frustration-aggression hypothesis both suggest that economic pressure and social frustration can drive deviant behaviour, a proposition Bello and Temitayo (2017) applied directly to Nigerian cities. Akpan and Nnamdi (2023), analysing Akwa Ibom State specifically, found a strong relationship between youth unemployment and participation in hacking. Cohen and Felson's (1979) Routine Activity Theory offers a complementary account: Holt and Bossler (2009) applied the theory to cybercrime, arguing that the ease of accessing online targets combined with infrequent, ineffective law enforcement creates opportunities for hacking to flourish.

Hacking in Uyo is further sustained by technological gaps and socio-economic vulnerabilities. Akpan, Etim, and Nkanta (2022) and Etim *et al.* (2022) both identified technological vulnerabilities and insufficient digital literacy as key factors exposing Uyo residents to hacking, a position reinforced by Essien and Etok (2023), who argued that the digital divide compounds vulnerability among those with lower access to technology and education. Ekpo and Etim (2021) and Essien (2022) found that efforts to raise the population of digitally literate individuals in Uyo have not been as effective as intended.

Ogbonnaya's (2020) demographic analysis of cybercrime offenders in Uyo found that they tend to be young, educated, and unemployed, a pattern also noted by Ibekwe and Okoro (2021) in their study of youth involvement in cybercrime in the area. Legal and institutional responses to hacking remain constrained. Adebayo and Mohammed (2021), focusing on Uyo, criticised the poor legal system and shortage of qualified law enforcement personnel as obstacles to enforcing the Cybercrime (Prohibition, Prevention) Act 2015. Jones (2021) noted the difficulty of tracking transnational cybercriminals, which reduces the effectiveness of local enforcement, while Bassey *et al. (2023)* proposed public-private partnerships as a more effective strategy for Uyo.

The social and psychological effects of hacking on victims constitute an important, though comparatively under-examined, dimension of the phenomenon. Ayodeji *et al.* (2018) examined the psychosocial impacts of cyberstalking, a related form of hacking, on victims in Nigeria, while Inyang and Abasi (2023), focusing on Uyo, found that digital vulnerability produces measurable stress and anxiety among business owners. Bassey and Inyang (2020) further observed that victims of hacking-related financial fraud in Uyo often feel ashamed and decline to report the crime, a pattern consistent with the concept of social stigma discussed by Mendes (2020) in relation to digital harassment more broadly. Hacking also threatens entrepreneurship and innovation, which are central to Uyo's economic future. Acs and Szerb (2023) argued that entrepreneurship is a primary source of economic development in developing countries and that the absence of digital security threatens it directly. This is corroborated by Ajayi's (2016) finding that hacking impedes the growth of SMEs in Uyo and their adoption of newer technologies.

2.3 Theoretical Framework

Routine Activity Theory (RAT), developed by Cohen and Felson (1979), holds that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge in time and space. Applied to Uyo, the theory suggests that constant online routines, such as banking, shopping, and social networking, expose residents and businesses to motivated hackers, while weak passwords, unpatched software, and low cybersecurity awareness represent a lack of capable guardianship online (Holt and Bossler, 2009). RAT has, however, been criticised for focusing narrowly on situational opportunity while underplaying the deeper socio-economic drivers of offending and for implicitly shifting the burden of prevention onto victims through an emphasis on "target hardening".

General Strain Theory (GST), formulated by Agnew (1992), holds that strain arising from blocked goals, the loss of valued stimuli, or exposure to negative experiences generates negative emotions that may be resolved through criminal behaviour. Applied to hacking, GST suggests that the frustration of unemployed or economically disadvantaged youth may find expression in hacking as an alternative route to material success, a proposition consistent with Akpan and Nnamdi (2023) finding of a link between youth unemployment and hacking in Akwa Ibom State. Both theories jointly frame this study: RAT explains why hacking opportunities persist in Uyo's digital environment, while GST explains the socio-economic pressures that motivate offenders.

3. METHODOLOGY

The study adopted a descriptive survey design, considered appropriate for investigating the prevalence and impact of cybercrime victimisation on socio-economic activities. The research was carried out in

Uyo Urban, Akwa Ibom State, a fast-developing urban centre and state capital characterised by rising internet penetration and a heterogeneous population engaged in banking, e-commerce, hospitality, telecommunications, and education. The population of the study comprised residents and business operators in Uyo who use internet-based services such as online banking, e-commerce, and social media. Based on the 2024 projected population of Uyo metropolitan area (1,393,000; NPC, 2024), the Taro Yamane (1966) formula was applied at a 5% margin of error to derive a sample size of 400 respondents, to whom questionnaire were administered, and 384 were successfully retrieved. A multi-stage sampling technique was used: cluster sampling across three political wards (Uyo Urban I, II, and III), followed by stratified sampling to ensure representation across age, socioeconomic status, and occupational sector, and simple random sampling within each stratum.

Data were collected using the Cybercrime Victimisation and Socioeconomic Impact Questionnaire (CVSIQ), a structured instrument comprising sections on demographic data, cybercrime victimisation experience, and perceived socio-economic impact, administered through both face-to-face and online channels. The instrument was reviewed for content and construct validity and the reliability was assessed through a test-retest procedure on 20 respondents (10 of whom were excluded from the main study), yielding a Cronbach's alpha above the acceptable threshold of 0.80. Data were analysed using the Statistical Package for the Social Sciences (SPSS); descriptive statistics (frequencies, means, and standard deviations) summarised respondents' experiences, while Simple Linear Regression Analysis (SLRA) tested the relationship between hacking victimisation and socio-economic activities. Ethical procedures included informed consent, voluntary participation, and assurance of confidentiality and anonymity.

4. RESULTS AND DISCUSSION

4.1 Impact of Cyber-Hacking on Socio-Economic Activities

The Table 1 presents respondents' ratings of the impact of cyber-hacking on socio-economic activities (N = 384). Respondents rated the negative effect on financial transactions highest (mean = 3.73; SD = 0.60), followed by reduced business productivity (mean = 3.42; SD = 1.06), discouragement of digital payment (mean = 2.53; SD = 1.18), and loss of customers (mean = 2.96; SD = 1.06). All mean scores exceeded the midpoint (2.00) of the four-point Likert scale, indicating a widespread and significant experience of hacking's impact in the study area. The comparatively high standard deviation associated with digital payment (SD = 1.18) suggests divergent respondent experiences, reflecting differing causes and patterns of hacking-related disruption across businesses in Uyo.

Table 1: Respondents' Rating of the Impact of Cyber-Hacking on Socio-Economic Activities (N = 384)

Effect of Cyber-Hacking	Mean	SD
Negatively affects financial transaction	3.73	0.60
Discourages digital payment	2.53	1.18
Reduces business productivity	3.42	1.06
Loss of customers	2.96	1.06

Source: Fieldwork (2025)

In assessing the significant effect of cybercrime (hacking) on socio-economic activities in Uyo urban. A simple linear regression analysis was conducted, with respondents' ratings of the proliferation of hacking as the independent variable and their ratings of hacking's impact on socio-economic activities as the dependent variable. The relationship between the two variables was strong and positive (R = .955), with the independent variable explaining 91.2% of the variance in socio-economic activities (R^2 = .912). The Analysis of Variance (ANOVA) was statistically significant, F (1, 382) = 3952.9, p < .05, a significant effect. The beta weight contribution of hacking on socio-economic activities was negative and significant (β = -.955; t = 62.872; p < .05), such that a unit increase in hacking activity was associated with a 0.986-unit reduction in socio-economic activities in the study area.

Table 2: Simple Linear Regression Analysis of the Effect of Cyber-Hacking on Socio-Economic Activities in Uyo Local Government Area (N = 384)

Statistic	Value
R	.955
R^2	.912
Adjusted R^2	.912
Std. Error	.240
F (1, 382)	3952.893
Sig.	.000
B (Hacking)	-.986
Beta	-.955
t	62.872
Sig.	.001

Dependent Variable: Socioeconomic activities

4.2 Discussion of Findings

The finding that socio-economic activities are significantly affected by cyber-hacking (p < .05) is supported by the broader literature, which highlights concerns beyond direct financial loss. Inyang and Abasi (2023) found that the stress and fear experienced by victimised business owners have a direct negative bearing on productivity and operational effectiveness. This suggests that the psychological toll of hacking, when experienced across a business community, can stifle economic growth by creating an atmosphere of fear that discourages the use of digital technology and innovation, a dynamic Akpan and Inyang (2023) argue can seriously undermine regional competitiveness.

The finding also resonates with

broader theoretical arguments about how cyber-risk constrains socio-economic mobility and access to opportunity in emerging digital economies. Udotong and Usen (2021) reported that chronic victimisation undermines users' willingness to engage in online economic activity, which is central to building sustainable jobs and economic resilience. The existence of significant effects in this study therefore provides empirical support for the view that hacking is not simply a criminal act but a structural block to socio-economic growth, actively obstructing the digital interaction that is a plausible source of diversification and development.

The finding is also consistent with the two guiding theories. Under General Strain Theory, the stress resulting from victimisation, resource loss, or heightened insecurity can reduce productivity and economic participation; hacking victims in Uyo therefore suffer not only monetary losses but also a loss of confidence in computerised systems that discourages continued digital engagement. Under Routine Activity Theory, the frequency of hacking attempts is a function of the availability of suitable targets, in this case, businesses with insufficient digital infrastructure and low levels of cybersecurity awareness. The combination of psychological strain and structural vulnerability substantiates the rejection of the null hypothesis and demonstrates that cybercrime constitutes a direct threat to economic viability both because it diminishes personal engagement with digital platforms and because it exploits systemic weaknesses in local cybersecurity infrastructure.

5. CONCLUSION AND RECOMMENDATIONS

The study concludes that cyber-hacking exerts a statistically significant negative effect on socio-economic activities in Uyo urban, explaining over 91% of the variance in the disruption of such activities. Hacking undermines financial transactions, discourages digital payment, reduces business productivity, and contributes to loss of customers while simultaneously eroding consumer trust and deterring the digital innovation on which Uyo's economic future depends. Hacking should therefore be understood not merely as an isolated criminal act but as a structural impediment to sustainable digital and economic development in the study area.

Based on these findings, the study recommends that the Government of Uyo Local Government Area, in partnership with tech hubs and universities, establish a subsidised cybersecurity audit programme for small and medium-sized enterprises, offering low-cost professional assessments of online infrastructure and guidance on applying necessary security patches. Financial institutions and digital service providers operating in Uyo should be encouraged to strengthen network security and deploy effective firewall systems, while regular cybersecurity training and periodic penetration testing should be institutionalised within local businesses. Furthermore, public-private partnerships, as proposed by Bassey, Ekong and Udo (2023), should be strengthened to improve the enforcement of the Cybercrime Act 2015 within the Local Government Area, and mental health and victim-support services should be incorporated into local cybercrime response strategies to address the psychological toll documented among victimised business owners.

REFERENCES

Abdullah, H., Karim, A. and Zhang, T. (2023). Business email compromise: A growing cyber threat to organizations. *Journal of Cybersecurity,* 8(3), 115-129.

Accenture. (2019). *Consumer Cybersecurity Confidence Index.*

Acs, Z. J. and Szerb, L. (2023). Entrepreneurship and economic growth in developing nations. *Entrepreneurship Theory and Practice*, 47(3), 430-450.

Adebayo, T. O., and Mohammed, S. J. (2021). The challenges of enforcing cybercrime laws in Nigeria: A case study of Uyo. *Journal of Nigerian Law and Technology,* 19(4), 72-88.

Adesanya, A. and Akinyele, J. (2023). Cybercrime victimization in Nigeria's urban areas: An examination. *Journal of Digital Security Studies,* 15(2), 45-67.

Adesina, O. (2021). *Trends in cybercrime and the Nigerian youth*. Abuja: Nigerian Cybersecurity Review.

Agnew, R. (1992). *Foundation for a general strain theory of crime and delinquency*. *Criminology,* 30(1), 47-88.

Ainsworth, S. (2017). How Business Email Compromise Attacks Disrupt Global Supply Chains. *Business Insider.* 10(2), 34-40.

Ajayi, O. A. (2016). *Cybercrime and its impact on small and medium-sized enterprises in Nigeria: A study of Uyo Local Government Area. Journal of Information Security and Privacy,* 5(2), 45-61.

Akpan, I., and Nnamdi, O. (2023). Factors influencing youth engagement in cybercrime in Akwa Ibom. *Nigerian Journal of Criminology,* 8(4), 123-145.

Akpan, O. E., and Ekanem, U. (2024). The economic consequences of cybercrime in Uyo Local Government Area: A focus on SMEs. *Business and Technology Journal,* 11(1), 58-72.

Akpan, O. E., and Ekong, S. (2022). Cybercrime and its economic implications for SMEs in Uyo Local Government Area. *Journal of Nigerian Business and Economics,* 14(2), 134-148.

Akpan, O. E., and Inyang, I. (2023). The psychological impact of cybercrime on Uyo's entrepreneurs: The stress of digital vulnerability. *Journal of Entrepreneurship and Digital Economy,* 4(2), 22-38.

Akpan, O. E. and Udoh, M. (2024). Cybercrime and consumer trust in Uyo's digital economy: Impacts on e-commerce and financial stability. *Journal of Digital Economy and Security,* 9(1), 101-116.

Akpan, O., Etim, I., and Nkanta, M. (2022). Cybercrime victimization in Uyo: Technological vulnerabilities and limited digital literacy. *Journal of Cybersecurity and Law*, 5(2), 112-129.

Ayodeji, O., Olamide, F., and Akinbile, B. (2018). Psychosocial impacts of cyberstalking on victims in Nigeria. *African Journal of Criminology and Psychology,* 6(2), 88-104.

Bassey, E., Ekong, S., and Udo, M. (2023). Public-private partnerships as a strategy for combating cybercrime in Uyo Local Government Area. *Journal of Cybersecurity Policy,* 7(1), 33-49.

Bassey, E., and Inyang, I. (2020). Hacking and its effects on online business transactions in Uyo. *Nigerian Journal of Business and Technology,* 6(2), 71-85.

BBC. (2014). Sony Pictures hack: What we know. *BBC News.*

BBC. (2017). Maersk cyberattack: Shipping giant hit by global ransomware. *BBC News.*

Bello, K., and Temitayo, O. (2017). Economic strain and cybercrime in Nigerian cities. *Journal of Criminology and Social Development,* 5(1), 22-38.

Berkowitz, L. (1989). Frustration-aggression hypothesis: Examination and reformulation. *Psychological Bulletin,*

106(1), 59-73.

Calo, R. (2019). *Privacy and the future of identity protection.* Cambridge: Cambridge University Press.

Chioma, N., Uche, O., and Eze, F. (2017). Cyber insecurity in Nigeria: Root causes and responses. *West African Journal of Security Studies,* 4(2), 51-69.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology,* 2(1), 308-333.

Choo, K. R., Smith, R., and Doe, J. (2023). The economic and reputational costs of business email compromise. *Journal of Cybercrime and Corporate Security,* 9(2), 77-95.

Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 44(4), 588-608.

Cybersecurity Ventures. (2021). *Cybercrime damages report.*

Ekong, S. (2023). Digital infrastructure expansion and cybersecurity vulnerabilities in Uyo. *Journal of Development Studies and Technology,* 8(1), 12-29.

Ekpo, E., and Etim, U. (2021). The effect of digital literacy campaigns on cybersecurity awareness in Uyo. *Journal of Media and Communication Studies,* 9(3), 66-82.

Essien, I. (2022). Evaluating the effectiveness of cybersecurity awareness campaigns in Uyo Local Government Area. *African Journal of Information Systems,* 14(2), 101-119.

Essien, I., and Etok, U. (2023). The digital divide and cybercrime vulnerability in Uyo Local Government Area. *Journal of Digital Inequality Studies,* 5(1), 40-58.

Etim, I., Ufot, M., and Akpan, S. (2022). Technological vulnerabilities and digital literacy in Uyo Local Government Area. *Journal of Cybersecurity Awareness,* 3(2), 55-70.

Federal Trade Commission. (2019). *Equifax data breach settlement.*

Holt, T. J. and Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior,* 30(1), 1-25.

Ibekwe, C. and Okoro, F. (2021). Youth involvement in cybercrime in Uyo Local Government Area. *Nigerian Journal of Youth Studies,* 9(2), 33-51.

Inyang, I., and Abasi, A. (2023). Psychological effects of digital vulnerability on business owners in Uyo. *Journal of Entrepreneurial Psychology,* 6(1), 15-31.

Jones, C. (2021). Tracking transnational cybercriminals: Challenges for local law enforcement. *International Journal of Cybercrime and Law Enforcement,* 5(2), 88-104.

Jones, C. and Brown, T. (2020). Anonymity and geographic distance in global cybercrime victimization. *Journal of International Criminology,* 7(3), 45-60.

Kothari, R. (2019). From lone hackers to organized syndicates: The evolution of cybercrime. *International Journal of Cybersecurity Research,* 3(1), 12-28.

Leukfeldt, R. and Holt, T. J. (2020). The human factor of cybercrime. New York: Routledge.

Markets and Markets. (2020). *Global cybersecurity market report.*

Mendes, K. (2020). Social stigma and the reporting of digital harassment. *Journal of Media and Gender Studies,* 8(2), 91-108.

Nakashima, E. (2015). The financial impact of

business email compromise on global supply chains. *Washington Post Technology Review.*

Nse, U. (2023). The cost of cybersecurity compliance for small businesses in Uyo. *Journal of Small Business Economics,* 11(2), 45-61.

Obinna, C. and Nneka, A. (2024). Types of cybercrimes among undergraduates in tertiary institutions in Anambra State. *Nigerian Journal of Educational Technology,* 12(1), 21-40.

Ogbonnaya, C. (2020). Demographic and socioeconomic analysis of cybercrime offenders in Uyo. *Journal of Criminological Research,* 8(3), 102-119.

Omorogbe, O.H., Amoforitse, F. I., Ozobialu. E.C., Eduje, A.I., Obande, B.O., & Ukaoha, K, C.,(2026) Resolving the Scalability Explainability – Adaptability Trilemma in Hybrid Optimization Systems for Disaster Management, International Journal Of Data Science And Analytics (Ijdsa) pp 54-59

https://www.pacadpub.com/index.php/ijdsa/index

Omorogbe, O. H. & Amenaghawon, V.A. (2026) Development of an Embedded Artificial Intelligence Framework for Intelligent E-Learning Management Systems , GAIJIST Vol.1.1.2026 pp.20-24 http://globreshub.org/index.php/gaijist

Omorogbe, O.H. Amoforitse, F. I. Ozobialu, E.C.Ukaoha, K.C.& Eduje, A. I., (2026) Explainable Reinforcement Learning for Adaptive Autonomous Agents: A Frame work for interpretable Decision-Making in Dynamic Environments, https://www.pacadpub.com/index.php/ijdsa/index

Okon, E. (2023). Trust erosion in Uyo's digital economy: The role of cybercrime. *Journal of Digital Economy Studies,* 6(2), 55-72.

Okpa, J. T. (2022). Cyberspace, hacking and the economic sustenance of corporate organizations in Cross River State. *Nigerian Journal of Corporate Security,* 10(1), 33-52.

Pius, N. (2021). Youths and cyber insecurity in Nigeria: Hacking, identity theft, and religious response. *West African Journal of Youth and Development,* 9(2), 61-79.

Smith, J. (2020). The sophistication of cyber-enabled threats. *Journal of Global Cybersecurity,* 4(1), 5-19.

Sullivan, C. (2020). Cybercrime and the erosion of the digital dividend in developing economies. *Journal of Development and Technology,* 7(1), 22-38.

U.S. Department of Homeland Security. (2018). *Cybersecurity and infrastructure resilience report.*

Udotong, I., and Usen, S. (2021). Digital trust and cybercrime victimisation in Nigerian urban centres. *Journal of Digital Behaviour,* 4(2), 71-88.

Wilson, P. (2020). Technology and cybercrime. *Journal of Digital Society,* 10(4), 98-134.

Funding: This research is not funded.

Acknowledgments

Not applicable.

Conflicts of Interest

The authors declare no conflict of interest.

Authenticity

This manuscript is an original work