NIGERIAN LECTURERS' PERCEPTION OF DIGITAL VULNERABILITY AND CYBER SECURITY GOVERNANCE IN NIGERIA

By

AWODI, Sheidu[1]

Department of Mass Communication,Kogi State University, Kabba
awodisheidu@gmail.com, +2348059138971, +2349131144929,
https://orcid.org/0000-0001-7944-017X

AKINWUMI, Rasheed Paul[2]

Department of Mass Communication, Achievers University, Owo, Nigeria
akinwumi2128@gmail.com, akinwumi.rp@achievers.edu.ng
+2349034251305, +2347025269929,
https://orcid.org/0009-0003-3578-11

OLOGUN, Opeyemi Olorunishola[3]

Department of Mass Communication, Kogi State University, Kabba
ooologun@ksukabba.edu.ng, ologunopeyemi@gmail.com
08164916157, 08054945991
https://orcid.org/0009-0008-1375-6575

Corresponding Email: awodisheidu@gmail.com

Abstract

The high level of internet penetration has led to significant security concerns in Nigeria, placing internet users at risk of increased cyberattacks. This study explores the perception of Nigerian university lecturers on digital vulnerability and cybersecurity governance. It specifically examined risky online behaviours, effects of cybercrime on national development, and the effectiveness of Nigerian digital policies. The study was anchored on the Routine Activity theory and Technological Determinism. A descriptive survey design was adopted, involving 146 respondents from two public universities in Kogi State. The data were analysed using Mean Score Analysis with a benchmark mean of 3.00. Findings revealed that insecure passwords (3.34), using unsecured Wi-Fi connections (3.22), and disclosing personal data through the Internet (3.47) are significant contributors to vulnerability. Cybercrime was reported by the respondents as affecting national development (3.45), resulting in the closing of businesses and job losses

(3.41), degradation of morals (3.07) and decreased foreign investments (3.32). The Study also identified the weaknesses in cybersecurity governance in Nigeria as a weak policy implementation (2.85), a lack of institutional coordination (3.15) and insufficient resources (2.71). It concluded that the Nigerian digital ecosystem is not safe for online users due to personal and institutional vulnerability. It recommends digital literacy, behavioural change, investment in cybersecurity infrastructure, skills development and international collaboration as important measures in the establishment of a strong, inclusive and secure digital ecosystem in the country.
Keywords:*Cybercrime, Digital Vulnerability, Governance, Routine Activity TheoryandDigital Policy*.

Introduction

As Nigeria advances in digitalisation, the Nigerian Communications Commission (2024) submits that there were about 134.78 million internet subscribers in the country as of October 2024. This percentage constitutes a significant portion of the national population, signifying a large number of people using digital infrastructure. Nevertheless, this online growth does not come without a cost. The proportion of the population that is poorly informed on the practise of cybersecurity is quite substantial, which means that they are susceptible to digital threats. Presently, Nigeria is faced with an increasing level of cybercrime at a time when its online economy is beginning to grow exponentially, having serious adverse consequences on its national economy (Ukhami& Abdulsalam, 2024; Olalekan, 2025).

Nigeria currently battles with the incessant rise in cases of cybercrimes, leading to the enactment of the Cybercrime Prohibition and Prevention Act of 2015, amended in 2024 (LawCareNigeria, 2024). As submitted by the Economic and Financial Crimes Commission (EFCC, 2024), the country lost over 764.1 billion Naira to cybercrime from 2015 to 2024. Organisations in Nigeria saw a bewildering average weekly number of cyberattacks of 4388 in the first quarter of 2025 over 2024, with a 47.30% year-on-year increase (BusinessDay, 2025; Pulse Nigeria, 2025). Placing Nigeria in the 13th position on the Global Threat Index in 2023, Nigerian banks lost approximately 3.7 billion Naira through mobile device customers. Thus, these records constitute a huge level of concern for Nigeria's national progress, electronic credibility and economic sustainability (Pulse Nigeria, 2025).

Even though cybercrime is generally perceived as a technical problem, some recent investigations have shown that causal factors of cybercrime in Nigeria are deeply rooted in the socioeconomic basis in terms of

unemployment among young people, poverty, and more or less ideology behind internet fraud among the users (Uzochukwu and Nwankwo, 2020). They posited that such a challenge is synonymous with a severe and troubled interaction between various socio-economic and technological problems. They argued that cybercrime is propagated by the search for easy money, particularly among the youth, against the background of a high rate of unemployment and poverty in Nigeria (ThisDay, 2025).

In addition, the online fraud (also known as *Yahoo-Yahoo*) and a cult-like version have emerged (*Yahoo Plus*), which means that it is not only digitally manipulated but also socially cum diabolically (Ayotunde, 2025). The situation is worsened by the fact that Nigeria lacks digital strengths both in its structure and its human resources. The extreme shortage of cybersecurity expertise also left most establishments short-staffed and individuals ill-equipped to handle the growing threats.

Also, this threatening reality is worsened by the growing sophistication of Artificial Intelligence (AI) in making phishing adverts automatically, creating polymorphic malware, and deepfakes hyper-realistic contents (Thisdaylive, 2025). Such developments as AI are causing a loss of credibility for digital communication. Although the Nigerian government had amended the corresponding cybercrime laws (Cybercrime Prohibition and Prevention Amendment Act 2024 and the Nigeria Data Protection Act [NDPA] 2023), problems still exist in regulatory gaps, large-scale corruption, and the insufficiency of law enforcement agencies (Ukhami& Abdulsalam, 2024; Ayotunde, 2025).

The digital governance system in Nigeria is still reactive and divisive despite the formulation of policies such as the National Cybersecurity Policy and Strategy (2021), and the absence of a cross-policy investigation into the interrelationship between cybercrime drivers and digital vulnerabilities. Although cybercrime has been individually researched, few studies have engaged in a systematic analysis of the relationship between them to develop a cyber-insecure ecosystem (Uwakwe & Oji, 2021).

Statement of problem

The level of the digital transformation in Nigeria has given the country vast internet access, with a population of internet active subscribers reaching 134.78 million (NCC, 2024). However, this advancement has been accompanied by an increase in cybercrimes, which have laid bare serious gaps in the digital ecosystem of the country. Cheque Point Software Technologies showed that Nigerians suffered an average of 4,200 cyberattacks per organisation weekly in 2025, which was 60% higher than the global average (BusinessDay, 2025). Socio-economic

conditions, including unemployment among young people, poverty, and internet illiteracy, add to such threats and provide a fertile ground for cybercriminal activity (Tijani & Adams, 2024). Although the implementation of the Cybercrime Act in 2015 and its enhancement in 2024 took place, not all actions have been taken, and the institutional responses are disjointed (Oliobi et al., 2026). The ongoing disconnect between policy development and actualisation has exposed the digital infrastructure in Nigeria (Uzochukwu and Nwankwo, 2020). Therefore, this study answers the following questions;

i. What are risky online behaviours that contribute to digital vulnerability?
ii. What are the impacts of cybercrime on the national development of Nigeria?
iii. How effective are Nigeria's digital policies and institutional responses in combating cyber threats?

Digital Vulnerability and Cyber Security in Nigeria

Digital vulnerability refers to the susceptibility of people, institutions, and systems to threats that arise from the use of digital technologies. The fast spread of online connectivity and mobile connections in Nigeria has subjected the users to an increasing number of cyber threats. With the increased pace of digital development, the risk of exploitation by cybercriminals is equally high since vulnerable infrastructure, low levels of digital literacy, and insufficient policy implementation contribute to the ease with which cybercriminals exploit and abuse it (Ibrahim and Adamu, 2021).The level of attacks on the digital environment of the country is increasing due to the growing number of online citizens and poor cybersecurity.

Adenenyi (2022) argues that cybercrime has become a national security issue which affects individuals andinstitutions. The cyberspace in Nigeria is porous because of the absence of a forensic capacity, and this has ensured that the offenders cannot be easily tracked and prosecuted. As opined by Sibe &Kaunert (2024), there are not only technical types of vulnerability, but also behavioural ones, which depend on socio-economic conditions and digital illiteracy. Some of the reasons behind the digital vulnerability situation in Nigeria include low cybersecurity awareness and a lack of digital hygiene and infrastructure. The majority of users are ill-educated about what online safety means, and, hence, they are easy prey for phishing and social engineering crimes. Moreover, the fact that most platforms do not have solid encryption algorithms and effective authentication heightens the risk.

Cybersecurity governance in Nigeria is yet to be developed, even though the Cybercrime Act of 2015 has offered a platform with regard to cyber threats and the legal responses; it has not been properly implemented. Cybersecurity overseers do not have resources and are commonly not coordinated, which results in disjointed responses. Adelaiye, Ibrahim and Ipole (2024) submit that governance operations will not be effective unless they are supported by a cohesive approach to cybersecurity within the country and enhanced institutional capacity. Digital governance has no accountability or transparency, further eroding the trust of the populace. The digital development in Nigeria is strictly connected with the capacity of the country to protect its cyberspace. The vulnerabilities not only pose a threat to individual users, but also hinder economic growth, innovation and foreign investment. Companies do not want to use digital solutions when data breaches and cyber fraud are widespread. Furthermore, the digital divide continues to grow because vulnerable groups of people, particularly in rural settings, are left out either out of fear or distrust towards digital systems (Adeniyi, 2022).

The fight against cybercrime should be systematised with the aid of elaborate policies and interagency cooperation. Nigeria is in need of reinforcing its digital governance system by adopting cybersecurity as part of national development policies. This involves investing in cybersecurity training, setting up forensic laboratories, and ensuring that the digital service providers comply. The value of involvement of a multi-stakeholder, such as civil society and the private sector, in the process of creating a robust digital ecosystem is emphasised by Ibrahim and Adamu (2021). The role of behavioural change is as significant as technological solutions are in combating cybercrime, as Sibe and Kaunert (2024) observe.

Due to the transnationalism of cybercrime, Nigeria needs to cooperate with regional and international partners to exchange resources through intelligence sharing, harmonise the laws, and build capacity. The countries of West Africa are not an exception, as they have to struggle with the same issues, and cooperation is the way to become more resilient together. There are models of cooperation in international frameworks such as the Budapest Convention. As Adelaiye et al. (2024) emphasise, the Nigerian involvement in international cybersecurity efforts is crucial to the enhancement of its protection at home. Overall, digital vulnerability and cybercrime have been a big threat to the digital development and governance of Nigeria. These problems can only be solved through a multi-dimensional solution involving policy changes, technological development, education of society, and international

collaboration. With the ongoing digitalisation of Nigeria, cyberspace security should be given priority to be able to craft the development to be inclusive, secure and sustainable.

Empirical Review

Opesade and Adetona (2021) evaluated the use of the internet and the prevalence of cyber-risk in secondary school students in Nigeria. Through a survey approach and the Technology Acceptance Model (TAM), the researchers discovered that students were well exposed to the internet, though they were not very aware of the dangers associated with cyber. Such risky behaviours as the use of unsecured Wi-Fi connections and the lack of software updates were typical. The studyconcluded that a deficiency in organised digital education contributed to the enhancement of digital vulnerability. Some of the recommendations included school-based cybersecurity awareness. This is consistent with the present study since it does identify behavioural risks, but its demographic emphasis and theoretical concept are different.

Gimba and Ibrahim (2023) used the Routine Activity Theory in a study that examined online fraud victimisation among youths in Gombe. Using a 300-responder quantitative survey, the research established that low digital hygiene, such as using weak passwords and high usage of free Wi-Fi, contributed greatly to a higher vulnerability. The study concluded that the socio-economic factors and absence of digital literacy were important facilitators of cyber victimisation. They suggested specific awareness and community-based interventions. This work is rather closer to the ongoing research in terms of theory and conclusions, which supports the behavioural aspect of digital vulnerability.

Tijani and Adams (2024) investigated the effects of cybercrime on national security in Nigeria through a desk review based on a mixed-method. The study used the Routine Activity Theory and General Strain Theory to examine official statistics and policy documents. It was discovered that cybercrime compromises societal confidence, destabilises essential infrastructure, and is a threat to national security. The study came to the conclusion that cyber-offending is motivated by socio-economic pressure and the poor guardianship of institutions. They did suggest organisational reinforcements and investment in digital resilience. This study is consistent with the existing studies in terms of theoretical grounds and focuses on the socio-economic impact of cybercrime.

Okoru and Oluku (2024) examined how cybercrime is associated with national development in Nigeria. Based on the Conflict Theory, the

qualitative study found unemployment, poverty, and poor digital infrastructure to be among the major sources of cybercrime. Results showed that cybercrime negatively affects the development of the economy, discourages foreign investment, and undermines social values. The study concluded that the solution to cybercrime lies in a comprehensive approach of economic reforms and the realisation of digital policies. Although the study under consideration has the same conclusions, it is different in its approach and theoretical orientation.

Munachimso and Badillo-Urquiola (2024) examined the concept of digital access and online risks among adolescents in the Federal Capital Territory of Nigeria by applying a mixed-methodology. The study was based on the Ecological Systems Theory and attempted to comprehend the path that adolescents undertake in the online space and the dangers that they face. The study included a survey and an interview with 409 students, and it was discovered that risk behaviours like sharing personal information, communicating with strangers and poor password habits were common. The study inferred that adolescents had low levels of digital literacy, which exposed them to cyber threats. They suggested that digital safety should be introduced in schools. Both of them have a commonality in their focus on behavioural vulnerabilities, as compared to the current study, which includes university lecturers, whereas the former focuses on teenagers.

Obajobi, Akoji, and Umaru (2024) carried out a review on how cybercrime affects the development of Nigeria as a country. The research was a synthesis of secondary data and a chance to use the Socio-Technical Systems Theory in the analysis of the interaction of technology and society. It was discovered that cyberspace crime has negative impacts on political stability, economic performance, and societal cohesion. The studystressed the necessity to work as multi-stakeholders and on international collaboration. This will be an addition to the existing study in that it documents the effects of cybercrime in aspects other than the economic aspect.

Ogene (2025) discussed the issue of cybersecurity and IT governance in Nigeria, but employed a mixed-method research design. The study has found the lack of funding, laxity in regulations, and skills shortage as key obstacles to effective cybersecurity. It has been found that a strong digital economy requires strategic investment and regulatory reform. Public-private partnerships, as well as cybersecurity workforce development, were recommended. The research is useful in the context of complementing existing studies, since it focuses on structural and resource-based issues in policy implementation.

Framework

Routine Activity Theory (RAT)

Routine Activity Theory (RAT) was propounded by Lawrence E. Cohen and Marcus Felson in 1979. Initially developed to describe patterns of conventional crime, the theory states that crime happens when three factors come together: (i) a motivated offender, (ii) an appropriate target, and (iii) the lack of an effective guardian. It places more importance on the situational nature of crime in place of the psychological makeup of the criminal. Even though RAT was originally used in physical crimes, its concepts have been translated to the online environment, where internet-based criminals use their regular internet usage and systemic vulnerability to conduct attacks (Cohen and Felson, 1979; Yar, 2020).

The Routine Activity Theory has been criticised for its inability to consider more of the wider structural and psychological factors. Critics believe that RAT does not consider the factors of systemic inequality, cultural norms, and other offender motivations other than opportunity (Tade, 2013). In application to this study, cybercrime thrives in the presence of accessible digital targets, when an offender is driven by socio-economic factors, or the protective systems, like cybersecurity infrastructure or awareness, are ineffective or lacking (Yar, 2020; Ukhami and Abdulsalam, 2024). In application, the theory aligns with the submission that the prevalence of internet use in Nigeria, low levels of digital literacy, and institutional deficiencies are significant factors of cybercrime.

Digital Determinism Theory

The Technological Determinism Theory (TDT) was initially put forward by Thorstein Veblen at the beginning of the 20th century, and then developed by Harold Innis and Marshall McLuhan in the middle of the previous century (Wikipedia, 2024; eGyanKosh, 2024). Its basic principle is that technology is an autonomous evolving influence on society, institutions and human behaviour, which is frequently not dependent on human agency. As an illustration, communication technologies like the printing press and the internet are considered to be transformative and multi-structure their societies (Helpful Professor, 2024).

However, critics have argued that the theory is too reductionist because it does not consider social-economic, political and cultural contexts that shape the adoption and use of technology (Smith and Marx, 1994; Williams, 2003).

In application to this study, Technological Determinism describes how fast the penetration of the internet and mobile connectivity has offered both opportunities and threats. It helps determine risky online behaviour as an inevitable by-product of digital expansion, the socio-economic implications of cybercrime, the structural effects of technological evolution and the problems of policy efficacy as a sign of governance lagging behind technological innovation.

Material and Methods

This study adopted the descriptive survey method. The method was selected because it is effective in collecting data from a large population and drawing the patterns in perception and experience. From a population size of one thousand, one hundred and twenty-seven (1,127), the questionnaire was self-structured and administered to one hundred and forty-six (146) respondents from Kogi State University, Kabba and Prince Audu Abubakar University, Anyigba, both in Kogi State, respectively, via the online link https://forms.gle/oykizXdmvS7n29z79. This was done through random sampling to guarantee the representation. The instrument was structured to align with the objectives of the study, in line with digital vulnerability, awareness of cybercrime, and responses to digital governance policy. The items were measured using a 5-point Likert scale, where Strongly Agree (5) and Strongly Disagree (1) were on both ends. To ascertain the reliability of the instrument, a pilot test was done at the Confluence University of Science and Technology, Osara, Kogi State, which gave the Cronbach's alpha value of 0.82, which is considered an excellent internal consistency. As pointed out by Bryman (2016), pilot testing not within the main sample allows avoiding bias and preserving the research design integrity. The data collected were analysed using descriptive statistics, which consisted of mean scores and Standard Deviation, and, hence, assisted in the determination of the measures of central tendency and dispersion of the responses. Decisions were made using the benchmark mean score of 3.00; a score of more than 3.00 was regarded as accepted, and a score less than 3.00 was regarded as rejected. Tables were generated so that it would be easy to read the results, and interpretations regarding the statistical results were generated. This methodology guaranteed objectivity, transparency, and relevance concerning the aims of the study.

Results

Table 1: Risky Online Practices that contribute to Digital Vulnerability of users

Item Statement	SA	A	N	D	SD	Mean	SD	Decision

Weak passwords increase vulnerability	47	36	21	28	14	***3.34***	***1.19***	*Accepted*
Public Wi-Fi is a major threat	42	33	26	31	14	***3.22***	***1.23***	*Accepted*
Most users are aware of phishing techniques	28	30	29	36	23	***2.81***	***1.31***	*Rejected*
Sharing personal info online increases risk	51	39	18	24	14	***3.47***	***1.17***	*Accepted*
Mobile apps often compromise user privacy	38	35	27	29	17	***3.14***	***1.25***	*Accepted*
Many users ignore software updates	33	32	30	34	17	***2.97***	***1.28***	*Rejected*
Digital literacy reduces vulnerability	45	40	19	27	15	***3.36***	***1.20***	*Accepted*
Most people use secure passwords	26	29	31	38	22	***2.76***	***1.30***	*Rejected*

Source: Field work, 2025

Table 1 shows the perceptions of the respondents with regard to online digital risks, including the use of weak passwords, open Wi-Fi, and low levels of digital literacy. Such items as weak passwords heighten vulnerability, and sharing personal info online heightens risk, were rated above the benchmark of 3.00, meaning that there is general agreement. But such statements as the majority of users know about phishing methods, the majority of people use secure passwords, were disapproved, which indicates the user awareness and behaviour gaps.

Table 2: Perceived Impact of Cybercrime on Digital Eco-system of the Nigerian Society

	SA	**A**	**N**	**D**	**SD**	**Mean**	**SD**	**Decision**
Cybercrime affects national development	52	41	17	20	16	**3.54**	**1.18**	Accepted
It makes people vulnerable to	40	38	24	28	16	**3.27**	**1.22**	Accepted

quick success syndrome against hard work.								
Cybercrime threatens the digital economy and integrity.	22	27	32	39	26	**2.63**	**1.35**	Rejected
Cybercrime leads to closure of businesses and increases unemployment	48	37	20	25	16	**3.41**	**1.20**	Accepted
Cybercrime affect moral standard of society	36	34	28	30	18	**3.07**	**1.26**	Accepted
Cybercrime affect the health of victims	39	33	25	31	18	**3.11**	**1.24**	Accepted
Cybercrime is more prevalent in urban areas	30	31	29	35	21	**2.88**	**1.29**	Rejected
It affects foreign investment potentials	44	36	22	27	17	**3.32**	**1.21**	Accepted

Source: Field work, 2025

Table 2 the impacts of cybercrimes on society on national development, such as digital economy and integrity, closure of businesses and increases unemployment, affect moral standard of the society, affect the health of victims and foreign investments potentials. The vast majority of the items were accepted, and this indicates a good understanding of the effects of cybercrime affecting national development economically and socially.

Table 3: Perceived Effectiveness of Digital Policy and Responses to Cybercrime in Nigeria

Item Statement	**SA**	**A**	**N**	**D**	**SD**	**Mean**	**SD**	**Decision**
Cybercrime laws are effectively enforced	27	33	30	34	22	**2.85**	**1.28**	***Rejected***
Government supports digital literacy programmes	43	38	21	26	18	**3.30**	**1.22**	***Accepted***
Agencies	36	35	28	29	18	**3.15**	**1.25**	***Accepted***

collaborate on cybersecurity issues								
Cybercrime policies are well communicated to the public	29	31	30	33	23	**2.87**	**1.29**	***Rejected***
Funding for cybersecurity is adequate	25	28	32	36	25	**2.71**	**1.33**	***Rejected***
Government responds quickly to cyber incidents	34	32	27	31	22	**2.98**	**1.27**	***Rejected***
Public-private partnerships improve digital security	41	39	20	28	18	**3.29**	**1.23**	***Accepted***
Cybersecurity is prioritized in national development plans	38	36	24	30	18	**3.17**	**1.24**	***Accepted***

Source: Field work, 2025

Table 3 shows the views on the digital governance of Nigeria in the context of enforcement, funding, and cooperation of the institutions. Items such as government support for digital literacy programmes or public-private partnerships that enhance digital security were accepted, which means that people had moderate confidence in this policy work. In its turn, the claims on the effectiveness of enforcement and funding adequacy were dismissed, indicating the perceived flaws in the system of cybersecurity control in Nigeria.

Discussion

In line with the first objective of the study, which aims at examining lecturers' perceptions of risky online practices that contribute to the digital vulnerability of users, the first finding reveals that the major risky online behaviours that make online users vulnerable to cyberattacks are weak passwords, public Wi-Fi usage, the disclosure of personal information on the Internet, and neglecting software upgrades. In particular, weak passwords (mean = 3.34), disclosure of personal information online (mean = 3.47), highly accepted as risks and awareness of phishing techniques (mean = 2.81) and digital illiteracy (3.36), which indicates the gaps in user awareness and use. This affirms that poor digital hygiene and low cybersecurity literacy are two of the

major determinants of digital vulnerability among the Nigerian communities in universities. These findings are in agreement with Ibrahim and Adamu (2021), who submitted that the low level of digital literacy and ineffective cybersecurity habits increase the vulnerability to cyber threats in Nigeria.

On the same note, Sibe and Kaunert (2024) stated that technical vulnerabilities are not as fundamental as behavioural vulnerabilities in facilitating users to fall prey to cybercrime through the use of weak passwords and irresponsible sharing of information online. The evidence presented, according to which most users do not bother with software updates (2.97, rejected), is in alignment with Adeniyi (2022), who also reported that most Nigerian users do not pay much attention to basic digital hygiene, which exposes them to cybercriminals. In such a way, the present results support the previous research, which stated that user behaviour is a key factor of vulnerability. The findings, however, deviate from the position of Uzochukwu and Nwankwo (2020) that Nigerian youths are becoming more conscious of the methods of phishing, but the current results do not support it, as they reveal low awareness of phishing (mean = 2.81, rejected).

The disjunction implies that institutionalised attempts at password protection have failed to convert into the widespread use of protective practices among users. These vulnerabilities are also serious and are statistically substantiated. According to the Economic and Financial Crimes Commission (EFCC, 2024), Nigeria reported a loss of more than N764.1 billion to cybercrime between 2015 and 2024, and banks lost N3.7 billion to mobile device customers. These were losses in line with the current study's finding that mobile apps undermine user privacy (mean = 3.14, accepted), indicating that the perceived digital vulnerability is manifested in the actual economic implications. The NCC (2024) also recorded the fact that more than 172 million Nigerians are online, and this implies that even a small number of people who engage in risky habits may mean that their countries have been exposed to huge numbers.

From leans of Routine Activity Theory, in the online environment, the lack of strong passwords, low knowledge of phishing, and lack of software updates form an ideal target, and low digital literacy and insufficient institutional protection are the manifestations of the lack of a proper guard which validates the hypothesis that the communities in Nigerian universities are a representation of this theory, because their reckless internet habits offer avenues for cybercriminals with socio-economic intentions.

In response to the second objective which assess the perceived impacts of cybercrime on the digital eco-system of the Nigerian society, the finding indicated that cybercrime have negative impact on digital eco-system and national development as it affects digital economy and integrity, leads to closure of businesses and increases unemployment, affect moral standard of the society, affect the health of victims and foreign investments potentials. This finding affirms that cybercrime is not just a technical challenge, but also a socio-economic and developmental problem (Ibrahim and Adamu, 2021; Uzochukwu and Nwankwo, 2020). These findings also agree with Uzochukwu and Nwankwo (2020), who stated that unemployment and poverty are heightened by cybercrime in Nigeria, as people are scared of participating in online economic activities or opportunities.

On the same note, Ibrahim and Adamu (2021) pointed out that the digital space is being affected as individuals are seen as lacking integrity, which is a form of social capital in the digital economy. Moreover, the view that cybercrime has an impact on foreign investment is similar to Adeniyi (2022), who observed that pervasive cyber fraud discourages the use of digital solutions in Nigeria. These findings resonate with the RAT that crime happens when committed offenders see an appropriate target and the system of control does not work effectively.

Regarding the third objective, which concerns the evaluation of the perceived effectiveness of digital policy and responses to cybercrime in Nigeria, the Nigerian digital policy on cybercrime was rated as being moderate, with the majority seeing it as unsatisfactory. Some of the submissions are that cybercrime laws are effectively enforced (2.85), Cybercrime policies are well communicated to the public (2.87), funding for cybersecurity is adequate (2.71), and the government responds quickly to cyber incidents (2.98), being rejected. The data showed that there are policy structures, but they are not effectively implemented and enforced, which creates loopholes in cybersecurity policy implementation and regulation. This is in consonance with the argument of Adelaiye, Ibrahim, and Ipole (2024) that the National Cybersecurity Policy and Strategy (2021) is only alive on paper but far from reality, as the level of enforcement of cybercrime laws is inconsistent and underfunded.

The rejection of the efficacy of law enforcement and the sufficiency of funding in the study also agrees with the position of Sibe and Kaunert (2024), who highlighted that the system of cyber-governance in Nigeria lacks coordination and accountability. The idea of public-private collaboration as a means of enhancing the security of the digital environment is echoed by Ibrahim and Adamu (2021), who emphasised

the need to have multi-stakeholders in the development of a robust digital environment.

The findings can be attributed to the RAT that policies and governance structures in the Nigerian digital space are intended to be the theorised guardians against motivated offenders; nonetheless, the lack of effectiveness of law enforcement, the insufficiency of funding, and the poor responsiveness of the government to the fact that there is inadequate or no guardianship, breed opportunities for the escalating level of cybercrime.

Conclusion

The study concludes that digital vulnerability is self-incurred by engaging in risky online behaviours such as weak passwords, using open Wi-Fi connections, and poor digital literacy. It submits that there are technical cum socio-economic consequences of cybercrime as it affects the digital economy and integrity, leads to closure of businesses and increases unemployment, affects the moral standard of society, affects the health of victims and foreign investment potential. The assessment on governance responses gave an unsatisfactory view of the performance of the government policies in response to cybercrime in the country. These conclusions support the argument that cybercrime in Nigeria is both a systemic and behavioural issue, which needs better guardianship as stipulated by the Routine Activity Theory, where motivated offenders would take advantage of weak targets in the absence of effective institutional protection. Based on this conclusion, the following recommendations are put forth;

i. Nigerian education institutions should step up digital literacy initiatives in order to curb risky online behaviours amongst university lecturers.
ii. The government agencies need to intensify the application of the laws against cybercrime to bridge the gap between the formulation of the laws and their enforcement.
iii. Corresponding funding also needs to be made to the cybersecurity infrastructure and training to enhance national resilience against cyber threats.
iv. It needs to increase the public-private partnerships that will boost collaboration in ensuring the security of Nigeria's digital ecosystem.
v. The awareness programme must be developed to foster reporting of cybercrime incidents among the victims, hence the improvement of accountability and deterrence.

References

Adams, K., & Tijani, H. O. (2024). *Impact of cybercrime on national security in Nigeria*. Journal of Cybersecurity Studies.

Adelaiye, O., Ibrahim, Y. A., &Ipole, N. (2024). *Cybersecurity and Cybercrimes in Nigeria: An Overview of Challenges and Prospects*. Bingham University.

Adeniyi, I. (2022). *Cyber Security in Nigeria: Appraising Cybercrime, the Existing Legal Framework, the Challenges and the Way Forward*. The Erudite Journal of Leadership and Development.

Ayotunde, G. O. (2025, January 20). *CP-PSFU Receive in Audience Leadership of Ogun State Chapter of NANS, NAPS, ASONIS & GAPOSA*. Special Fraud Unit. https://www.specialfraudunit.org/2025/01/20/cp-psfu-receive-in-audience-leadership-of-ogun-state-chapter-of-nans-naps-asonis-gaposa/

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

BusinessDay. (2025, February 17). *Nigeria climbs cyber threat index as attacks mount*. Retrieved from https://businessday.ng/technology/article/nigeria-climbs-cyber-threat-index-as-attacks-mount.

Check Point Software Technologies. (2025). *African Perspectives on Cyber Security Report 2025*.

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

Economic and Financial Crimes Commission (EFCC). (2024). *EFCC Records Best-Ever Performance in 2024, Recovers N364bn, Secures 4,011 Convictions*. Arise News. https://www.arise.tv/efcc-records-best-ever-performance-in-2024-recovers-n364bn-secures-4011-convictions/

Gimba, A., & Ibrahim, M. (2023). Assessment on the vulnerability of online fraud victimization among youths in Gombe. Journal of Digital Risk and Security, 5(1), 45–59.

Ibrahim, M. T., & Adamu, Y. (2021). Youth, social media and cybercrime: A study of fraud culture in urban Nigeria. *African Communication Research, 14*(1), 55–74.

International Telecommunication Union (ITU, 2020). *Global cybersecurity index 2020*. International Telecommunication Union. https://www.itu.int/en/ITU-T/Result_Publications/gci2020.html

Interpol. (2024). *Cybercrime trends in Africa: Threat landscape and national responses*. Retrieved from https://www.interpol.int

Munachimso, B. O., & Badillo-Urquiola, K. (2024). Teens need to be educated on the danger: Digital access, online risks, and safety practices among Nigerian adolescents. arXiv.org.

National Cybersecurity Policy and Strategy. (2021). *Federal Government of Nigeria official publication*. Abuja: Office of the National Security Adviser.

Nigerian Communications Commission (NCC). (2024). *Internet subscription and digital access in Nigeria: A 2024 report*. Retrieved from https://www.ncc.gov.ng

Obajobi, J. J., Akoji, F. O., & Umaru, C. (2024). Impact of cybercrime on national development: A review on Nigeria. ResearchGate.

Ogene, F. (2025). Cybersecurity and IT governance challenges in Nigeria: Strategic investment needs and the path forward for a resilient digital economy. International Journal of Computer Applications, 178(12), 34–42.

Okoru, A. O., &Oluku, O. (2024). Cybercrime, crime security and national development in Nigeria. FUOYE Journal of Criminology and Security Studies, 3(2), 88–102.

Olalekan, O. (2025). *Nigeria Faces Rising Cybersecurity Threats in 2025: CSEAN Report Warns of Crypto Scams and AI-Powered Attacks*. Fintech Magazine Africa.

Oliobi, E. O., Bassey, S. I., Chaku, E., &Aimufua, G. I. O. (2026). *Evaluating the challenges of cybersecurity policy implementation in Nigeria*. SEAHI Publications.

Opesade, A. O., &Adetona, A. O. (2021). An assessment of internet use and cyber-risk prevalence among students in selected Nigerian secondary schools. Journal of Cybersecurity Education, Research and Practice, 2020(2), Article 3.

Pulse Nigeria. (2025, August 12). *Nigeria faces most cyber attacks globally as Africa becomes hackers' top target*. Retrieved from https://www.pulse.ng/news/local/nigeria-faces-most-cyber-attacks-globally-as-africa-becomes-hackers-top-target/6z9c9xg

Sibe, R. T., &Kaunert, C. (2024). Cybercrime and Digital Forensic Readiness in Nigeria: A Conceptual and Theoretical Framework.*International Journal of Cybersecurity Studies*.

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The "Yahoo Plus" phenomenon. *Journal of Financial Crime*, *20*(4), 445–459.

ThisDay. (2025, April 14). Youth, unemployment, and cybercrime: The Nigerian dilemma. *ThisDay Newspaper*. Retrieved from https://www.thisdaylive.com

Tijani, H. O., & Adams, K. (2024). Impact of cybercrime on national security in Nigeria. Journal of Cybersecurity and National Development, 6(2), 112–130.

Ukhami, S. M., & Abdulsalam, A. O. (2024). Cybersecurity Challenges in Nigeria: Threat Landscape, Economic Impact, and Strategic Solutions. *Zenodo*.

Uwakwe, A., & Oji, J. O. (2021). Socioeconomic roots of cybercrime in Nigeria: A contextual analysis. *Nigerian Journal of Sociology, 13*(1), 71–86.

Uzochukwu, C. E., & Nwankwo, M. O. (2020). Youth unemployment and cybercrime in Nigeria: A critical analysis. *Journal of Economic and Social Research, 7*(2), 89–104.

Waminaje, Y. Z., & Garba, D. (2025). An institutional analysis of Nigeria's foreign policy response to cybersecurity. Open Research Africa.

Yar, M. (2020). *Cybercrime and Society* (2nd ed.). London: SAGE Publications.