

An Assessment of the Effectiveness of Cybersecurity Policies in Nigeria: Implications for Community Security

By

Ladi Kunoba Aduwak

Apudi Institute for Peace and Social Rehabilitation, an Affiliate of Nasarawa State University, Keffi,
Nasarawa State, Nigeria

ladi4c@gmail.com

Abstract

This study assessed the effectiveness of cybersecurity policies in Nigeria and their implications for community security. It examined how Nigeria's cybersecurity policy and legal frameworks contribute to cybercrime prevention, data protection, digital trust, and community safety. The study was anchored on Socio-Technical Systems Theory and Routine Activity Theory. A descriptive survey design was adopted, with a population of 2,000 personnel of the Ministry of Foreign Affairs, Abuja. Using the Krejcie and Morgan sample-size table, 322 respondents were selected through multistage sampling, of which 305 completed questionnaires were found usable. Data were collected using Nigeria's Cybersecurity Policies and Community Security Questionnaire (NCPCS-Q), which had a reliability coefficient of 0.84 (Cronbach's alpha). Data were analysed using the mean, standard deviation, and an independent-samples t-test. Findings revealed a generally low perception of cybersecurity policy effectiveness, with an overall mean of 1.86 (SD = 0.79), below the criterion mean of 2.50. The independent-samples t-test showed no statistically significant difference between male and female respondents' perceptions of cybersecurity policy effectiveness, $t(303) = 0.655$, $p = .513$. The null hypothesis was therefore retained. The study concludes that the principal challenge lies in translating cybersecurity policy formulation into effective implementation and community-level protection. It recommends stronger inter-agency coordination, improved institutional and technical capacity, sustained cybersecurity awareness and digital-literacy programmes, transparent enforcement, and community-oriented cybersecurity governance.

Interpret the findings within the study's institutional scope. Because the respondents were drawn from one federal ministry in Abuja, the results indicate informed institutional perceptions rather than a nationally representative measure of community experience. Future studies should use multi-institutional and community-based samples across Nigeria's geopolitical zones.

Keywords: Cybersecurity Policies, Community Security, Cybercrime Prevention

Introduction

We live in an increasingly interconnected world where technology influences virtually every aspect of human life. The rapid advancement of digital systems, the proliferation of the internet, and the growing reliance on online platforms have transformed how individuals, governments, and organisations operate. While this digital transformation offers immense opportunities for growth, communication, and innovation, it also introduces complex challenges, particularly in cybersecurity. The International Telecommunication Union (ITU, 2021) notes that the rapid uptake of information and communication technologies and growing dependence on digital solutions have made cybersecurity increasingly important for securing digital ecosystems and building user confidence. As cyber threats continue to evolve in scale and sophistication, protecting digital infrastructure, personal data, and national assets has therefore become a critical priority for governments and organisations worldwide.

In Nigeria, the adoption of digital technologies has accelerated in recent years, driven by expanding internet access, mobile connectivity, and the increasing use of digital platforms for business, government services, and financial transactions. However, this digital transformation has also increased

exposure to cybersecurity risks and cybercrime. Kovács (2022) observes that the growing use of the internet and digital technologies in Nigeria has created new opportunities for communication, commerce, and institutional activities while simultaneously increasing exposure to cybercrime and other digital threats. Cyberattacks can therefore threaten economic stability, undermine public trust, and adversely affect national and community security. Recognising these risks, the Nigerian government has developed cybersecurity policies and legal frameworks, including the National Cybersecurity Policy and Strategy, to strengthen cybersecurity governance and promote a safer digital environment.

Despite these policy efforts, the effectiveness of Nigeria's cybersecurity policies for community security remains a subject of concern. Osimen et al. (2025) found that implementation failures and infrastructural deficits continue to affect the practical operation of Nigeria's cybersecurity framework. They also raised concerns about how cybersecurity measures are implemented and their implications for citizens' digital rights, privacy, freedom of expression, and internet access. Consequently, communities remain vulnerable to cybercrimes that can destabilise local economies, disrupt social order, and erode trust among citizens. Cyber insecurity affects not only individuals and institutions but also community security and national cohesion (Abubakar & Ijeoma, 2024).

This study, therefore, assesses the effectiveness of cybersecurity policies in Nigeria and examines their implications for community security. It seeks to identify the strengths and weaknesses of existing policies, evaluate their impact on mitigating cyber threats, and propose strategic measures to enhance cybersecurity governance. By exploring the link between cyber resilience and community safety, the study aims to contribute to a more secure, inclusive, and resilient digital environment in Nigeria.

Statement of the Problem

Nigeria's rapid adoption of internet services, electronic banking, e-commerce, social media, and digital public services has improved social and economic activities but has also increased exposure to cyber threats. Online fraud, ransomware, business email compromise, identity theft, data breaches, and other cybercrimes cause financial losses, privacy violations, disruption of essential services, and declining public confidence in digital systems. In response, the Federal Government introduced the National Cybersecurity Policy and Strategy (NCPS) 2021 to strengthen cybersecurity governance, institutional capacity, incident response, public awareness, and the protection of citizens and critical infrastructure (Federal Republic of Nigeria, 2021).

However, the continued growth and changing nature of cyber threats raise concerns about these policies' effectiveness. The INTERPOL Africa Cyberthreat Assessment Report identified online scams, ransomware, business email compromise, and digital sextortion as major threats across Africa. It also reported persistent weaknesses in law-enforcement capacity, technical training, cybercrime infrastructure, resources, and international cooperation (INTERPOL, 2025). These challenges suggest that cybersecurity laws and policies have not necessarily resulted in effective protection for individuals, organisations, and communities.

The central problem is therefore the gap between cybersecurity policy formulation and practical implementation. Although Nigeria has strengthened its legal framework through the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 and the Nigeria Data Protection Act 2023, questions remain concerning enforcement, institutional coordination, funding, technical capacity, public awareness, and incident-response mechanisms. Previous studies have similarly identified weaknesses in the workability and implementation of Nigeria's cybersecurity policy framework (Okaphor & Ezeama, 2023).

Cybersecurity enforcement also raises concerns about privacy, data protection, freedom of expression, and public trust. Effective cybersecurity policies must protect citizens from cybercrime without

undermining their fundamental digital rights. Recent studies have therefore emphasised the need to balance national cybersecurity objectives with privacy and constitutional protections (Obidiegwu, 2024).

These challenges have direct implications for community security. Weak policy implementation, limited cybersecurity awareness, poor reporting systems, inadequate institutional collaboration, and insufficient protection of personal data leave communities vulnerable to financial exploitation, identity theft, misinformation, and service disruption. Nevertheless, limited empirical research has examined the relationship between Nigeria's cybersecurity policies and community-level security outcomes (Oliobi et al., 2026).

This study therefore assesses the effectiveness of cybersecurity policies in Nigeria. It examines their implications for community security to address the persistent gap between cybersecurity policy formulation and its translation into measurable improvements in community security.

Research Objectives

The study sought to:

- i. assess respondents' perceptions of the effectiveness of cybersecurity policies in Nigeria in relation to community security;
- ii. examine perceived effectiveness across policy enforcement, institutional coordination, data protection, digital trust, and community-security outcomes; and
- iii. determine whether male and female respondents differ significantly in their perceptions of cybersecurity policy effectiveness.

Research Questions

- i. To what extent do respondents perceive cybersecurity policies in Nigeria as effective in promoting community security?
- ii. Which dimensions of cybersecurity policy implementation are perceived as most constrained?

Hypothesis

H₀₁ : There is no statistically significant difference between male and female respondents in their perceptions of the effectiveness of cybersecurity policies in Nigeria and their implications for community security.

Hypothesis

H₀₁ : There is no statistically significant difference between male and female respondents in their perceptions of the effectiveness of cybersecurity policies in Nigeria and their implications for community security.

Conceptual Review

Cybersecurity

Due to the digitalisation of the world system, cybersecurity has become a fundamental pillar of global security, governance, and socio-economic development. It is no longer just a technical concern for IT professionals but a critical necessity for individuals, organisations, and nations operating in the digital space. The International Telecommunication Union (ITU, 2020) defines cybersecurity as the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, and technologies used to protect cyberspace, users, and underlying infrastructure from cyber threats. The National Institute of Standards and Technology (NIST) provides a comprehensive framework for managing cybersecurity risks and achieving desired cybersecurity outcomes across organisations (Pascoe et al., 2024).

Cybersecurity therefore encompasses more than technical defences; it involves governance, risk management, organisational processes, human awareness, data protection, and responsive measures to manage cyber threats. Pascoe et al. (2024), through the NIST Cybersecurity Framework 2.0, identify six core functions, namely Govern, Identify, Protect, Detect, Respond, and Recover, which provide an integrated approach to managing cybersecurity risks. The framework also addresses cybersecurity governance, risk management, identity management, access control, awareness and training, data security, incident response, and recovery.

Cybersecurity also includes several specialised areas, such as application security, which protects software and apps from vulnerabilities; cloud security, which safeguards data stored on online servers; and endpoint security, which focuses on securing devices like laptops and smartphones. Other forms include internet security, which protects online communication; infrastructure security, which protects systems such as power grids and financial networks; and information security, which ensures data confidentiality and integrity. Cyber forensics and ethical hacking also help detect, investigate, and prevent cybercrimes.

The rise of digital transformation and increased internet penetration in Nigeria has heightened the need for robust cybersecurity frameworks. The country faces cyber-related risks including online fraud, data breaches, ransomware, identity theft, and other forms of digital abuse that can affect economic and community security. Nigeria's response is anchored in the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024, the National Cybersecurity Policy and Strategy 2021, and the Nigeria Data Protection Act 2023, which together address cybercrime, national cybersecurity governance, and the protection of personal data.

The importance of cybersecurity extends beyond national defence; it is integral to community security and individual well-being. By safeguarding digital systems, communities can prevent cybercrimes that disrupt social order, spread misinformation, or compromise privacy. Effective cybersecurity fosters resilience, trust, and stability, which are qualities essential for sustainable development in an increasingly digital world. Thus, cybersecurity serves not only as a technological safeguard but also as a cornerstone for national progress and community safety.

Concept of Community Security

Community security refers to protecting the well-being of individuals and groups within a community, ensuring people live in safety, dignity, and harmony. It emphasises that security extends beyond military or state protection to encompass human and social dimensions. Akinola and Paul (2022) argue that community security is a bottom-up approach that empowers local communities to identify and address threats to their peace, safety, and development. Caballero-Anthony (2015) identifies community security as a key dimension of human security and argues that it concerns the security of particular groups and communities, particularly those vulnerable to insecurity, exclusion, violence, and inadequate protection. She further emphasises that gaps in human development, security, and democratic governance can hinder progress in community security.

Community security is rooted in the principle of human security, which prioritises the safety and well-being of individuals and communities rather than focusing exclusively on state protection. Caballero-Anthony (2015) identifies community security as an important dimension of human security and explains that its advancement is closely connected to human development, security, and democratic governance. From this perspective, community security involves protecting communities from threats that undermine their social cohesion, identity, safety, and well-being. It therefore requires approaches that strengthen social inclusion, collective resilience, effective governance, and the capacity of communities and institutions to respond to threats.

In the Nigerian context, community security plays a vital role in addressing challenges such as insurgency, banditry, farmer-herder conflict, communal clashes, and cybercrime. Oke et al. (2021) argue that community participation in security provision can strengthen Nigeria's security architecture by improving cooperation between citizens and security agencies and enhancing intelligence gathering to prevent and manage insecurity. They emphasise that effective community-based security requires stronger collaboration between security institutions and the communities they serve. Consequently, strengthening community security requires the active participation of local communities alongside formal security agencies and other relevant stakeholders.

Effective community security promotes unity, peaceful coexistence, and sustainable development. It ensures that citizens actively participate in protecting their environment and supporting peace initiatives. By integrating technology, civic education, and local collaboration, community security becomes a cornerstone for national stability and resilience in an increasingly interconnected world.

Cybersecurity Policies in Nigeria

Nigeria has developed several cybersecurity policies and regulatory frameworks to protect its digital ecosystem and secure individuals, organisations, and national infrastructure. These policies aim to combat cybercrime, protect personal data, and enhance national cyber resilience. They include the Cybercrimes Act of 2015 (amended in 2024), the Nigeria Data Protection Regulation (NDPR) of 2019, the National Cybersecurity Policy and Strategy (NCPS) 2021, and the Central Bank of Nigeria (CBN) Cybersecurity Guidelines for financial institutions.

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, provides a central legal framework for preventing, prosecuting, and responding to cybercrime in Nigeria. The 2024 amendment updated institutional, enforcement, and financing provisions and strengthened the coordination framework for relevant security, intelligence, law-enforcement, and military services. The Act therefore provides an important statutory foundation for cybercrime prevention and national cybersecurity governance, although its effectiveness depends on institutional capacity, coordination, technical expertise, and rights-sensitive enforcement.

A major strength of the Act is that it provides a statutory basis for investigating and prosecuting cybercrime and for coordinating relevant institutions. However, legal powers alone do not guarantee effective community security. Implementation may be constrained by limited technical capacity, resource gaps, institutional overlap, low public awareness, and concerns about privacy and rights. Consequently, the effectiveness of the amended Act should be assessed not only by the existence of legal provisions but also by how consistently those provisions are implemented and translated into practical protection for citizens and communities.

The Nigeria Data Protection Act (NDPA) 2023 is now the principal statutory framework for personal data protection in Nigeria. The Act established the Nigeria Data Protection Commission (NDPC) and provides for regulating personal-data processing, protecting data-subject rights, and promoting accountable data-governance practices. The Act is directly relevant to community security because misuse, loss, or unauthorised processing of personal data can undermine privacy, trust, and citizens' willingness to participate safely in digital systems. The earlier Nigeria Data Protection Regulation (NDPR) 2019 remains relevant to the development of Nigeria's data-protection regime. However, it should not be presented as the current principal statute after the enactment of the NDPA 2023.

The National Cybersecurity Policy and Strategy (NCPS) 2021, developed by the Office of the National Security Adviser (ONSA), provides a strategic roadmap for protecting critical national infrastructure, promoting cybersecurity education, and enhancing collaboration between public and private stakeholders (ONSA, 2021). The framework emphasises resilience, information sharing, and

coordinated incident response. Its strength lies in its holistic, multi-stakeholder approach; however, insufficient funding, poor inter-agency coordination, and lack of real-time intelligence sharing have limited its operational effectiveness.

The CBN Cybersecurity Guidelines complement these efforts by establishing robust standards for the financial sector. Banks must implement multi-factor authentication, conduct annual penetration testing, and appoint Chief Information Security Officers (CISOs) to oversee cyber risk management (Adam, 2024). These measures have strengthened Nigeria's financial institutions' resilience against cyberattacks. Still, challenges persist in compliance monitoring and in integrating cybersecurity awareness among bank staff.

Overall, Nigeria's cybersecurity policies demonstrate significant progress in creating a structured and responsive digital security framework. However, implementation gaps, limited awareness, and inadequate coordination remain persistent weaknesses. While the Cybercrimes Act and NDPR have strengthened deterrence and data protection, overregulation and enforcement challenges risk undermining public trust. To improve policy effectiveness, Nigeria needs capacity building, transparent enforcement mechanisms, and public-private partnerships that promote innovation alongside security. Strengthening these areas will ensure that Nigeria's cybersecurity policies not only mitigate threats but also contribute to sustainable digital and community security.

Factors Hindering the Effectiveness of Cybersecurity Policies for Community Security

Despite Nigeria's progress in developing cybersecurity policies, several challenges continue to undermine their effectiveness in ensuring community security and digital resilience. A major hindrance is citizens' lack of awareness and digital literacy. According to Adebayo and Okonkwo (2022), many Nigerians, especially in rural areas, remain unaware of cybersecurity risks, best practices, and the implications of data breaches. This knowledge gap leaves individuals and small businesses vulnerable to phishing, online scams, and misinformation. When the populace lacks digital literacy, the goals of cybersecurity policies, such as prevention, protection, and public participation, remain unachieved.

Another significant barrier is weak institutional capacity and enforcement mechanisms. Musa et al. (2026) found that Nigerian law-enforcement agencies face challenges including inadequate technological infrastructure, insufficient skilled personnel, weak information-sharing mechanisms, institutional rivalries, and bureaucratic inefficiencies in combating cybercrime. These limitations can undermine the effective implementation of cybersecurity policies, weaken monitoring and investigation, and reduce the capacity of relevant institutions to respond promptly to cyber offences. Consequently, strengthening institutional resources, specialised technical skills, inter-agency cooperation, and operational capacity is essential for improving cybersecurity governance and public confidence in Nigeria.

Lack of inter-agency collaboration and information sharing also weakens the effectiveness of cybersecurity policies. Musa, Yelwa, and Malumfashi (2026) found that although collaborative frameworks exist among Nigerian law-enforcement agencies, institutional silos, jurisdictional overlaps, inadequate technological infrastructure, limited skilled personnel, and weak information-sharing protocols constrain their effectiveness. This lack of effective synergy makes it harder for relevant institutions to detect, investigate, track, and respond promptly to cyber threats affecting individuals, communities, and national systems.

Furthermore, rapid technological evolution remains a major challenge. The emergence of artificial intelligence (AI)-driven scams, ransomware, and deepfake technologies has outpaced the current legal and policy frameworks (Chukwuma & Adeyemi, 2024). Consequently, cybersecurity policies struggle to adapt and respond to new forms of digital crime.

Legal ambiguities and public distrust further undermine the system. Overlapping mandates between regulatory agencies and inconsistent interpretations of the law create confusion and hinder accountability. In addition, public scepticism about government surveillance and data misuse discourages citizens from reporting cyber incidents or cooperating with authorities (Akinola & Paul, 2022).

Strategic Measures to Enhance Cybersecurity Policies for Community Security

Enhancing the effectiveness of cybersecurity policies for community security in Nigeria requires a comprehensive and strategic approach that integrates policy reform, institutional strengthening, technological innovation, and community participation. To ensure that cybersecurity initiatives translate into tangible protection and trust at the grassroots level, both government and private stakeholders must collaborate to create an inclusive, secure, and resilient digital environment.

A key strategy is improving cybersecurity awareness and digital literacy among citizens. According to Adebayo and Okonkwo (2022), promoting public education on safe online practices and data protection is vital for reducing cyber vulnerabilities. Incorporating cybersecurity education into school curricula and community training programs will empower individuals and small businesses to identify threats such as phishing, identity theft, and cyberbullying. Public campaigns, media outreach, and partnerships with civil society organisations can also enhance collective vigilance and foster a security-conscious culture.

Another critical measure involves strengthening institutional capacity and inter-agency collaboration. Musa et al. (2026) found that although collaborative mechanisms exist among Nigerian law-enforcement agencies, inadequate technological infrastructure, limited skilled personnel, weak information-sharing protocols, institutional rivalries, and bureaucratic inefficiencies constrain their effectiveness. Strengthening data-sharing mechanisms, improving technical and human capacity, and fostering greater cooperation among cybersecurity agencies, private-sector organisations, and academic institutions can therefore enhance policy implementation and incident response.

Additionally, updating and harmonising legal and regulatory frameworks is essential. Existing policies, such as the Cybercrimes Act, should be regularly reviewed to address emerging threats from artificial intelligence, ransomware, deepfakes, and digital espionage (Chukwuma & Adeyemi, 2024). Clearer mandates and coordination among regulatory bodies will also prevent overlaps and strengthen accountability in cybersecurity governance.

Furthermore, communities should be encouraged to lead cybersecurity initiatives. Local communities can serve as early warning systems through digital neighbourhood watch programs, reporting mechanisms, and community-based cyber awareness clubs. Integrating traditional leaders, youth groups, and local organisations into cybersecurity programs will deepen trust and participation.

Moreover, international cooperation and technology investment are vital for long-term resilience. Collaborating with global cybersecurity organisations, investing in research, and adopting advanced technologies such as threat intelligence systems can help Nigeria stay ahead of evolving cyber threats. By adopting these measures, Nigeria can strengthen its cybersecurity framework and enhance community security in the digital era.

Theoretical Framework

Socio-Technical Systems Theory (Trist & Bamforth, 1951)

The Socio-Technical Systems Theory, associated with the early work of Trist and Bamforth (1951), posits that a system's performance and stability depend on the harmonious interaction between its social and technical components. This theory emphasises that technology and human factors must function

cohesively to achieve optimal outcomes. In the context of cybersecurity and community security, the theory suggests that technological defences such as firewalls, encryption, and intrusion detection systems are only effective when complemented by human awareness, ethical conduct, and institutional collaboration. According to Adeyemi and Bello (2023), Nigeria's cybersecurity framework requires not just advanced infrastructure but also public education, stakeholder cooperation, and community participation to mitigate digital threats effectively. Thus, the Socio-Technical Systems Theory provides a foundation for understanding how integrating technological solutions with human and organisational elements can enhance cybersecurity resilience within communities.

Routine Activity Theory (Cohen & Felson, 1979)

Cohen and Felson's Routine Activity Theory (1979) explains that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. Applied to cybersecurity, the theory suggests that cybercrimes thrive when users lack adequate protection or awareness, and when digital guardianship mechanisms (such as monitoring systems, regulations, or enforcement agencies) are weak. This framework is relevant to Nigeria's digital environment, where low cybersecurity literacy, poor enforcement, and limited technical capacity increase vulnerability to online crimes. As Chukwuma and Adeyemi (2024) note, strengthening institutional guardianship through robust cybersecurity policies and active citizen engagement can reduce cyber threats that endanger community security. Therefore, the Routine Activity Theory helps explain the dynamics of digital victimisation and emphasises the need for preventive strategies and institutional vigilance.

Methodology

Research Design

The study adopted a descriptive research design, which was appropriate because it examined perceptions of policy effectiveness, institutional implementation, data protection, public awareness, and community security, and required interpretation of the policy environment in which cybersecurity measures operate.

Population of the Study, Sample Size and Sampling Technique

Population of the Study

The study population consisted of 2,000 personnel of the Ministry of Foreign Affairs, Abuja, Nigeria. The personnel include diplomats, foreign service officers, policy analysts, protocol officers, research officers, and administrative staff. The Ministry was selected as the study setting because its personnel operate within a federal institution that engages with national policy, international cooperation, and security-related issues, including emerging digital and transnational threats.

Sample Size and Sampling Technique

The sample size was 322 personnel, determined using the Krejcie and Morgan (1970) sample-size determination table for a known population of 2,000. A multistage sampling technique was adopted. First, the Ministry of Foreign Affairs was purposively selected as the focal institution. Second, personnel were stratified into relevant professional categories to ensure representation of different functional groups. Third, proportional allocation determined the number of respondents selected from each stratum. Finally, the researchers used simple random sampling within each stratum to select respondents. Of the 322 questionnaires administered, 305 were properly completed and found usable for the analysis, representing the valid-response base for the reported tables.

The empirical component of the study is therefore institution-specific. The findings represent the perceptions of sampled Ministry of Foreign Affairs personnel and should not be interpreted as a nationally representative assessment of all Nigerian citizens or communities. The Ministry was selected because its personnel engage with national policy, international cooperation, diplomacy, and transnational security issues; nevertheless, the restricted institutional setting limits the generalisability of the findings.

Method of Data Collection

The primary data collection instrument was a structured questionnaire titled Nigeria's Cybersecurity Policies and Community Security Questionnaire (NCPSC-Q). The questionnaire comprised two sections. Section A captured respondents' demographic and professional characteristics, while Section B contained 25 substantive items organised around the study's research questions, including cybersecurity policy development, institutional coordination, data protection, cybercrime prevention, public awareness, and community-security outcomes. Responses were measured on a four-point Likert scale: Strongly Agree (4), Agree (3), Disagree (2), and Strongly Disagree (1). The questionnaire was administered face-to-face with the assistance of trained research assistants.

Relevant policy and regulatory documents, including the National Cybersecurity Policy and Strategy 2021, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024, and the Nigeria Data Protection Act 2023, also provided documentary context for interpreting the survey findings.

Validity and Reliability of the Instrument

Experts in Political Science, International Relations, and cybersecurity-related fields conducted face and content validation of the questionnaire. Their comments improved the clarity, relevance, coverage, and consistency of the items before final administration. A pilot test was conducted with 40 respondents with characteristics similar to those of the study population but excluded from the final sample. Cronbach's alpha was 0.84, indicating satisfactory internal consistency.

Ethical Considerations

Participation was voluntary. Respondents were informed of the study's purpose and could decline participation or withdraw without penalty. No unnecessary personal identifiers were collected, and completed questionnaires were treated confidentially and used solely for academic purposes. Findings were reported in aggregate so individual respondents could not be identified.

Techniques for Data Analysis

The questionnaire data were analysed using descriptive and inferential statistical techniques. Frequencies and percentages summarised respondents' characteristics, while mean scores and standard deviations were used to answer the research questions. For the four-point Likert scale, a criterion mean of 2.50 was adopted. An independent-samples t-test was used to test the stated hypothesis at the 0.05 level of significance and to determine whether statistically significant differences existed between relevant respondent groups.

Results and Discussion

Research Question One

To what extent are cybersecurity policies effective in Nigeria, and what implications do they have for community security?

Research Question One

To what extent do respondents perceive cybersecurity policies in Nigeria as effective in promoting community security?

Table 1

Respondents' Assessment of the Effectiveness of Cybersecurity Policies and Their Implications for Community Security

(N=305)

S/N	Items	SA 4	A 3	D 2	SD 1	Sum	Mean	SD	Decision
1	Nigeria's cybersecurity policy responses have improved community security.	15	35	150	105	570	1.87	0.79	Disagreed
2	Enforcement of cybercrime policies has helped reduce cyber threats.	12	30	158	105	559	1.83	0.76	Disagreed
3	Data-protection measures have enhanced citizens' digital safety and trust.	20	45	145	95	600	1.97	0.83	Disagreed
4	Coordination among cybersecurity institutions is effective.	10	25	140	130	525	1.72	0.75	Disagreed
5	Nigeria's cybersecurity efforts have benefited from national and international support.	18	40	147	100	586	1.92	0.81	Disagreed
	Average mean/SD						1.86	0.79	Disagreed

Source: Field Survey, 2026

Table 1 shows that all five items recorded mean scores below the criterion mean of 2.50. The overall mean of 1.86 (SD = 0.79) indicates disagreement that Nigeria's cybersecurity policy responses have translated into effective community-security outcomes. Respondents particularly disagreed that

coordination among cybersecurity institutions is effective ($M = 1.72$) and that policy enforcement has reduced cyber threats ($M = 1.83$). This pattern suggests that policy formulation has not been matched by sufficiently strong implementation, coordination, and community-level awareness.

Test of Hypothesis

H_{01} : There is no statistically significant difference between male and female respondents in their perceptions of the effectiveness of cybersecurity policies in Nigeria and its implications for community security.

Table 2

Independent-Samples t-Test on Perceptions of Cybersecurity Policy Effectiveness Outcomes by Gender (N = 305)

Gender	N	Mean	SD	t	df	p	Decision
Male	171	1.89	0.81	0.655	303	.513	Retain H_0
Female	134	1.83	0.76				

Source: Field Survey, 2026

The results in Table 2 indicate no statistically significant difference between male and female respondents in their perceptions of cybersecurity policy outcomes, $t(303) = 0.655$, $p = .513$. Since $p > .05$, the null hypothesis was retained. The result indicates that the evidence was insufficient to conclude that gender was associated with differences in perceptions of cybersecurity policy effectiveness among the sampled respondents.

Discussion of Findings

The study found that respondents perceived Nigeria's cybersecurity policies as generally ineffective in producing community-security outcomes. Table 1 recorded an overall mean of 1.86 ($SD = 0.79$), below the criterion mean of 2.50, with all five items receiving low ratings. Respondents particularly rated institutional coordination ($M = 1.72$), policy enforcement ($M = 1.83$), improved community security ($M = 1.87$), national and international support ($M = 1.92$), and data protection and digital trust ($M = 1.97$) below the acceptable level. These results suggest that Nigeria's major challenge is not the absence of cybersecurity laws, but the gap between policy formulation and effective implementation.

Although instruments such as the National Cybersecurity Policy and Strategy 2021, the Cybercrimes Act, and the Nigeria Data Protection Act 2023 provide important legal foundations, respondents did not perceive them as sufficiently translated into practical protection for communities. This finding agrees with Oliobi et al. (2026) and Enokie (2025), who identified weak enforcement, limited institutional capacity, inadequate public awareness, and unclear implementation mechanisms as continuing challenges. The particularly low rating for institutional coordination indicates that fragmented responsibilities and limited information sharing may weaken the prevention, detection, and response to cyber threats. Similarly, the low assessment of data protection suggests that existing legal provisions have not yet generated adequate public trust in digital services.

This finding aligns with Socio-Technical Systems Theory, which emphasises the interaction of technology, institutions, and human behaviour, and Routine Activity Theory, which highlights the importance of effective guardianship. Thus, cybersecurity cannot depend solely on legislation or technology; it also requires capable institutions, informed citizens, coordinated enforcement, and accessible reporting mechanisms.

Table 2 further shows no significant gender difference in perceptions of cybersecurity policy effectiveness. Male respondents recorded a mean of 1.89, compared with 1.83 for females, with $t(303) = 0.655$ and $p = 0.513$. Since $p > 0.05$, the null hypothesis is retained under the revised interpretation that male and female respondents do not differ significantly in their assessments. However, this test does not directly establish a relationship between policy effectiveness and community security. Overall, the findings indicate that Nigeria needs stronger coordination, enforcement, public awareness, data protection, and community-focused implementation.

Conclusion

This study examined the relationship between cybersecurity policies and community security in Nigeria, with emphasis on the effectiveness of policy and legal measures in reducing cyber risks and promoting safe digital participation. The study recognises the progress represented by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024, the National Cybersecurity Policy and Strategy 2021, and the Nigeria Data Protection Act 2023. However, the empirical results indicate that these frameworks have not automatically translated into strong community-level perceptions of effectiveness. The study's theoretical framework, Socio-Technical Systems Theory and Routine Activity Theory, shows that cybersecurity effectiveness depends on the interaction of technology, capable guardianship, institutional coordination, public behaviour, and protection of human well-being. The findings therefore support a shift from policy formulation alone toward measurable implementation, stronger coordination, sustained digital literacy, transparent enforcement, and community-oriented cybersecurity governance.

Recommendations

- i. Enhance Public Awareness and Digital Literacy: Launch continuous cybersecurity awareness and digital-literacy programmes targeting youths, businesses, and local communities. This will help individuals recognise online threats, adopt safe digital practices, protect personal data, and contribute to community security.
- ii. Strengthen Institutional and Technical Capacity: Increase funding, specialised training, and technological support for cybersecurity and law-enforcement institutions. Improved capacity will strengthen threat detection, policy implementation, incident response, and enforcement of the Cybercrimes Act as amended in 2024.
- iii. Foster Collaborative Cybersecurity Governance: Establish a multi-stakeholder coordination framework involving government institutions, private-sector organisations, academia, civil society, and community groups. This should improve information sharing, reduce institutional fragmentation, and translate national cybersecurity policy into community-level protection.
- iv. Strengthen Data Protection, Reporting, and Rights-Sensitive Enforcement: Improve accessible cyber-incident reporting channels, strengthen compliance with the Nigeria Data Protection Act 2023, and ensure that enforcement measures are transparent, proportionate, and respectful of privacy and other digital rights.
- v. Institutionalise Community-Oriented Cybersecurity Programmes: Develop partnerships with local governments, schools, professional bodies, youth organisations, traditional institutions, and civil-society groups to deliver community-level cyber-awareness, early-warning, referral, and victim-support initiatives.
- vi. Broaden Future Evaluation and Research: Periodically evaluate cybersecurity policy implementation using multi-institutional and community-based samples across Nigeria to generate more nationally representative evidence on policy outcomes.

References

- Adebayo, T., & Okonkwo, C. (2022). Cybersecurity awareness and digital literacy in Nigeria: A pathway to digital safety. *Journal of Information Security and Digital Development*, 8(2), 45–58.
- Adeyemi, M. A., & Bello, T. A. (2023). Cybersecurity in Nigerian academic institutions: Challenges and prospects. *Nigerian Journal of Information Security*, 12(1), 45–57.
- Akinola, B., & Paul, D. (2022). Public perception and trust in Nigeria's cybersecurity governance. *African Journal of Security and Development*, 8(1), 72–86.
- Caballero-Anthony, M. (2015). Community security: Human security at 21\ . *Contemporary Politics*, 21(1), 53–69.
- Chukwuma, E., & Adeyemi, R. (2024). Emerging technologies and cybersecurity challenges in Nigeria. *Journal of ICT and Society*, 12(3), 114–129.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- Federal Republic of Nigeria. (2021). National cybersecurity policy and strategy 2021. Office of the National Security Adviser.
- International Telecommunication Union. (2020). Global cybersecurity agenda. International Telecommunication Union.
- International Telecommunication Union. (2021). Global cybersecurity index 2020. International Telecommunication Union.
- INTERPOL. (2025). Africa cyberthreat assessment report 2025. International Criminal Police Organisation.
- Kovács, A. M. (2022). Here there be dragons: Evolution, potentials and mitigation opportunities of cybercrime in Nigeria: A review, analysis, and evaluation. *Journal of Central and Eastern European African Studies*, 2(1), 68–81.
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607–610.
- Musa, A., Yelwa, M. M., & Malumfashi, A. L. (2026). Assessment of the collaborative efforts among law enforcement agencies in combating cybercrime in Nigeria. *Abuja Journal of Sociological Studies*, 5(4).
- Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. Federal Republic of Nigeria.
- Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act, 2023.
- Obidiegwu, I. (2024). Throwing the baby out with the bath water? Privacy concerns under the cybersecurity regime in Nigeria. SSRN.
- Oke, C. I. A., Braimah, F., & Masajuwa, F. U. (2021). Policing through the community in Nigeria: The missing link in security architecture. *Ikenga International Journal of Institute of African Studies*, 22(2), 146–169.
- Okaphor, E. F., & Ezeama, C. (2023). Appraising the workability of the National Cyber Security Policy and Strategy Document 2021. *Law and Social Justice Review*, 4(2).
- Oliobi, E. O., Bassey, S. I., Chaku, E., & Aimufua, G. I. (2026). Evaluating the challenges of cybersecurity policy implementation in Nigeria. *International Journal of Innovative Information Systems & Technology Research*, 14(1), 23–36.
- Osimen, G. U., Wonosikou, M. H., & Odeigah, T. N. (2025). National cybersecurity policy and citizens' digital rights in Nigeria. *African Human Rights Law Journal*, 25(2), 627–658.
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0. National Institute of Standards and Technology.
- Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations*, 4(1), 3–38.
- United Nations Development Programme. (1994). Human development report 1994: New dimensions of human security. Oxford University Press.