© IIJP 2026 | Volume 2, Issue 2, pp. 1525-1540 | ISSN: 2636-4484

ENVIRONMENTAL SUSTAINABILITY AND CYBERSECURITY IN NIGERIA: A SURVEY OF STAKEHOLDERS' PERCEPTIONS IN JOS METROPOLIS

***Tony Aku AMBA[1], Cleta GABA[2], Nanbil AMBA[3]**
[1]Neo-Tropical Urban Rural Environmental Resilience and Sustainable Development Initiative Jos, Plateau State,
****Corresponding Author:** revtonyakuamba@gmail.com/ORCID ID:0000-0002-81048756*
[3]Department of Mass-Communication, Plateau State Polytechnic, Plateau State

ARTICLE INFO
Article No.: 0383
Accepted Date: 28/05/2026
Published Date: 22/06/2026
Type: Research

ABSTRACT
The increasing integration of digital technologies into environmental governance has created new opportunities for achieving sustainable development while simultaneously exposing critical environmental systems to cyber threats. This study examined the nexus between environmental sustainability and cybersecurity and explored their implications for resilient sustainable development in Nigeria. Specifically, the study investigated the relationship between environmental sustainability and cybersecurity, assessed the role of cybersecurity in protecting environmental infrastructure, and examined the challenges posed by cyber threats to sustainability systems, and identified policy strategies for integrating cybersecurity into environmental governance. A descriptive survey research design was adopted, with data collected from 298 respondents selected through a stratified random sampling technique from environmental agencies, information technology organizations, renewable energy institutions, academia, and government establishments. Data were gathered using a structured five-point Likert scale questionnaire with a reliability coefficient (Cronbach's Alpha) of 0.89 and analyzed using descriptive statistics, Pearson Product Moment Correlation, and multiple regression analysis at a 5% level of significance. The findings revealed a significant positive relationship between environmental sustainability and cybersecurity ($r = 0.741$, $p < 0.05$), indicating that stronger cybersecurity measures enhance sustainable environmental management. The study also found that 82.6% of respondents agreed that cybersecurity is essential for protecting critical environmental infrastructure, while 79.2% identified cyber threats as a major challenge to environmental governance and digital sustainability initiatives. Furthermore, 87.4% supported the integration of cybersecurity policies into national environmental frameworks to improve resilience and institutional effectiveness. The study concludes that cybersecurity has become an indispensable pillar of environmental sustainability and recommends the adoption of integrated policy frameworks, increased investment in cyber-resilient infrastructure, capacity building, and strengthened institutional collaboration to promote resilient and sustainable development in an increasingly digital society.

Keywords: Environmental sustainability, cybersecurity, resilient sustainable development, digital resilience, critical infrastructure, environmental governance.

Introduction

Environmental sustainability has become one of the defining concerns of the twenty-first century due to escalating environmental challenges such as climate change, biodiversity loss, ecosystem degradation, pollution, and resource depletion. Governments, international organizations, and development institutions increasingly recognize that sustainable development requires innovative approaches capable of balancing environmental protection with economic growth and social well-being. Consequently, technological innovations have become integral to environmental management, providing new opportunities for monitoring ecosystems, improving resource efficiency, and supporting climate adaptation and mitigation strategies. Studies by Bibri *et al.,* (2023) and Achuthan *etal.,* (2025) emphasize that digital technologies are becoming indispensable tools for advancing environmental sustainability and achieving global sustainability targets. Hong and Xiao (2024) explained that the rapid advancement of digital technologies has significantly transformed environmental governance systems.

Artificial intelligence, big data analytics, cloud computing, blockchain technologies, remote sensing, and Internet of Things (IoT) devices according to Vinuesa *et al.,* (2024) now support environmental monitoring, natural resource management, renewable energy integration, and disaster risk reduction initiatives. Smart environmental systems provide real-time information that enables governments and organizations to make informed decisions regarding environmental protection and sustainable resource utilization. These technologies according to Ibekwe *et al.,* (2026) have enhanced the capacity of institutions to address complex environmental challenges while improving efficiency and accountability in environmental management. Despite the significant benefits associated with digital transformation, increasing dependence on digital infrastructure has created new vulnerabilities related to cybersecurity.

Critical environmental infrastructures such as smart grids, water treatment facilities, renewable energy systems, transportation networks, and environmental monitoring platforms rely heavily on interconnected information systems. As these systems become increasingly digitized, they become more susceptible to cyber-attacks, ransomware incidents, data manipulation, and other forms of cyber threats. Such attacks according to Obasi *et al.,* (2024) can undermine environmental sustainability efforts by disrupting critical services, compromising environmental data integrity, and weakening institutional resilience.

Recent global incidents involving cyber-attacks on critical infrastructure have demonstrated the far-reaching consequences of digital insecurity. Cyber-attacks targeting energy systems, water utilities, and industrial control systems have highlighted the potential for significant environmental, economic, and social disruptions. These incidents underscore the growing recognition that cybersecurity is not merely an information technology issue but a critical component of sustainable development and environmental governance. As environmental systems become increasingly dependent on digital technologies, Morales-Sáenz *et al.,*(2024) suggest that ensuring the security and resilience of these systems becomes essential for achieving sustainability objectives.

The convergence of environmental sustainability and cybersecurity has therefore emerged as an important area of scholarly and policy interest. Balogun (2026) increasingly argue that environmental sustainability and cybersecurity are interconnected dimensions of societal resilience. Effective environmental management requires secure digital systems, while sustainable development depends on resilient infrastructure capable of withstanding both environmental and cyber-related disruptions. Morales-Sáenz *et al.,* (2024) opined that understanding this nexus is

essential for developing integrated policies and strategies that can strengthen resilience, promote sustainability, and safeguard critical environmental assets in the digital age.

Statement of the Problem

The increasing adoption of digital technologies in environmental management has transformed the way environmental resources are monitored, managed, and protected in Jos Metropolis. Government agencies, environmental organizations, research institutions, and utility providers now rely on digital platforms, Geographic Information Systems (GIS), remote sensing technologies, environmental databases, and electronic communication systems to support environmental sustainability initiatives. While these technologies have improved environmental governance and decision-making, they have also increased the vulnerability of environmental systems to cyber threats such as data breaches, ransomware attacks, unauthorized access, and disruption of critical digital infrastructure.

In a city such as Jos, where environmental challenges including land degradation, urban expansion, waste management problems, and the legacy of mining activities require effective technological interventions, cyber vulnerabilities may undermine efforts aimed at achieving sustainable environmental management. Despite the growing dependence on digital technologies for environmental monitoring and governance, there is limited empirical evidence on how cybersecurity influences environmental sustainability within Jos Metropolis. Existing studies in Nigeria have largely focused on cybersecurity in the financial, telecommunications, and business sectors, with little attention given to its implications for environmental management. Similarly, most environmental sustainability studies in Jos have concentrated on issues such as mining impacts, waste management, biodiversity conservation, and urban environmental degradation without adequately examining the role of cybersecurity in safeguarding environmental information systems and digital infrastructure. Consequently, policymakers and environmental managers lack localized empirical data on the relationship between cybersecurity and environmental sustainability, creating a knowledge gap that may hinder effective planning and policy formulation. Furthermore, the increasing digitization of environmental governance in Jos Metropolis raises concerns about the preparedness of institutions to protect critical environmental infrastructure from cyber threats. Weak cybersecurity frameworks, inadequate technical capacity, limited awareness, and insufficient policy integration may expose environmental systems to disruptions capable of affecting environmental monitoring, resource management, and sustainable development initiatives. Given the strategic importance of environmental sustainability to the socio-economic development of Jos Metropolis, there is a need for empirical investigation into how cybersecurity contributes to environmental resilience and sustainable development outcomes. This study therefore seeks to generate primary data from relevant stakeholders in Jos Metropolis to provide evidence-based insights for strengthening cybersecurity practices, enhancing environmental governance, and promoting resilient sustainable development within the metropolis.

Aim and Objectives of the Study

The aim of this study is to assess the nexus between environmental sustainability and cybersecurity and determine their contributions to resilient sustainable development in Nigeria. To achieve the aim, the study seeks to:

i. Determine the nature and strength of the relationship between environmental sustainability and cybersecurity among selected stakeholders in Nigeria using Pearson Product Moment Correlation analysis.

ii. Assess the extent to which cybersecurity measures influence the protection and resilience of critical environmental infrastructure and sustainability initiatives using descriptive statistics and multiple regression analysis.
iii. Evaluate stakeholders' perceptions of the prevalence and impact of cyber threats on environmental governance, digital sustainability systems, and critical infrastructure using frequency distributions, percentages, mean scores, and standard deviations.
iv. Examine the effect of integrating cybersecurity policies, institutional capacity building, and cyber-resilient investments on resilient sustainable development in Nigeria using multiple regression analysis and predictive statistical models.

Research Questions

The study is guided by the following research questions:

i. What is the nature and strength of the relationship between environmental sustainability and cybersecurity among stakeholders in Nigeria?
ii. To what extent do cybersecurity measures contribute to the protection and resilience of critical environmental infrastructure and sustainability initiatives?
iii. What are the major cyber threats affecting environmental governance and sustainable development systems in Nigeria, and how are they perceived by stakeholders?
iv. To what extent do cybersecurity policy integration, institutional capacity building, and investments in cyber-resilient infrastructure influence resilient sustainable development in Nigeria?

Research Hypotheses

The following null hypotheses were tested at the 0.05 level of significance:

H_{01}: There is no statistically significant relationship between environmental sustainability and cybersecurity among stakeholders in Nigeria.
H_{02}: Cybersecurity measures do not significantly influence the protection and resilience of critical environmental infrastructure and sustainability initiatives in Nigeria.
H_{03}: Cyber threats do not have a statistically significant impact on environmental governance and sustainable development systems in Nigeria.
H_{04}: The integration of cybersecurity policies, institutional capacity building, and investments in cyber-resilient infrastructure does not significantly predict resilient sustainable development in Nigeria.

Literature Review

1 Concept of Environmental Sustainability

Environmental sustainability refers to the responsible use and management of natural resources in a manner that ensures their availability for present and future generations. The concept emerged from global concerns regarding environmental degradation, climate change, biodiversity loss, and unsustainable patterns of production and consumption. According to the United Nations Environment Programme (UNEP, 2024), environmental sustainability emphasizes maintaining ecological balance while supporting human development and economic prosperity. It involves the protection of ecosystems, conservation of biodiversity, reduction of pollution, and efficient utilization of natural resources. Contemporary scholars argue that environmental sustainability extends beyond conservation to encompass resilience, adaptation, and environmental governance. According to Purvis *et al.,* (2019), sustainability involves balancing environmental integrity with social and economic development objectives. More recent studies by Hong and Xiao, (2024) have highlighted the importance of integrating technological innovations into sustainability frameworks to improve environmental management and enhance resilience against emerging environmental

challenges. Achuthan *et al.,* (2025) in another development buttressed that the growing threat of climate change has further expanded the relevance of environmental sustainability. Rising global temperatures, extreme weather events, desertification, flooding, and declining biodiversity have intensified calls for sustainable environmental practices. The Intergovernmental Panel on Climate Change (IPCC, 2023) emphasizes that sustainability strategies are essential for mitigating greenhouse gas emissions and enhancing adaptive capacities. Environmental sustainability therefore remains central to achieving long-term development goals and safeguarding ecological systems. Recent literature also recognizes digital technologies as important enablers of environmental sustainability. Technologies such as remote sensing, artificial intelligence, geographic information systems, and environmental monitoring networks have improved environmental assessment and decision-making processes. However, the effectiveness of these technologies according to Vinuesa (2024) depends significantly on the security and resilience of the digital systems supporting them, thereby creating important links between sustainability and cybersecurity.

2. Concept of Cybersecurity

Cybersecurity refers to the protection of information systems, digital infrastructure, networks, and data from unauthorized access, cyber-attacks, theft, and disruption. The National Institute of Standards and Technology (NIST, 2024) defines cybersecurity as the practice of safeguarding digital assets through technologies, policies, procedures, and risk management frameworks designed to ensure confidentiality, integrity, and availability of information. Balogun (2026) asserted that the increasing digitalization of modern societies has elevated cybersecurity to a strategic priority for governments, organizations, and individuals. Cyber threats such as ransomware, phishing attacks, malware infections, denial-of-service attacks, and data breaches have become increasingly sophisticated and widespread. According to the International Telecommunication Union (ITU, 2024), cybercrime continues to grow globally, affecting critical infrastructure, financial systems, healthcare facilities, and government institutions. Recent studies emphasize that cybersecurity should be viewed as a multidimensional concept encompassing technical, organizational, legal, and human dimensions. Von Solms and Van Niekerk (2023) argue that effective cybersecurity requires not only technological defenses but also institutional capacity, regulatory frameworks, and public awareness. This broader perspective is particularly relevant for sectors that rely heavily on digital infrastructure, including environmental management and sustainability initiatives. The integration of cybersecurity into sustainable development discussions has gained momentum in recent years. Researchers increasingly recognize that cybersecurity is essential for protecting critical infrastructure systems that support environmental sustainability, including renewable energy networks, environmental monitoring platforms, water management systems, and smart city technologies (Morales-Sáenz et al., 2024). Consequently, cybersecurity has become a key component of societal resilience and sustainable development.

3 Digital Technologies and Environmental Governance

Environmental governance refers to the institutions, policies, and processes through which societies manage environmental resources and address environmental challenges. The emergence of digital technologies has transformed environmental governance by improving data collection, environmental monitoring, policy implementation, and stakeholder engagement. Digital tools enable governments and environmental organizations to obtain real-time information regarding environmental conditions and resource utilization (Bibri et al., 2023). Artificial intelligence, machine learning, and big data analytics have significantly enhanced environmental monitoring and predictive capabilities. These technologies facilitate the analysis of large

environmental datasets, enabling more effective management of climate risks, biodiversity conservation, and natural resource allocation. According to Vinuesa *et al.,* (2024), AI-driven environmental monitoring systems can improve the accuracy and efficiency of environmental decision-making processes. The Internet of Things has also revolutionized environmental governance by enabling continuous monitoring of environmental indicators. Sensors deployed in forests, water bodies, agricultural lands, and urban environments provide real-time information regarding environmental conditions. Such technologies support proactive responses to environmental threats and contribute to sustainable resource management. However, the interconnected nature of these systems increases their exposure to cybersecurity risks. Ibekwe *et al.,* (2026) noted that digital environmental governance systems depend heavily on secure information infrastructure. Data manipulation, cyber-attacks, and system disruptions can compromise environmental decision-making and undermine public trust in environmental institutions. Consequently, cybersecurity has become an indispensable component of effective environmental governance in the digital era.

4 Cybersecurity and Critical Environmental Infrastructure

Critical environmental infrastructure includes facilities and systems that support environmental protection, resource management, renewable energy generation, water supply, waste management, and climate resilience. These infrastructures increasingly depend on digital technologies and networked systems for their operation and management. As a result, they have become potential targets for cyber-attacks (World Economic Forum, 2024). Renewable energy systems such as smart grids, wind farms, solar energy facilities, and battery storage networks rely heavily on digital control systems. Cyber-attacks targeting these systems can disrupt electricity supply, reduce operational efficiency, and compromise climate mitigation efforts. According to the International Energy Agency (IEA, 2024), cybersecurity risks represent a growing concern for the sustainability and reliability of renewable energy infrastructure. Water management systems constitute another important area of concern. Modern water treatment facilities utilize supervisory control and data acquisition (SCADA) systems to regulate water quality and distribution. Cyber-attacks on these systems can lead to service disruptions, contamination risks, and environmental damage. Several studies have identified water infrastructure as one of the most vulnerable sectors within critical infrastructure networks (NIST, 2024). Environmental monitoring networks and climate information systems are equally vulnerable to cyber threats. Obasi et al., (2024) believes that manipulation of environmental data can affect policy decisions, climate adaptation strategies, and disaster response mechanisms. Consequently, strengthening cybersecurity within critical environmental infrastructure has become essential for ensuring environmental sustainability and societal resilience.

5 Sustainable Development, Resilience, and Digital Security

The concept of sustainable development according to Morales-Sáenz et al., (2024) emphasizes meeting present needs without compromising the ability of future generations to meet their own needs. Resilience, on the other hand, refers to the capacity of systems to absorb shocks, adapt to disturbances, and recover from disruptions. Contemporary sustainability discourse increasingly recognizes resilience as a critical component of sustainable development (United Nations, 2024). Digital security contributes significantly to resilience by protecting critical systems against cyber threats and ensuring continuity of operations. In the context of environmental sustainability, digital resilience enables environmental monitoring systems, renewable energy infrastructure, and climate adaptation technologies to function effectively despite cyber-related disruptions. Achuthan *et al.,* (2025) argues that cybersecurity should be incorporated into broader

resilience frameworks because digital vulnerabilities can undermine sustainability outcomes. The relationship between sustainability and resilience has become increasingly important as societies confront multiple interconnected risks, including climate change, environmental degradation, pandemics, and cyber threats. According to Folke *et al.,* (2023), resilient systems are characterized by their ability to adapt, transform, and maintain essential functions under conditions of uncertainty. Cybersecurity enhances these capacities by reducing digital vulnerabilities and strengthening institutional preparedness. Recent studies further emphasize that resilient sustainable development requires integrated approaches that address both environmental and digital risks simultaneously. Environmental sustainability cannot be achieved without secure digital infrastructure, while cybersecurity investments contribute to the protection of environmental assets and sustainability initiatives. Consequently, digital security has become an essential pillar of sustainable development in the contemporary world.

Theoretical Framework

This study is anchored on the Socio-Technical Systems (STS) Theory, supported by the Resilience Theory as a complementary framework. Together, these theories provide a comprehensive explanation of how cybersecurity and environmental sustainability interact to promote resilient sustainable development in an increasingly digital society.

1 Socio-Technical Systems

(STS) Theory The Socio-Technical Systems Theory was originally developed by Eric Trist and Fred Emery in the 1950s at the Tavistock Institute of Human Relations. Trist (1981) suggested that the theory posits that organizational performance depends on the effective interaction between social systems (people, institutions, policies, and organizational structures) and technical systems (technologies, infrastructure, tools, and processes). According to Baxter and Sommervile (2011), neither technological advancement nor human systems can function optimally in isolation; rather, sustainable outcomes are achieved when both dimensions are properly integrated and mutually reinforcing. Within the context of this study, environmental sustainability initiatives increasingly depend on sophisticated digital technologies such as Geographic Information Systems (GIS), remote sensing, artificial intelligence, Internet of Things (IoT) devices, smart grids, cloud computing, and environmental monitoring platforms. While these technologies enhance environmental management and resource efficiency, they also create vulnerabilities that expose environmental systems to cyber threats. The STS theory suggests that achieving environmental sustainability requires not only technological innovation but also effective cybersecurity governance, institutional coordination, skilled personnel, regulatory frameworks, and stakeholder participation. The empirical findings of this study strongly support the assumptions of the Socio-Technical Systems Theory. The significant positive correlation between environmental sustainability and cybersecurity ($r = 0.741$, $p < 0.05$) demonstrates that improvements in technological security are associated with better environmental outcomes. Similarly, the regression results indicating that cybersecurity explains a substantial proportion of environmental infrastructure resilience suggest that sustainable environmental management depends on the harmonious interaction between digital technologies and organizational systems. Therefore, the theory provides an appropriate framework for explaining why cybersecurity should be integrated into environmental governance and sustainable development planning.

2 Resilience Theory

The Resilience Theory, which has been widely advanced by scholars such as C. S. Holling (1973) explains the capacity of systems to absorb disturbances, adapt to changing conditions, and recover from disruptions while maintaining essential functions. Originally developed within

ecological studies, the theory has been extended to social, organizational, technological, and governance systems. Folk (2016) explained that it emphasizes adaptability, flexibility, learning, and preparedness as essential characteristics of sustainable systems. Applied to this study, resilience theory provides an explanation for how environmental systems and digital infrastructures can withstand cyber threats while continuing to deliver environmental services. Renewable energy facilities, climate monitoring systems, environmental databases, water management infrastructure, and smart cities increasingly operate through interconnected digital networks. Cyber-attacks on these systems can disrupt environmental governance and compromise sustainable development efforts. Therefore, resilience requires the simultaneous strengthening of ecological systems and cybersecurity capabilities to ensure continuity of operations during and after disruptions. The survey findings support the relevance of resilience theory. A majority of respondents (82.6%) agreed that cybersecurity is essential for protecting environmental infrastructure, while 87.4% supported integrating cybersecurity into environmental policies to enhance resilience. These results indicate that stakeholders perceive cybersecurity as an important mechanism for improving the adaptive capacity of environmental systems and reducing vulnerabilities to digital risks. Consequently, resilience theory provides a useful lens for understanding how cybersecurity contributes to long-term environmental sustainability.

The relevance of the Socio-Technical Systems Theory lies in its emphasis on the interaction between technological systems and social institutions in achieving organizational and developmental goals (Trist, 1981; Baxter & Sommerville, 2011). Similarly, Resilience Theory explains the capacity of environmental and technological systems to withstand disturbances and adapt to changing conditions, making it particularly relevant to understanding the role of cybersecurity in environmental sustainability (Holling, 1973; Folke, 2016). Recent studies have further demonstrated that resilient digital infrastructure and effective cybersecurity governance are essential for sustainable development and environmental management in an increasingly digital society (Xu et al., 2023; Morales-Sáenz et al., 2024; Kshetri, 2024). The integration of Socio-Technical Systems Theory and Resilience Theory provides a robust theoretical foundation for this research. While STS Theory explains the interaction between technological systems and human institutions in achieving sustainability objectives, Resilience Theory emphasizes the capacity of those integrated systems to withstand and recover from cyber disruptions. Together, the theories illustrate that environmental sustainability cannot be achieved solely through ecological interventions but must also incorporate secure digital infrastructure, effective governance, institutional preparedness, and adaptive policy frameworks. The empirical results of this study validate these theoretical assumptions. The significant correlation between cybersecurity and environmental sustainability, the substantial regression effects observed in protecting environmental infrastructure, and the overwhelming stakeholder support for policy integration collectively demonstrate that resilient sustainable development depends on both technological security and institutional resilience. The theories therefore justify the study's conclusion that cybersecurity should be recognized as a strategic pillar of environmental sustainability in Nigeria.

Methodology

This study adopted a descriptive survey research design to empirically investigate the nexus between environmental sustainability and cybersecurity and their implications for resilient sustainable development in Nigeria. The study focused on stakeholders whose professional activities intersect with environmental management, digital governance, cybersecurity, renewable energy development, and public policy implementation. The research was conducted across selected institutions in Nigeria to generate empirical evidence capable of informing policy and

practice in the emerging field of environmental cybersecurity. The target population comprised personnel from environmental protection agencies, cybersecurity organizations, information and communication technology (ICT) institutions, renewable energy companies, government ministries, academic institutions, and environmental non-governmental organizations. A stratified random sampling technique was employed to ensure adequate representation of the different stakeholder groups. Using Cochran's sample size determination formula, a sample size of 320 respondents was selected for the study. Of the questionnaires administered, 298 were correctly completed and returned, representing a response rate of 93.1%, which was considered adequate for statistical analysis and generalization of findings. The broad representation of respondents enhanced the credibility and reliability of the empirical results. Data were collected using a structured questionnaire developed on a five-point Likert scale ranging from Strongly Agree (5) to Strongly Disagree (1). The instrument contained items addressing environmental sustainability practices, cybersecurity measures, cyber threats to environmental systems, environmental infrastructure protection, and policy integration strategies. To ensure the validity of the instrument, experts in environmental management, cybersecurity, and research methodology reviewed the questionnaire for clarity, relevance, and content adequacy. A pilot study involving 30 respondents outside the sampled population was conducted to test reliability, and the instrument yielded a Cronbach's Alpha reliability coefficient of 0.89, indicating a high degree of internal consistency and suitability for data collection. Data obtained from the survey were coded and analyzed using the Statistical Package for Social Sciences (SPSS) Version 27. Descriptive statistical tools including frequencies, percentages, means, and standard deviations were used to summarize respondents' opinions and answer the research questions. Pearson Product Moment Correlation (PPMC) was employed to determine the strength and significance of the relationship between environmental sustainability and cybersecurity, while Multiple Regression Analysis was used to examine the influence of cybersecurity measures, institutional capacity, and policy integration on resilient sustainable development. All hypotheses were tested at a 5% level of significance ($p < 0.05$).

Results and Discussion

Response Rate

Table 1: Questionnaire Administration and Response Rate

Questionnaire Status	Frequency	Percentage (%)
Administered	320	100.0
Retrieved	298	93.1
Not Retrieved	22	6.9
Total	320	100.0

A total of 320 questionnaires were administered to respondents drawn from environmental agencies, cybersecurity institutions, renewable energy organizations, academia, and government establishments across Nigeria. Out of these, 298 questionnaires were properly completed and returned, representing a 93.1% response rate, while 22 questionnaires (6.9%) were either not

returned or were discarded due to incomplete responses. The high response rate indicates adequate participation and enhances the reliability and validity of the findings.

Demographic Characteristics of Respondents

Table 2: Distribution of Respondents by Sector

Sector	Frequency	Percentage (%)
Environmental Agencies	68	22.8
ICT/Cybersecurity Organizations	54	18.1
Renewable Energy Institutions	46	15.4
Government Ministries	52	17.4
Academic Institutions	49	16.4
NGOs/Development Partners	29	9.7
Total	**298**	**100.0**

The distribution indicates that respondents were drawn from diverse professional backgrounds, ensuring broad representation of stakeholders involved in environmental sustainability and cybersecurity.

Results Based on Research Objectives Objective One: Examine the Relationship between Environmental Sustainability and Cybersecurity

Table 3: Respondents' Perception of the Relationship between Environmental Sustainability and Cybersecurity (n = 298)

Statement	SA	A	U	D	SD	Mean
Cyber Security supports environmental Sustainability initiatives	136	96	24	28	14	4.05
Digital environmental systems require cyber security protection	148	89	20	27	14	4.11
Sustainable development depends on secure digital infrastructure	142	90	25	26	15	4.07
Cyber resilience enhances environmental governance	130	99	29	24	16	4.02

Grand Mean = 4.06

The grand mean of 4.06 exceeds the benchmark value of 3.00, indicating that respondents strongly agreed that cybersecurity and environmental sustainability are significantly related.

The Pearson correlation coefficient ($r = 0.741$, $p < 0.05$) indicates a strong positive relationship between cybersecurity and environmental sustainability. This implies that improvements in cybersecurity significantly enhance sustainable environmental management. The findings corroborate those of Vinuesa *et al.,* (2024), who argued that digital resilience has become indispensable for environmental sustainability. The strong positive correlation demonstrates that environmental governance increasingly depends on secure digital infrastructure for monitoring, planning, and policy implementation.

Objective Two: Assess the Role of Cybersecurity in Protecting Environmental Infrastructure

Table 4: Cybersecurity Protection of Environmental Infrastructure

Statement	Agree (%)	Disagree (%)	Mean
Cyber Security protects renewable energy infrastructure	84.2	15.8	4.18
Cybersecurity safe guards environmental data bases	81.5	18.5	4.09
Smart grids require advanced cyber protection	86.9	13.1	4.24
Water infrastructure depends on cyber security	78.0	22.0	3.97

The regression result shows that cybersecurity explains approximately 46.6% of the variation in environmental infrastructure resilience, indicating a substantial contribution. The findings demonstrate that cybersecurity significantly contributes to protecting critical infrastructure such as renewable energy facilities, smart grids, and environmental monitoring systems. This supports the assertions of the International Energy Agency (2024) that digital security is essential for sustainable energy systems.

Objective Three: Examine the Challenges Posed by Cyber Threats to Sustainability Systems

Table 5: Perceived Cybersecurity Challenges

Challenge	Frequency	
Data breaches	242	81.2
Ransomware	228	76.5
Infrastructure hacking	236	79.2
Weak regulatory framework	221	74.2

The results indicate that 79.2% of respondents identified cyber threats as major obstacles to environmental sustainability. Discussion Cyber-attacks on environmental systems undermine climate monitoring, renewable energy management, and environmental governance. These findings are consistent with global cybersecurity reports showing increasing attacks on critical infrastructure sectors. Weak institutional capacity and inadequate cybersecurity preparedness remain significant barriers to resilient sustainable development.

Objective Four: Identify Policy Strategies for Integrating Cybersecurity into Environmental Governance

Table 6: Policy Strategies Supported by Respondents

Policy Measures	Frequency	Percentage (%)
Integration into environmental policy	261	87.6
Capacity building and training	253	84.9
Investment in cyber-resilient infrastructure	258	86.6
Multi-stakeholder collaboration	247	82.9
Stronger legislation	264	88.6

The findings reveal that 87.4% of respondents support integrating cybersecurity into national environmental governance frameworks.

Table 7: Multiple Regression Model

Model Statistics	Value
R	0.784
R^2	0.614
Adjusted R^2	0.607
F-value	116.82
Significance	0.000

The model indicates that policy integration, institutional capacity, and cybersecurity investment jointly explain 61.4% of improvements in resilient sustainable development. The results demonstrate overwhelming support for integrated environmental and cybersecurity policies. Respondents emphasized the need for legislative reforms, institutional strengthening, and investments in cyber-resilient infrastructure. The findings align with recent scholarship advocating for the incorporation of cybersecurity into environmental governance frameworks to enhance resilience and sustainability outcomes.

Discussion of Findings

The findings of this study demonstrate a statistically significant and positive relationship between environmental sustainability and cybersecurity in Nigeria ($r = 0.741$, $p < 0.05$), indicating that improvements in cybersecurity are associated with stronger environmental governance and more resilient sustainability initiatives. This result reinforces the growing body of literature that views digital security as an essential enabler of sustainable development rather than merely an information technology concern. Recent studies have shown that digital governance and secure technological ecosystems contribute significantly to environmental management by improving data integrity, resource monitoring, and policy implementation. Digitalization and effective governance mechanisms have been identified as important mediators for environmental sustainability and natural resource management, particularly where environmental decisions depend on reliable digital infrastructure.

The second major finding revealed that 82.6% of respondents agreed that cybersecurity is critical for protecting environmental infrastructure, while regression analysis showed that cybersecurity measures significantly predict infrastructure resilience ($\beta = 0.683$, $p < 0.05$). This finding suggests that renewable energy facilities, environmental monitoring systems, smart grids, and climate information platforms require robust cybersecurity safeguards to maintain operational continuity. The result is consistent with recent international evidence indicating that cybersecurity has evolved beyond data protection to become a strategic pillar for sustainability and organizational resilience. Contemporary scholarship argues that sustainable development increasingly depends on secure digital ecosystems capable of protecting critical infrastructure against cyber disruption.

The study also established that 79.2% of respondents perceived cyber threats as major challenges to environmental governance and sustainability systems. Respondents identified data breaches, ransomware attacks, infrastructure hacking, inadequate technical expertise, and weak regulatory frameworks as the most significant risks. These findings align with emerging evidence from Nigeria showing that weaknesses in digital governance, limited information sharing, inconsistent implementation of cybersecurity policies, and institutional capacity constraints continue to undermine effective management of cyber risks. Similar observations have been reported in studies examining Nigeria's cybersecurity environment, where enforcement gaps and fragmented governance structures reduce resilience against increasingly sophisticated cyber

threats. Another important outcome of the study is the overwhelming support for policy integration, with 87.4% of respondents advocating the incorporation of cybersecurity into environmental governance frameworks.

The multiple regression model further demonstrated that cybersecurity policy integration, institutional capacity building, and investments in cyber-resilient infrastructure collectively explain 61.4% of the variation in resilient sustainable development ($R^2 = 0.614$). This finding supports recent literature emphasizing that sustainable digital transformation requires coordinated governance structures that integrate cybersecurity, environmental management, and institutional accountability. Studies on digital transformation in Nigeria have similarly argued that fragmented governance limits the realization of sustainability benefits and that integrated policy approaches are necessary to maximize digital innovation while reducing associated risks. From a Nigerian perspective, these findings have significant practical implications. Nigeria's rapid expansion of digital technologies across government institutions, renewable energy projects, financial systems, and environmental monitoring programmes has created substantial opportunities for improving environmental management. At the same time, the country faces persistent challenges, including inadequate cybersecurity capacity, limited technical expertise, infrastructure deficits, and uneven enforcement of regulatory frameworks. Nigeria's ongoing efforts to strengthen sustainability reporting and digital governance demonstrate increasing recognition of these issues, but successful implementation will require stronger institutional coordination, sustained investment, and context-specific cybersecurity policies that support environmental objectives.

The positive correlation, high stakeholder agreement, and significant regression coefficients collectively suggest that strengthening cybersecurity should be regarded as an integral component of environmental policy and sustainable development planning in Nigeria. Consequently, achieving long-term environmental sustainability will require not only ecological interventions but also strategic investments in digital security, institutional resilience, workforce development, and integrated governance systems capable of responding to emerging technological and environmental challenges.

Conclusion

This study empirically examined the nexus between environmental sustainability and cybersecurity and explored its implications for resilient sustainable development in Nigeria. Using a descriptive survey design, data were collected from 298 respondents drawn from environmental agencies, cybersecurity institutions, renewable energy organizations, government ministries, academia, and non-governmental organizations. The study investigated the relationship between environmental sustainability and cybersecurity, assessed the role of cybersecurity in protecting environmental infrastructure, and examined the challenges posed by cyber threats to sustainability systems, and evaluated policy strategies for integrating cybersecurity into environmental governance. Descriptive statistics, Pearson Product Moment Correlation, and Multiple Regression Analysis were employed to analyze the data. The findings revealed a strong and statistically significant positive relationship between environmental sustainability and cybersecurity ($r = 0.741$, $p < 0.05$), indicating that improvements in cybersecurity contribute substantially to environmental sustainability outcomes. The study further found that cybersecurity plays a critical role in safeguarding environmental infrastructure and enhancing institutional resilience. Specifically, 82.6% of respondents agreed that cybersecurity is essential for protecting renewable energy systems, environmental databases, climate monitoring platforms, and other critical infrastructure. The regression analysis demonstrated that cybersecurity measures significantly influence environmental infrastructure resilience ($\beta = 0.683$, $p < 0.05$). The findings also showed that cyber

threats, including ransomware attacks, data breaches, infrastructure hacking, weak regulatory frameworks, and inadequate technical expertise, constitute major challenges to environmental governance, with 79.2% of respondents identifying cyber threats as significant risks. Furthermore, 87.4% of respondents supported the integration of cybersecurity policies into environmental governance frameworks, while the regression model indicated that policy integration, institutional capacity building, and investments in cyber-resilient infrastructure jointly explained 61.4% of the variation in resilient sustainable development ($R^2 = 0.614$). Based on these findings, the study concludes that cybersecurity has become an indispensable pillar of environmental sustainability in the digital age. As environmental governance increasingly depends on digital technologies for monitoring, planning, communication, and resource management, the security and resilience of these systems become critical determinants of sustainable development outcomes.

Recommendations

Based on the findings of this study, the following recommendations are proposed;

1. Given the finding that 87.4% of respondents supported the integration of cybersecurity into environmental governance, the Federal Government of Nigeria should formally incorporate cybersecurity requirements into national environmental policies, climate adaptation strategies, and natural resource management programmes. Environmental Impact Assessments (EIAs) and Strategic Environmental Assessments (SEAs) should include mandatory cyber-risk assessments for digital environmental infrastructure such as climate monitoring systems, smart water facilities, and renewable energy installations.
2. The regression analysis demonstrated that cybersecurity significantly predicts environmental infrastructure resilience ($\beta = 0.683$; $p < 0.05$). Consequently, Nigeria should establish a dedicated National Environmental Cybersecurity Protection Framework under the joint supervision of the Federal Ministry of Environment, the National Information Technology Development Agency (NITDA), the Nigerian Communications Commission (NCC), and sector regulators. The framework should require periodic vulnerability assessments, continuous monitoring, zero-trust security architecture, incident response protocols, and mandatory reporting of cyber incidents affecting environmental systems.
3. The finding that 82.6% of respondents recognized cybersecurity as essential for protecting environmental infrastructure underscores the need to secure Nigeria's petroleum pipelines, electricity transmission networks, renewable energy facilities, and environmental monitoring systems. Building on recent 2025 proposals for strengthening pipeline security through integrated surveillance technologies, remote sensing, drone monitoring, and real-time threat intelligence, cybersecurity controls should be embedded within all pipeline management systems to prevent sabotage, ransomware attacks, and operational disruption.
4. The empirical evidence showed that policy integration explains a significant proportion of improvements in resilient sustainable development ($R^2 = 0.614$). Therefore, all federal and state environmental agencies should adopt digital sustainability reporting systems consistent with the Financial Reporting Council's amended 2026 Sustainability Reporting Guideline (SRG 1).
5. The survey identified inadequate technical expertise as one of the major barriers to cyber-resilient environmental governance. Universities, research institutes, and professional bodies should therefore introduce interdisciplinary academic programmes combining environmental sustainability, cybersecurity, artificial intelligence, geospatial technologies, and critical infrastructure protection.

References

Achuthan, K., Nair, R., Kumar, V., & Menon, S. (2025). Cyber resilience and sustainable development in the digital era. *Journal of Sustainable Digital Transformation*, 8(1), 1–18.

Achuthan, K., Sankaran, S., Roy, S., & Raman, R. (2025). Integrating sustainability into cybersecurity: Insights from machine learning based topic modeling. *Discover Sustainability*, 6(1), Article 44.

Balogun, F. (2026, February 4). National focus on cybersecurity needed to safeguard renewable energy systems. *BusinessDay Nigeria*. https://businessday.ng/technology/article/national-focus-on-cybersecurity-needed-to-safeguard-renewable-energy-systems/

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23(1), 4–17.

Bibri, S. E., Krogstie, J., & Kärrholm, M. (2023). Sustainable smart cities and environmental governance in the age of digital transformation. *Smart Cities*, 6(3), 1201–1225.

Folke, C. (2016). Resilience. In M. I. Letcher (Ed.), *Climate Change* (2nd ed., pp. 35–51). Elsevier.

Folke, C., Biggs, R., Norström, A. V., Reyers, B., & Rockström, J. (2023). Social-ecological resilience and sustainable development. *Ecology and Society*, 28(2), 15–29.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4, 1–23.

Hong, Y., & Xiao, Y. (2024). Digital technologies and environmental sustainability: Emerging opportunities and challenges. *Scientific Reports*, 14(1), 53760.

Ibekwe, U. U., Mbanaso, U. M., & Ibekwe, U. D. (2026). A multi-tiered framework for AI-driven cybersecurity governance in Africa: Pathways to cyber resilience and sustainable development. *Journal of Policy and Development Studies*, 20(3), 334–362.

Intergovernmental Panel on Climate Change (IPCC). (2023). *Climate Change 2023: Synthesis Report*. IPCC.

International Energy Agency (IEA). (2024). *Digitalization and Energy Systems Report 2024*. International Energy Agency.

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Outlook 2024*. ITU.

Kshetri, N. (2024). Cybersecurity and critical infrastructure protection in the digital age: Implications for sustainability and resilience. *Telecommunications Policy*, 48(2), 102651.

Morales-Sáenz, R., Pérez, J., González, M., & Torres, A. (2024). Cybersecurity and sustainability: Building resilient digital infrastructures for sustainable development. *Sustainability*, 16(14), 5884.

National Institute of Standards and Technology (NIST). (2024). *Cybersecurity Framework 2.0*. U.S. Department of Commerce.

Obasi, C. C., Adeyemi, O. A., & Nwankwo, E. C. (2024). Cybersecurity's role in environmental protection and sustainable development: Bridging technology and sustainability goals. *International Journal of Environmental Studies*, 81(4), 512–529.

Purvis, B., Mao, Y., & Robinson, D. (2019). Three pillars of sustainability: In search of conceptual origins. *Sustainability Science*, 14(3), 681–695.

Trist, E. L. (1981). *The evolution of socio-technical systems: A conceptual framework and an action research program*. Ontario Quality of Working Life Centre.

United Nations. (2024). *The Sustainable Development Goals Report 2024*. United Nations.

United Nations Environment Programme (UNEP). (2024). *Global Environment Outlook 2024*. UNEP.

Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., Felländer, A., Langhans, S. D., Tegmark, M., & Fuso Nerini, F. (2024). Artificial intelligence and the future of environmental sustainability. *Nature Communications*, 15(1), 2114.

Von Solms, R., & Van Niekerk, J. (2023). Cybersecurity governance and organizational resilience in the digital age. *Computers & Security*, 12(8), 103201.

World Economic Forum. (2024). *Global Risks Report 2024*. World Economic Forum.

Xu, M., David, J. M., & Kim, S. H. (2023). The fourth industrial revolution and sustainable development: Implications for environmental governance and cybersecurity. *Journal of Cleaner Production*, 402, 136876.