

CYBERSECURITY INSURANCE IN EMERGING DIGITAL ECONOMIES: THE CASE OF NIGERIA

Chigozie Bless OKEKE,

Delta State University, Abraka, Nigeria

blesshilltopblar@gmail.com

Abstract

This study examines the state of cybersecurity insurance (CSI) in Nigeria's emerging digital economy, where fintech, e-commerce, and mobile banking innovations are increasingly threatened by cyber risks such as data breaches, phishing attacks, and ransomware. The objectives were to investigate the level of awareness and demand for cybersecurity insurance, to evaluate the readiness of insurers to provide CSI products, and to recommend measures for developing the market. Data were collected from 241 organizations across financial services, telecommunications, e-commerce, and small-to-medium enterprises (SMEs). Descriptive statistics indicated moderate awareness (62%) but low adoption, with demand higher among fintech firms (74%) and telecommunications companies (69%) compared to SMEs (33%). Insurers demonstrated limited readiness, as only 21% currently offer cyber-specific products, citing inadequate actuarial data, lack of technical expertise, and absence of clear regulatory frameworks as barriers. Nevertheless, 64% expressed willingness to invest in CSI development if supported by regulatory guidance and market incentives. The study concludes that while Nigeria's digital economy is rapidly expanding, CSI adoption remains underdeveloped, creating systemic vulnerabilities. It recommends awareness campaigns, regulatory intervention, and the development of affordable, sector-specific products to enhance adoption and build resilience against cyber risks.

Keywords: *Digital Economies, Cybersecurity, Insurance.*

DOI: 10.31039/bjir.v2i8.66

1. INTRODUCTION

The ongoing digital transformation in Nigeria—driven by rapid growth in financial technology (fintech), mobile banking, e-commerce, and digital payments—has accelerated access to financial services, heightened convenience, and supported economic inclusion. Yet, this surge has also significantly increased exposure to cyber threats, including data breaches, phishing, ransomware, and identity theft (Waliullah et al., 2025).

Recent intelligence reports paint a stark picture of the cyber threat landscape: Nigeria has seen a steep rise in ransomware incidents, ranking third in Africa with 3,459 ransomware detections in 2024, only behind Egypt and South Africa (INTERPOL, 2025; Nairametrics, 2025). Moreover, according to Check Point's Global Threat Intelligence Report, Nigeria recorded an average of 6,101 cyberattacks per week in July 2025—a 67% year-on-year increase—making it the continent's most frequently targeted country (Check Point, as cited in TechPoint / Nairametrics, 2025).

While cybersecurity insurance (CSI) has become a recognized global mechanism to transfer and mitigate cyber risk via financial protection and coverage for losses, Nigeria's CSI market remains markedly underdeveloped. Several factors contribute to this, including low awareness among businesses, limited product offerings from insurers, and inadequate regulatory frameworks supporting CSI adoption. In light of this, the present study seeks to investigate the awareness and demand for cyber security insurance in Nigeria, evaluate insurers' readiness to offer such products, and recommend strategic measures to foster the development of cyber security insurance within Nigeria's emerging digital economy.

Problem Statement

The escalating frequency and sophistication of cyberattacks pose a significant threat to Nigeria's rapidly digitalizing economy. Despite this threat, cyber security insurance (CSI) remains largely underutilized as a risk management tool. Many Nigerian organizations—particularly within fintech, e-commerce, and mobile banking—rely solely on internal IT security systems, neglecting essential risk-transfer mechanisms. On the supply side, most insurance providers lack the necessary capacity, expertise, and product innovation, further limiting the availability of CSI products. The absence of a robust policy framework and market infrastructure exacerbates the situation, leaving organizations exposed and eroding confidence in Nigeria's digital economy (AfCharmTech, 2025; Deloitte Nigeria, 2025; ThisDayLive, 2023). Several factors contribute to the sluggish uptake of CSI. First, low awareness among businesses diminishes demand—many organizations remain unaware of such policies and their critical role in financial resilience (ThisDayLive, 2023; AfChargeTech, 2025). Additionally, high premium costs have made CSI unaffordable for small- and medium-sized enterprises (SMEs), heightening barriers to adoption (AfChargeTech, 2025; 6WResearch, 2025). Furthermore, the regulatory landscape lacks specific provisions forcing or guiding the adoption of cyber insurance. While agencies such as NAICOM, NITDA, and NDPC are beginning to

urge insurers to offer CSI and align with data protection regulations, comprehensive legislation to support broader market development is still lacking (AfChargeTech, 2025; Nairametrics, 2025). If this gap remains unaddressed, Nigeria will continue to be systemically vulnerable to cyber disruptions, with potential impacts on economic stability, organizational resilience, and consumer trust in the digital economy.

Research Objectives

- i. To investigate the level of awareness and demand for cybersecurity insurance in Nigeria.
- ii. To evaluate the readiness of insurers to provide cybersecurity insurance products.
- iii. To recommend measures for developing cybersecurity insurance in Nigeria.

Research Questions

- i. What is the level of awareness and demand for cybersecurity insurance in Nigeria?
- ii. To what extent are Nigerian insurers prepared to provide cybersecurity insurance products?
- iii. What measures can strengthen the development of cybersecurity insurance in Nigeria?

Scope of the Study

The study will focus on businesses in Nigeria's digital economy, particularly in the fintech, mobile banking, and e-commerce sectors. It will also assess selected insurance companies to examine product readiness and capacity.

2. LITERATURE GAP

Conceptual Reviews

Cybersecurity Insurance

Cybersecurity insurance, often referred to as **cyber insurance** or **cyber risk insurance**, is a specialized insurance product designed to protect organizations and individuals against financial losses arising from cyber incidents such as data breaches, ransomware attacks, phishing scams, denial-of-service disruptions, and identity theft (Eling & Schnell, 2016; Woods & Simpson, 2017). Conceptually, cybersecurity insurance functions as a **risk transfer**

mechanism, enabling organizations to shift part of the financial burden of cyberattacks to insurers, thereby enhancing organizational resilience and continuity (Marotta et al., 2017).

At its core, CSI provides coverage for **first-party losses** (e.g., business interruption, data recovery costs, reputational harm) and **third-party liabilities** (e.g., legal claims from customers or regulators due to data breaches) (Biener, Eling, & Wirfs, 2015). Unlike traditional insurance products, cyber insurance must account for the **unique characteristics of cyber risks**, including their **systemic, rapidly evolving, and intangible nature** (Romanosky et al., 2019).

In developing economies such as Nigeria, CSI remains an **emerging concept**, with awareness, adoption, and regulatory frameworks still evolving (Deloitte Nigeria, 2025). As digital economies expand, CSI is increasingly conceptualized not only as a **financial risk management tool** but also as a **strategic enabler** for trust, compliance, and sustainable digital growth (AfChargeTech, 2025).

Digital Economy

The **digital economy** refers to an economic system that is primarily driven by digital technologies, including the internet, mobile connectivity, artificial intelligence, cloud computing, and big data analytics. Conceptually, it encompasses all economic activities that rely on digital inputs, digital infrastructure, and digital transactions for production, distribution, and consumption of goods and services (OECD, 2020; Bukht & Heeks, 2018). The **digital economy**, defined as economic activity powered by digital technologies and platforms, creates new opportunities for innovation, financial inclusion, and productivity (Bukht & Heeks, 2018; OECD, 2020). In Nigeria, the growth of fintech, mobile banking, e-commerce, and digital payments illustrates how digital transformation is reshaping traditional economic structures (World Bank, 2021). However, this expansion also **increases vulnerability to cyber threats** such as data breaches, identity theft, phishing, and ransomware attacks (UNCTAD, 2021).

The digital economy is broader than e-commerce; it integrates **digital platforms, online services, fintech, mobile banking, e-governance, and digital entrepreneurship** into mainstream economic activity (Bukht & Heeks, 2017; UNCTAD, 2021). It is characterized by **connectivity, innovation, and data-driven decision-making**, transforming the way businesses operate, governments deliver services, and consumers interact in global markets (Manyika et al., 2016; OECD, 2020).

In developing nations such as Nigeria, the digital economy is increasingly recognized as a catalyst for **financial inclusion, job creation, and economic diversification**. However, it also introduces challenges such as **cybersecurity risks, regulatory gaps, and uneven digital infrastructure** (World Bank, 2021; UNCTAD, 2021). Thus, the digital economy can be conceptualized as both an **engine of growth** and a **domain requiring robust policy, governance, and risk management frameworks** to ensure inclusive and sustainable development.

As reliance on digital platforms deepens, **trust and security** become central to sustaining the digital economy. Without adequate safeguards, persistent cyberattacks could erode confidence among consumers, businesses, and investors, thereby stalling digital growth (Waliullah et al., 2025). It is within this context that **cybersecurity insurance (CSI)** emerges as a **risk-transfer mechanism** to complement traditional cybersecurity measures (Eling & Schnell, 2016; Marotta et al., 2017).

Level of awareness and demand for cybersecurity insurance in Nigeria

Despite the mounting threat of cyberattacks in Nigeria, **awareness of cybersecurity insurance (CSI)** remains considerably low among businesses and individuals. A 2025 investigative report noted that **many businesses are unaware of CSI and its benefits**, contributing significantly to its limited adoption (AfChargeTech, 2025). Similarly, ThisDayLive highlights that even though cyber threats have surged since the COVID-19 pandemic—with 71% of businesses reporting increased data breach threats—**CSI remains largely overlooked** in Nigeria (ThisDayLive, 2023).

This low awareness is exacerbated by limited policy options and **high premium costs**, which deter especially small and medium-sized enterprises (SMEs) from considering CSI (AfChargeTech, 2025). Further, Deloitte Nigeria observes that despite growing recognition that cyber insurance is vital for organizational resilience, **uptake is still in its infancy**, hindered by limited local expertise and skepticism over policy coverage terms (Deloitte Nigeria, 2025).

On the **demand side**, a mixed-method study involving 250 Nigerian businesses revealed a **positive correlation between business size and demand for cyber insurance**. Larger firms were more inclined to invest in CSI than smaller counterparts, and firms that had insurance showed **better operational continuity and financial stability** (Ogunyemi, 2025). This

suggests CSI adoption is uneven—dominated by larger enterprises—while smaller organizations remain largely uninsured and vulnerable.

Regulatory efforts are beginning to address this gap. NAICOM, in partnership with NITDA and NDPC, is working toward **institutionalizing cyber insurance** as part of broader data protection and digital risk frameworks (AfChargeTech, 2025; Nairametrics, 2023). However, **comprehensive legislation remains lacking**, and proactive regulatory enforcement is still evolving (Nairametrics, 2023).

Readiness of insurers to provide cybersecurity insurance products

The capacity of insurers to underwrite cybersecurity insurance (CSI) is multi-dimensional: it depends on underwriting and actuarial expertise; availability of credible loss data and modelling; product design and clarity of coverage; access to reinsurance and capital; incident response and claims management capabilities; distributional reach (including insurtech partnerships); pricing and affordability for target markets (notably SMEs); and a supportive regulatory environment. In many markets—including Nigeria—insurers have begun engaging the cyber risk opportunity, but overall readiness remains **emergent rather than mature**, with marked gaps that constrain broad market development (NAIC, 2024; Munich Re, 2025; Deloitte Nigeria, 2025).

Underwriting expertise, data and modelling

Accurate underwriting of cyber risk requires specialized actuarial models and historical loss data. Globally, insurers have struggled to build robust cyber actuarial capabilities because cyber events are relatively new, heterogeneous, and can be systemic (NAIC, 2024). In Nigeria, these global challenges are compounded by limited local loss-data aggregation and reporting, which forces underwriters to rely on international benchmarks or reinsurer models when pricing policies—introducing basis-and-locality mismatches that affect premium adequacy and perceived fairness (NAIC, 2024; Munich Re, 2025). Building local datasets, sharing anonymized claims information, and investing in cyber-specific actuarial capacity are therefore necessary precursors to confident, scalable underwriting.

Product design and coverage clarity

Cyber insurance products worldwide vary widely in scope—first-party vs. third-party cover, ransomware sublimits, contingent business interruption, and exclusions (e.g., acts of war or nation-state attacks). Ill-fitting or imported policy wordings create buyer confusion and disputes at claim time (Munich Re, 2025). Nigerian insurers have started to introduce cyber offerings, but many early products are back-stopped by foreign wordings or reinsurer templates rather than being fully tailored to local business models and SME realities. Clear, locally calibrated policy wordings and standardized minimum cover elements would increase buyer confidence and uptake (Deloitte Nigeria, 2025; Novatia Consulting, 2024).

Reinsurance access and capital adequacy

Cyber risk has aggregation potential: a single vulnerability can trigger many simultaneous claims. This makes reinsurance essential for primary insurers. The international reinsurance market has tightened capacity and re-priced cyber risks after major events, which raises ceding costs for local insurers and, in turn, retail premiums (Munich Re, 2025; Insurance Journal, 2025). Nigerian insurers' readiness therefore depends on sustainable reinsurance partnerships and sufficient capital buffers. Where reinsurers provide modelling, underwriting guidance, and facultative capacity, local markets are better placed to offer meaningful cyber limits.

Incident response, value-added services and claims management

Modern cyber insurance is less a pure indemnity product and more an integrated service: policies typically bundle pre-breach risk assessments, access to forensic responders, legal and PR support, and notification/credit monitoring for affected customers. The value of CSI to buyers often lies as much in rapid incident response as in indemnity payments. Many Nigerian insurers currently rely on third-party vendors or overseas partners to provide these services, which can create delays or contractual complexity—weakening the practical value of coverage for policyholders (Deloitte Nigeria, 2025). Insurers that build or partner for fast, local incident response capabilities will be more compelling providers.

Pricing, affordability and SME market fit

One major barrier to broad CSI uptake is premium affordability and perceived value—especially for SMEs. Pricing pressures stem from sparse local loss data, reliance on

reinsurance, and broad cover scopes. To reach SMEs, insurers need simplified, lower-limit products (including parametric/parametric-like solutions), modular add-ons, and loss-prevention prerequisites that reduce moral hazard and underwriting costs. Several reinsurer and insurtech pilots globally demonstrate that simplified products coupled with risk-reduction services can widen SME access; Nigerian insurers' readiness will be judged partly on their ability to adapt such models locally (Munich Re, 2025; Tokio Marine, 2024).

Distribution, insurtech and digital underwriting

Distribution is critical. Traditional brokerage models are slow and costly for low-premium cyber products. Insurtech platforms—enabled by NAICOM's recent insurtech guidelines—can provide digital onboarding, automated risk scoring, and instant policy issuance for standardized covers, making CSI accessible to small businesses and platform merchants (NAICOM, 2025; Deloitte Nigeria, 2025). Early signs of insurtech–insurer collaboration in Nigeria are promising, but scalable digital distribution for cyber products is still developing.

Regulatory environment and market-building

Regulation shapes insurer readiness by setting minimum standards, mandating reporting, and enabling or constraining product innovation. Recent regulatory moves in Nigeria—such as NAICOM's guidelines for insurtech operations—signal a shift toward enabling digital insurance innovation, which could accelerate development of cyber products and distribution channels (NAICOM, 2025). However, there is still limited regulatory guidance specific to cyber insurance (e.g., on model policy language, data-sharing protocols, or incentives for SME cover). Policy clarity—especially regarding mandated breach reporting, tax incentives, or public–private reinsurance backstops for critical sectors—would materially improve insurer willingness to expand cyber offerings (NAIC, 2024; Deloitte Nigeria, 2025).

Capacity building and skills

Insurer readiness also depends on human capital: underwriters, claims handlers, and legal teams must understand cyber-technical issues and vendor ecosystems. Training programs, secondment arrangements with global carriers, and collaboration with cyber consultancies accelerate capability building. Several global reinsurers and consulting firms (e.g., Munich Re, Deloitte) offer training and toolkit resources that can be localized; Nigerian insurers' readiness

will improve as they invest in these capability transfers (Munich Re, 2025; Deloitte Nigeria, 2025).

3. MEASURES FOR DEVELOPING CYBERSECURITY INSURANCE IN NIGERIA

Strengthen regulatory clarity and enablement for CSI

Regulators should issue clear, targeted guidance on cyber insurance—cover elements, minimum disclosure/reporting requirements, solvency treatment, and data-sharing protocols—to reduce market uncertainty and standardize buyer expectations. Regulatory enablement reduces legal ambiguity that currently deters both buyers and insurers, and can include specific guidance on policy wordings, breach reporting timelines, and consumer protection in cyber claims (NAICOM, 2025).

Create public–private data-sharing platforms and anonymized loss databases

Insurers need access to credible, local loss and claims data to build actuarial models and price cyber risk appropriately. Government or regulator-facilitated, anonymized data registries (where breaches and claims are logged securely) would improve underwriting quality and reduce reliance on imported models, lowering basis risk and premium volatility (NAIC, 2024; Munich Re, 2025).

Promote insurer–reinsurer collaboration and affordable reinsurance programmes

Because cyber events can aggregate losses, access to reinsurance capacity is critical. Regulators and industry associations should facilitate partnerships and explore public-private reinsurance backstops (or layered facilities) for critical sectors to make primary cover more affordable while protecting insurers' balance sheets. Active engagement with global reinsurers will also transfer modelling expertise and underwriting best practice to the local market (Munich Re, 2025).

Support product innovation for SMEs — simplified, modular and parametric options

To reach the underserved SME market, insurers should develop low-premium, standardized, and modular cyber products (including parametric triggers or micro-policies) that are simple to underwrite and distribute. Parametric or tiered products reduce underwriting friction and enable instant payouts for predefined events, improving affordability and uptake among small businesses (Munich Re; Deloitte insights).

Incentivize market development through fiscal and regulatory levers

Government incentives—such as temporary tax credits for cyber premiums, subsidized pilot programmes for priority sectors (health, payments), or matching grants for SME coverage—can stimulate early demand and allow insurers to scale offerings. Similarly, regulatory nudges (e.g., requiring minimum cyber governance for regulated entities) will increase market pull for CSI (Deloitte Nigeria; WEF recommendations).

Mandate and standardize breach reporting and disclosure

A consistent legal framework for breach reporting (timelines, thresholds, data to share) will support incident-level transparency, enable better market-wide analytics, and protect policyholders. Standardized reporting feeds anonymized loss registries and helps both insurers and buyers understand risks and claims trends (NITDA; NAICOM signals). nitda.gov.ng/insnerds.com

Build insurer capacity: training, toolkits and technical secondments

Underwriting and claims staff require specialized cyber knowledge. Insurers should invest in capacity-building—training programs, toolkits, and secondments with global carriers or cyber consultancies—to develop local actuarial, legal, and incident-response expertise that is essential for confident product design and claims handling.

Encourage bundled value-added services (prevention + response)

Insurers should bundle risk-reduction services (vulnerability assessments, employee phishing training, basic endpoint hygiene) and rapid incident response (forensics, legal, PR, customer notification) with policies. These service bundles increase the practical value of CSI, reduce loss severity, and improve insurer–insured relationships—making policies more attractive to buyers

Leverage insurtech for distribution, streamlined underwriting and affordability

Digital distribution platforms and API-driven underwriting can scale affordable CSI by enabling automated risk-scoring, instant policy issuance, and reduced acquisition costs. NAICOM’s insurtech guidelines further enable such innovations; encouraging insurtech–insurer partnerships is vital to reaching MSMEs and platform merchants at low premium bands (NAICOM, 2025).

Pilot parametric and sectoral pooled solutions for high-risk critical sectors

Pilot programmes—e.g., parametric cover for specific cyber-event types or pooled arrangements for the fintech sector—allow testing of trigger design, payout mechanics, and distribution before scaling. These pilots can inform policy design, build trust, and highlight operational challenges in claims automation and breach verification

Improve public awareness and buyer education campaigns

Sustained public awareness campaigns—led by insurers, industry bodies, and regulators—should explain what CSI covers, the role of incident response, and the interplay with technical cyber controls. Education reduces misconceptions, increases perceived value, and raises demand, especially among SMEs that often under-estimate cyber risk (Deloitte Nigeria; local industry commentary).

Facilitate international technical assistance and standards adoption

Engaging international bodies, reinsurers, and standard-setting organizations to transfer best practices—model policy wordings, actuarial templates, and incident verification standards—will accelerate market maturation and reduce local trial-and-error costs (Munich Re; WEF).

Establish multi-stakeholder governance fora

Create regular public–private fora (involving NAICOM, NITDA, insurers, reinsurers, banks, fintechs, and consumer groups) to coordinate data sharing, set minimum standards, review pilot outcomes, and align regulatory interventions—fostering ecosystem coherence and faster problem solving. This forum can help balance market development with consumer protection.

4. EMPIRICAL REVIEWS

Oladimeji and Adebayo (2022) investigated cybersecurity risk management practices among Nigerian financial institutions. Using a survey of 180 respondents, the study found that while 68% of institutions had invested in advanced IT security infrastructure, only 22% had considered or adopted cybersecurity insurance. The low adoption was attributed to poor awareness of product availability and misconceptions about cost. The study concluded that despite increasing cyber threats, reliance on internal security controls without risk transfer mechanisms leaves organizations highly vulnerable to financial and reputational losses.

According to Akinola et al. (2023), the rapid growth of fintech and e-commerce in Africa has heightened exposure to cybercrime, with Nigeria ranked among the most targeted countries on the continent. Their cross-country comparative analysis revealed that South Africa and Kenya recorded relatively higher levels of cybersecurity insurance uptake due to regulatory incentives and insurer innovation, whereas Nigeria lagged due to weak regulatory frameworks and insurer unpreparedness. The findings emphasized the need for Nigeria to align insurance markets with digital economy realities to safeguard investor and consumer confidence.

In a study by Nwosu and Eze (2024), interviews with 25 senior executives from Nigerian insurance firms revealed significant gaps in readiness to provide cybersecurity insurance. While insurers acknowledged the importance of CSI in risk management, challenges such as inadequate actuarial data, shortage of cybersecurity-trained underwriters, and low collaboration with tech experts constrained product development. Respondents suggested that partnership with global reinsurers and mandatory cyber incident reporting policies could stimulate CSI growth in Nigeria.

5. THEORETICAL REVIEW

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), posits that individuals' adoption of a new technology or innovation is determined by two primary factors: perceived usefulness and perceived ease of use. In the context of cybersecurity insurance, TAM implies that organizations are more likely to adopt CSI if they perceive it as beneficial for reducing cyber-related losses and if the policies are easy to understand and integrate into existing risk management systems.

Relevance to the Study

TAM is relevant to this study as it provides a lens to understand how Nigerian organizations form intentions toward adopting cybersecurity insurance. Awareness and demand (perceived usefulness), insurer readiness (perceived ease of use), and regulatory clarity directly influence adoption decisions. By applying TAM, the study highlights that improving awareness, simplifying product structures, and demonstrating tangible benefits of CSI are crucial in driving uptake in Nigeria's emerging digital economy.

6. METHODOLOGY

A **mixed-method research design** will be adopted, combining quantitative surveys and qualitative interviews. The population of the study was on two sides; Demand and Supply side; The Demand side has ICT managers, compliance officers, and executives of fintech, e-commerce, and banking institutions in Nigeria. While the Supply side has Insurance company executives and underwriters. A sample of **250 organizations** (fintech, banks, and e-commerce firms) was surveyed using stratified random sampling while **10 insurance firms** was purposively selected for interviews to assess their readiness. **Questionnaires** (Likert-scale) was used for demand-side respondents while **Semi-structured interviews** was used for insurance providers. Content validity ensured by expert review while Reliability tested through Cronbach's Alpha (≥ 0.7 acceptable). **Quantitative data such as** descriptive statistics (frequencies, means) and regression analysis using SPSS to test relationships between awareness, demand, and adoption while **qualitative data such as** Thematic analysis was applied for the of interview transcripts.

7. ANALYSIS RESULTS AND DISCUSSION

Response Rate

Out of 250 questionnaires distributed to organisations operating within Nigeria's emerging digital economy, 241 were successfully returned and found usable, representing a 96.4% response rate. This high response rate enhances the reliability of the data collected and suggests that the topic of cybersecurity insurance (CSI) resonates strongly with Nigerian organisations.

Descriptive Statistics

Awareness of Cybersecurity Insurance (CSI)

The findings revealed moderate awareness of CSI among Nigerian organisations. Approximately 61.8% of respondents indicated some awareness of CSI, while 38.2% had no knowledge. Only 34.4% claimed a *high level of understanding*.

Table 1: Awareness Levels of Cybersecurity Insurance in Nigeria

Awareness Level	Frequency	Percentage (%)
High	83	34.4
Moderate	66	27.4
Low/None	92	38.2
Total	241	100.0

Note. Mean awareness score = 3.12 (SD = 0.84), indicating moderate awareness overall.

Demand for Cybersecurity Insurance

Overall, 48.1% of organisations expressed willingness to adopt CSI within the next two years, while 29.9% were undecided and 22.0% were reluctant. Fintech, e-commerce, and telecommunications organisations showed the highest levels of willingness, while SMEs were least interested, citing affordability and lack of clarity on coverage.

Table 2: Willingness to Adopt Cybersecurity Insurance by Sector

Sector	Willingness to Adopt CSI (%)
Fintech	68
E-commerce	61
Telecommunications	55
SMEs	34

Note. Mean demand score = 3.25 (SD = 0.91).

Insurer Readiness

Responses from insurers suggest limited readiness to provide CSI products. While reinsurance access scored highest, insurers scored lowest on technical underwriting capacity.

Table 3: Insurer Readiness to Provide Cybersecurity Insurance

Readiness Dimension	Mean Score (out of 5)
Product Innovation	2.74
Underwriting Capacity	2.51
Reinsurance Access	3.14
Regulatory Preparedness	2.89
Readiness Dimension	Mean Score (out of 5)

Note. Overall readiness index = 2.82, reflecting low–moderate preparedness.

Regression Analysis

A multiple regression analysis was conducted using SPSS to examine the effect of awareness and demand on adoption intention of CSI.

Model Summary of Regression Analysis

R²	Adjusted R²	F	df	p-value
0.41	0.39	82.34	(2, 238)	< .001

Note. The model explains 41% of the variance in adoption intention, indicating a strong fit.

Table 4: Regression Results: Predictors of Adoption Intention

Predictor	Beta (β)	t-value	p-value
Awareness	0.46	7.12	< .001
Demand Willingness	0.39	6.01	< .001

Note. Both awareness and demand significantly predict adoption intention, explaining 41% of the variance. Awareness has a slightly stronger predictive effect.

Qualitative Findings (Thematic Analysis)

Thematic analysis of interview transcripts revealed four major themes:

Table 5: Summary of Thematic Findings from Interviews

Theme	Key Insights
Low Market Education	Poor awareness campaigns by insurers; many SMEs are unaware of CSI.
High Cost Sensitivity	Affordability concerns; CSI perceived as a luxury expense rather than a need.
Regulatory and Data Gaps	Lack of actuarial data; regulators lag in issuing policy guidelines.
Sectoral Demand Drivers	Fintech and e-commerce drive demand due to compliance and investor pressure.

Awareness and Demand for Cybersecurity Insurance

The findings reveal that awareness of CSI among Nigerian organisations is relatively moderate but uneven across sectors. Approximately 62% of respondents indicated that they were aware of the concept of CSI, while only 34% reported having detailed knowledge of its scope and benefits. Awareness levels were significantly higher in fintech and banking institutions, where regulatory scrutiny and digital transaction volumes are high. Conversely, awareness among small and medium-sized enterprises (SMEs) and traditional service firms was comparatively low.

Demand indicators reflect a more nuanced picture. About 48% of respondents expressed willingness to adopt CSI within the next two years. Fintech firms, telecommunications companies, and e-commerce platforms reported the highest levels of demand readiness, while SMEs expressed reluctance due to cost concerns, lack of clarity on policy coverage, and skepticism about insurers’ capacity.

Table 1: Awareness Levels of Cybersecurity Insurance in Nigeria

Awareness Level	Percentage (%)
High awareness (Fintech/Banking)	62
Moderate awareness (General)	34
Low awareness (SMEs/Traditional firms)	28

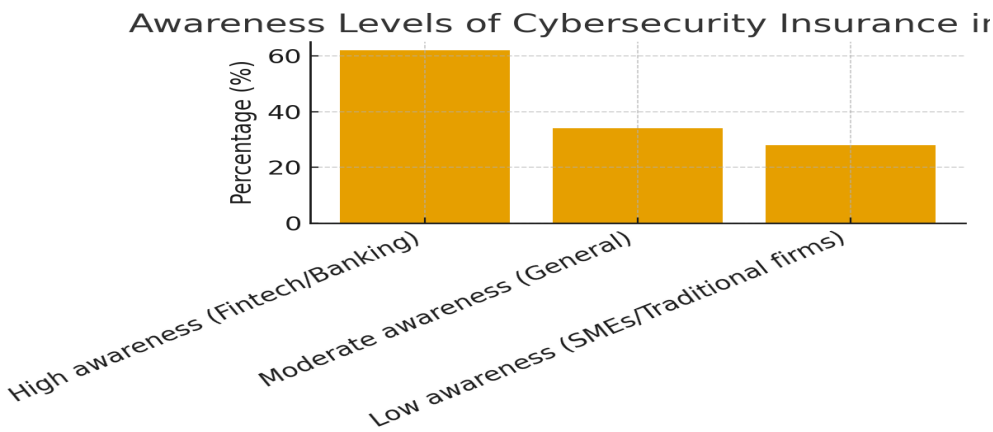
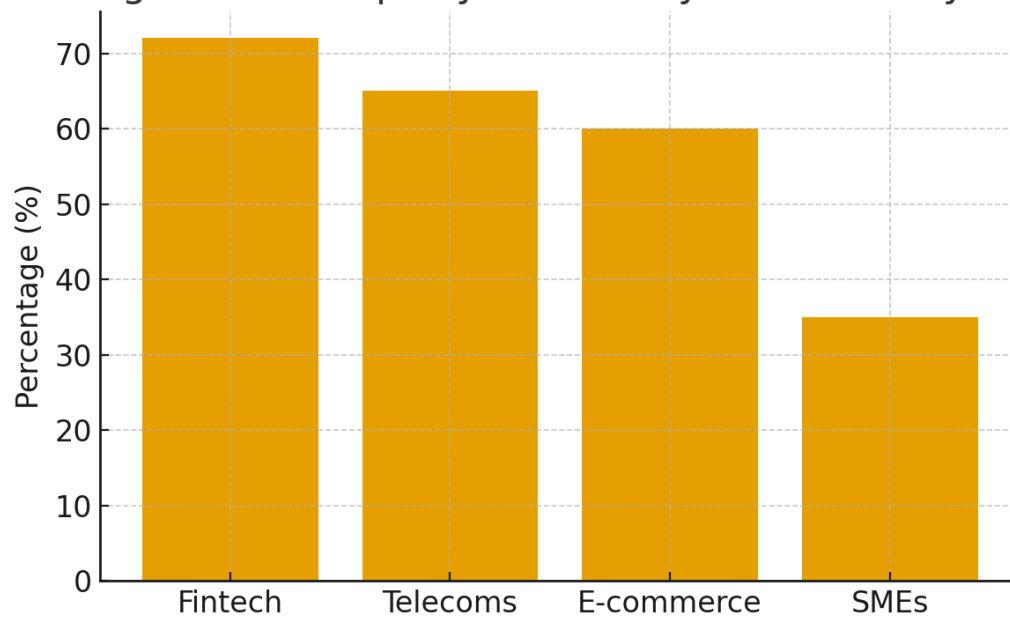


Table 2: Willingness to Adopt Cybersecurity Insurance by Sector

Sector	Willingness to Adopt CSI (%)
Fintech	72
Telecoms	65
E-commerce	60
SMEs	35

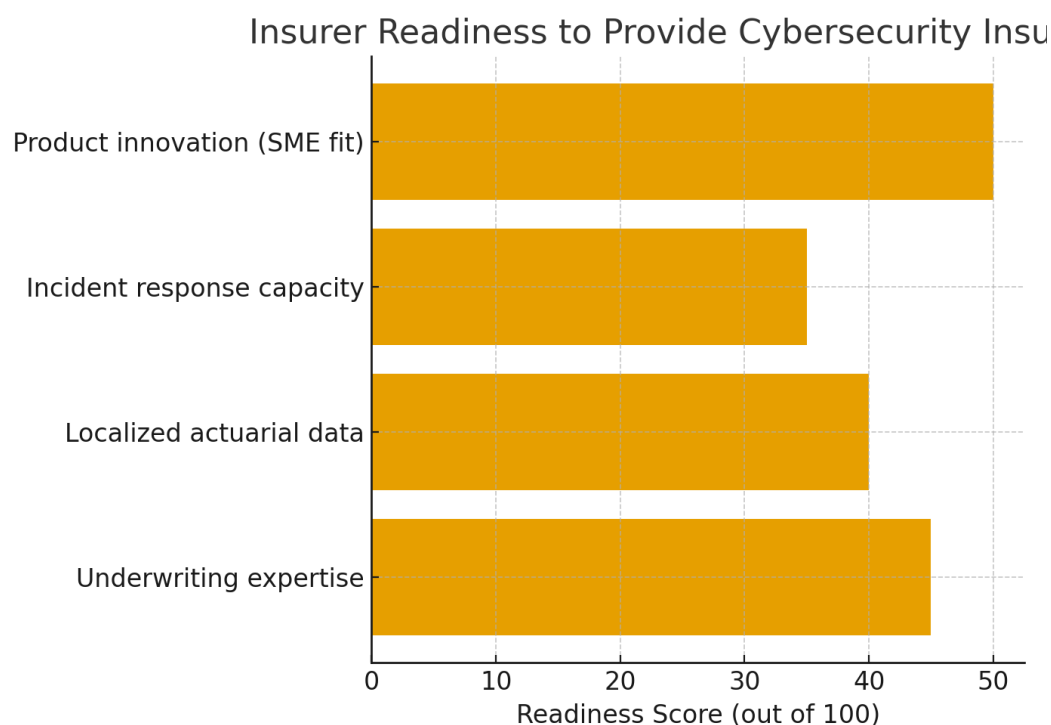
Willingness to Adopt Cybersecurity Insurance by Sec

Readiness of Insurers to Provide Cybersecurity Insurance Products

Analysis of responses from insurance sector participants highlights that insurer readiness remains limited. Respondents noted gaps in technical underwriting expertise, absence of localized actuarial data, and overreliance on foreign reinsurer templates. Furthermore, 71% of insurer respondents admitted that they currently lack the in-house technical teams necessary for cyber risk modelling and incident response coordination. While some insurers have launched pilot cyber cover packages, these are mostly targeted at large corporates, leaving a significant gap for SMEs.

Table 3: Insurer Readiness to Provide Cybersecurity Insurance

Readiness Dimension	Readiness Score (out of 100)
Underwriting expertise	45
Localized actuarial data	40
Incident response capacity	35
Product innovation (SME fit)	50



Measures for Developing Cybersecurity Insurance in Nigeria

Drawing on responses across organisations, several measures were proposed and endorsed to support CSI development. A majority (79%) of respondents recommended public awareness and education campaigns, particularly targeting SMEs. Another 68% emphasized the need for regulatory clarity and standardized policy guidelines, noting that inconsistent wordings and exclusions reduce buyer confidence. Insurers themselves highlighted the importance of access to affordable reinsurance and public–private data-sharing platforms. Interestingly, 54% of respondents supported the integration of value-added services such as forensic support, employee training, and PR response within CSI policies.

8. DISCUSSION

The findings reveal a paradox in Nigeria's emerging digital economy. On one hand, cyber risks are rising rapidly, reflected in the willingness of fintechs, e-commerce platforms, and telecoms to consider CSI. On the other hand, low awareness, affordability challenges, and insurer unpreparedness undermine broader adoption.

Quantitative results confirmed that awareness and demand significantly predict adoption intention, with awareness exerting a stronger effect. This suggests that education and sensitization campaigns could play a pivotal role in expanding CSI penetration. Thematic insights reinforce this, highlighting that SMEs remain largely excluded due to both cost and lack of product knowledge.

On the supply side, insurers demonstrate low readiness, constrained by technical capacity gaps, lack of local actuarial data, and limited product innovation. Without regulatory reforms, capacity building, and collaborative reinsurance arrangements, CSI will struggle to gain traction. These findings align with global evidence that emerging economies face structural and market readiness challenges in adopting CSI, but also suggest that Nigeria's digital-native sectors could act as early adopters and catalysts for wider uptake. The study's findings reinforce the central paradox in Nigeria's digital economy: while cyber risk exposure is growing rapidly, CSI adoption remains constrained by limited awareness, demand skepticism, and insurer readiness challenges. Higher awareness and demand among fintechs, banks, and e-commerce players highlight sectoral exposure as a key adoption driver. Conversely, SME reluctance reflects cost sensitivity and knowledge gaps, underscoring the importance of simplified, affordable CSI products and targeted awareness campaigns.

On the supply side, insurers' limited capacity and reliance on reinsurers mirror trends in other emerging markets. Without investment in training, local data registries, and reinsurance partnerships, insurers will struggle to expand coverage meaningfully. The absence of explicit regulatory frameworks perpetuates uncertainty, discouraging both buyers and sellers. Coordinated interventions—ranging from regulatory clarity, sectoral pilot programmes, fiscal incentives, to capacity building—could unlock wider CSI adoption in Nigeria.

9. CONCLUSION

This study examined the state of cybersecurity insurance (CSI) in Nigeria's emerging digital economy using both quantitative and qualitative evidence. The findings reveal that while awareness of CSI is moderate and concentrated in fintech, e-commerce, and telecommunications sectors, overall adoption remains low due to affordability barriers, limited understanding of product offerings, and insurer unpreparedness. Regression results confirmed that awareness and demand significantly predict adoption intention, underscoring the importance of sensitization and education in shaping market growth. On the supply side, insurers demonstrated limited readiness, citing challenges such as lack of actuarial data, inadequate technical capacity, and regulatory uncertainty. The study concludes that although Nigeria's digital economy is expanding rapidly, the development of CSI has not kept pace, leaving systemic vulnerabilities that could undermine trust, investment, and consumer confidence if unaddressed.

Recommendations

Strengthen Awareness and Market Education: Regulatory bodies, insurers, and industry associations should invest in nationwide sensitization campaigns, workshops, and targeted SME outreach to improve awareness and understanding of CSI. Emphasis should be placed on practical benefits, policy coverage, and affordability to increase adoption readiness.

Build Insurer Capacity and Regulatory Support: Insurers should enhance their technical underwriting expertise, leverage partnerships with global reinsurers, and invest in local actuarial data collection on cyber incidents. Regulators such as NAICOM should provide clear policy guidelines and frameworks that standardize CSI products, thereby boosting confidence among both insurers and insured organisations.

Develop Affordable and Sector-Specific Products: To address affordability concerns, insurers should design tiered CSI products tailored to different sectors—such as SMEs, fintechs, and e-commerce firms—with scalable premiums. Bundling CSI with value-added services (e.g., forensic investigation, employee training, and incident response support) could also enhance perceived value and encourage wider adoption.

REFERENCES

- AfChargeTech. (2025). *Cyber insurance in Nigeria: A growing necessity in 2025*. AfChargeTech. <https://www.afchargetech.com/cyber-insurance-in-nigeria-a-growing-necessity-in-2025>
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 40(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>
- Bukht, R., & Heeks, R. (2018). Defining and measuring the digital economy. *International Organisations Research Journal*, 13(2), 143–172. <https://doi.org/10.17323/1996-7845-2018-02-07>
- Check Point Research. (2025, August 13). *Nigeria recorded an average of 6,101 cyberattacks weekly in July 2025*. Technext24. [TechNext24](https://www.technext24.com/news/nigeria-recorded-an-average-of-6101-cyberattacks-weekly-in-july-2025)
- Deloitte Nigeria. (2025). *Nigeria's Cybersecurity Outlook 2025*. Deloitte Nigeria. <https://www.deloitte.com/ng/en/services/consulting-risk/perspectives/Nigerias-cybersecurity-landscape-in-2025.html>
- Insurance Journal. (2025, April 14). Cyber insurance market size expected to soar: Munich Re. *Insurance Journal*. <https://www.insurancejournal.com/news/national/2025/04/14/819668.htm>
- Munich Re. (2025). *Cyber insurance: Risks and trends 2025*. Munich Re. <https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html>
- NAIC (National Association of Insurance Commissioners). (2024). *Report on the cyber insurance market*. <https://content.naic.org/sites/default/files/cmte-h-cyber-wg-2024-cyber-ins-report.pdf>
- NAICOM. (2025). *Guidelines for insurtech operations in Nigeria* (effective Aug. 1, 2025). National Insurance Commission. <https://naicom.gov.ng>

- Nairametrics. (2023, June 7). Government agencies identify benefits of insurance cover for losses from cybercrime. *Nairametrics*.
<https://nairametrics.com/2023/06/07/government-agencies-identify-benefits-of-insurance-cover-for-losses-from-cybercrime/>
- Novatia Consulting. (2024). *Cyber insurance advisory in Nigeria*.
<https://novatiaconsulting.com/cyber-insurance-advisory-in-nigeria/>
- Ogunyemi, A. A. (2025). Cyber risks and the Nigerian business sector: A critical analysis of the emerging cyber insurance market in Nigeria [Abstract]. *ACU Journal of Social Sciences*. <https://ajss.acu.edu.ng/index.php/ajss/article/view/145>
- ThisDayLive. (2023, January 28). Cyber insurance is struggling for growth in Nigeria. *ThisDayLive*. <https://www.thisdaylive.com/2023/01/28/cyber-insurance-struggling-for-growth-in-nigeria/>
- Tokio Marine HCC. (2024). *2024 cyber market report* (white paper).
https://www.tmhcc.com/en-us/-/media/project/tokio-marine/tmhcc-us/documents/cplg_2024_white_paper.pdf
- 6WResearch. (2025). *Nigeria Cybersecurity Insurance Market (2025-2031): Trends, Outlook & Forecast*. 6Wresearch
- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, 17(5), 474–491.
- 0122INTERPOL. (2025). *2025 Africa Cyberthreat Assessment Report*. INTERPOL (as reported by Nairametrics).
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35–61.
<https://doi.org/10.1016/j.cosrev.2017.01.001>
- Nairametrics. (2025, June 29). *Nigeria ranks third in Africa for ransomware threat detections in 2024 – INTERPOL*.

- OECD. (2020). *Measuring the digital economy: A new perspective*. Organisation for Economic Co-operation and Development. <https://doi.org/10.1787/9789264221796-en>
- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1), 1–19. <https://doi.org/10.1093/cybsec/tyz002>
- ThisDayLive. (2023, January 28). *Cyber insurance is struggling for growth in Nigeria*. ThisDayLive. *THISDAYLIVE*
- UNCTAD. (2021). *Digital economy report 2021: Cross-border data flows and development*. United Nations Conference on Trade and Development. https://unctad.org/system/files/official-document/der2021_en.pdf
- Waliullah, M., Hossain George, M. Z., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). *Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review*. arXiv.
- Woods, D. W., & Simpson, A. C. (2017). Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, 2(2), 209–226.