Deloitte.

Nigeria Cybersecurity Outlook 2025

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

The year 2024 marked a pivotal shift in the global cybersecurity landscape, as escalating cyber threats pushed organisations to near breaking point. As predicted in the 2024 Nigeria Cybersecurity Outlook, ransomware attacks reached unprecedented levels, phishing scams grew more sophisticated, and insider threats surged amidst economic downturns. The rapid adoption of AI by both defenders and attackers further intensified this battle, elevating cybercrime to a formidable challenge that demanded constant vigilance and innovation.

As we look ahead to 2025, we envisage that the cybersecurity landscape will become increasingly dynamic and fraught with challenges. The battle between AI-powered attacks and AI-driven defenses will intensify, reshaping the tactics of bad actors and defenders alike. This publication explores key cybersecurity predictions for Nigeria in 2025, addressing emerging threats, evolving regulatory priorities, and strategies to foster a safer and more resilient digital ecosystem.

1 A race between AI-Powered attacks and AI-Powered defense

The adoption of Artificial Intelligence (AI) is revolutionizing the cybersecurity landscape, with AI-powered defense tools becoming indispensable in the fight against increasingly complex threats. Organisations are leveraging AI tools to enhance threat detection, automate incident response, and analyze patterns to identify risks early. These AI-driven solutions enable businesses to respond quickly and effectively, improving resilience by detecting anomalies, predicting potential attacks, and mitigating threats before they escalate.

On the flip side, the same technology is empowering cybercriminals. AI-powered attacks are making cyber threats more sophisticated, automated, and precise. Malicious actors are using AI to automate phishing campaigns, create polymorphic malware that evade detection, and craft hyper-realistic deepfakes.

This dual-use of AI creates a paradox. While it bolsters defense capabilities, it also amplifies the scale and precision of cyberattacks, moving them closer to pandemic-like proportions. In 2025, the race between AI-powered cyberattacks and AI-driven defense is expected to intensify, highlighting the urgent need for continuous adaptation and innovation. Organisations must embrace AI not only as a defensive measure but as an integral part of their broader cybersecurity strategy to stay ahead of increasingly sophisticated adversaries.

> "AI-powered attacks are making cyber threats more sophisticated, automated, and precise."

2 Increased Scrutiny on Cybersecurity Spending Amid Economic Pressures

As organisations grapple with economic pressures in 2025, the drive to reduce costs and seek innovative locally sourced cybersecurity solutions will take center stage. While this shift holds promise, it also carries inherent risks.

On one hand, the demand for affordable solutions, preferably be paid for in local currency could lead to security gaps and increased breaches since these solutions are not yet readily available and widely tested. On the other, it presents an opportunity for the growth of indigenous security tool developers who can offer tailored, cost-effective alternatives.

The rise of indigenous security tool developers in Nigeria introduces both opportunities and challenges. These local innovators, with their deep understanding of the unique threat landscape, are well-positioned to address specific needs. However, rapid development and deployment of these tools often come at the expense of rigorous testing and comprehensive threat intelligence. Without these critical safeguards, organisations may inadvertently introduce vulnerabilities into their security infrastructure, undermining the very defenses they seek to strengthen.

Organisations must adopt a strategic, forward-looking approach to cybersecurity investments. Rather than reactive, piecemeal solutions, businesses should focus on integrating cost-effective measures that align with their broader objectives. This entails careful evaluation of indigenous tools, thorough risk assessments, and maintaining a holistic view of their security posture. In 2025, the key to navigating the cybersecurity landscape lies in striking a delicate balance between innovation, cost-efficiency, and robust security. Organisations that manage to integrate these elements effectively will not only protect their digital assets but also position themselves as resilient players in a challenging economic climate.

The key to navigating the cybersecurity landscape lies in striking a delicate balance between innovation, cost-efficiency, and robust security.

3 Third-Party Risk will remain a growing concern

In 2024, several high-profile incidents exposed vulnerabilities in third-party networks, resulting in data breaches, financial losses, and operational disruption. The growing complexity of business ecosystems, where sensitive information is often shared among multiple partners, further amplifies these risks.

As Nigeria's digital economy continues to expand, third-party risks are becoming increasingly concerning. Cybercriminals frequently target the weakest links in the supply chain, exploiting gaps in third parties' security practices.

This challenge is exacerbated by the widespread adoption of cloud-based solutions, including financial applications, HR platforms, and document-signing tools, which are now commonplace across Nigeria. Additionally, the proliferation of APIs, which are critical for integrating applications and enabling seamless operations across entities, introduces new vulnerabilities. Poorly secured APIs can serve as entry points for attackers, allowing unauthorized access to systems and data. The interconnected nature of APIs means a single compromised integration can have a ripple effect across multiple systems, escalating the impact of an attack.

To address these risks, organisations must move beyond one-time checks and adopt continuous monitoring activities for third-party networks. This involves having complete API visibility, conducting thorough risk assessments, enforcing stringent contractual obligations, deploying automated real-time monitoring tools and ensuring protection from API to entire application and network infrastructure. Regular audits and closer oversight of third-party relationships will also play a vital role in building a resilient cybersecurity strategy, helping businesses mitigate third-party risks and navigate an increasingly interconnected digital landscape.

4 Data Protection Compliance and Enforcement Will Level Up

There appears to be a positive trajectory for data protection in Nigeria. A key initiative was the introduction of mandatory registration for Data Controllers and Processors, a move aimed at enhancing oversight. This is important especially as businesses continue to process large volumes of personal and sensitive information, which is increasingly targeted by cybercriminals.

The Nigeria Data Protection Commission has also intensified efforts to raise awareness about data protection with a notable step of having a brand ambassador to promote data protection across the country. Looking ahead to 2025, we foresee that data protection compliance and enforcement reaching new levels. Businesses will face stricter regulatory scrutiny, with steeper penalties for non-compliance. These actions are expected to elevate the standard for handling personal data, pushing organisations to adopt more robust compliance systems and greater transparency in data practices.

Organisations that view data protection from a “beyond-compliance” perspective will stand out. By embedding data protection into their core business practices, rather than simply meeting regulatory requirements, businesses will not only ensure compliance but also foster trust with their customers, safeguard their reputation, and mitigate potential risks associated with non-compliance. This forward-thinking approach will be key to differentiating organisations in a rapidly evolving regulatory landscape.

> Organisations that view data protection from a “beyond-compliance” perspective will stand out.

5 Identity Theft and Fraud Will Escalate

As digital transformation accelerates, identity theft and fraud are becoming increasingly pervasive in Nigeria, raising serious concerns for businesses and individuals alike. With the growing reliance on online services for banking, e-commerce, and communication, cybercriminals are leveraging advanced tools and tactics to steal personal information, financial data, and corporate identities.

According to the Nigeria Inter-Bank Settlement System (NIBSS) report released in 2024 , there were notable incidents involving fraudsters using techniques such as social engineering to gain unauthorized access to sensitive information and successfully performing account takeovers. The rapid adoption of digital payment systems, mobile banking, and e-commerce platforms in Nigeria has also fueled the growth of these crimes. With many businesses still working on enhancing their security infrastructure, criminals are finding new ways to exploit system weaknesses and gain access to consumers' financial information. Time is, therefore, of the essence.

In 2025, the upward trajectory of identity theft and fraud is expected to persist, placing personal data at even greater risk. Organisations must evolve their fraud prevention strategies by implementing advanced identity verification technologies and layered security measures, such as continuous behavioral analysis, risk-based access management, and AI-driven anomaly detection. Additionally, educating users about emerging threats like deepfakes and advanced phishing will be crucial in mitigating risks. A proactive and multi-faceted approach is essential for managing identity theft effectively and safeguarding the digital ecosystem.

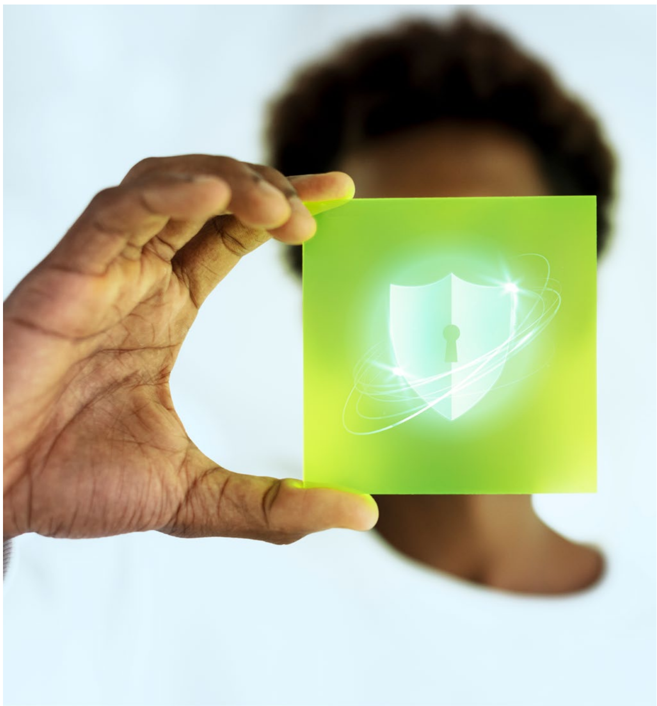
6 Rising Cyber Risks Will Make Cybersecurity Insurance the New Lifeline

The saying “cyberattacks are no longer a question of ‘if’, but a matter of ‘when’” has never been more accurate. According to Deloitte Global’s Future of Cyber survey in 2024, 25% of respondents from cyber-mature organisations reported 11 or more cybersecurity incidents in the past year, a 7% increase from the 2023 survey.

This underscores that even the most prepared organisations remain vulnerable to increasingly sophisticated cyber threats.

The rising frequency and complexity of cybercrimes have made cybersecurity insurance a vital tool for organisations’ cyber resilience. These specialized policies provide financial protection against incidents like data breaches, ransomware attacks, and third-party liabilities. While cyber insurance has been historically underutilized in Nigeria, businesses are now recognizing its critical role in mitigating the financial fallout of cyber threats.

In 2025, cyber insurance is expected to gain significant popularity in Nigeria. This shift will be fueled by high-profile cyber incidents, heightened regulatory pressures, and greater awareness of the benefits these policies offer. However, challenges such as high premiums, limited local expertise, and skepticism about coverage details may hinder widespread adoption. Overcoming these barriers will be essential to building trust and driving broader acceptance within Nigeria’s business ecosystem.



In 2025, cyber insurance is expected to gain significant popularity in Nigeria

7 Increased Perpetuation of Misinformation through Gen AI

The widespread adoption of Generative AI (Gen AI) is reshaping industries and economies worldwide, and Nigeria is no exception. From transforming customer service with AI-driven chatbots to enabling creative solutions in media, healthcare, and education, Gen AI has become a cornerstone of innovation in the country's digital economy.

However, this widespread integration is also amplifying cybersecurity and ethical concerns that could define 2025.

Cybercriminals are increasingly exploiting Gen AI's ability to mimic human communication and create hyper-realistic content. In a country already grappling with phishing and social engineering attacks, AI-generated fake emails, texts, and voice impersonations are poised to make scams virtually indistinguishable from legitimate communication. Data privacy concerns are also mounting as these AI models require extensive datasets for training, often involving sensitive personal or corporate information.

Beyond technical risks, Gen AI's potential to perpetuate bias and misinformation poses societal challenges. If left unchecked, biased AI outputs could result in unfair practices in critical areas like hiring and financial services, disproportionately affecting Nigeria's diverse population. As Gen AI adoption accelerates, a new wave of risks both known and unknown will emerge. Nigeria's ability to balance innovation with accountability will determine whether its digital transformation fosters progress or exacerbates vulnerabilities. The question remains: Are Nigerian businesses and regulators prepared for the wave of risks and opportunities that come with embracing Gen AI?

8 Cyber Talent Drain will Push Nigerian Businesses to Nurture Homegrown Experts

The cybersecurity talent shortage is a pressing global issue, but in Nigeria, it has reached a critical level. Over the past few years, the country has experienced a significant brain drain in its cybersecurity workforce, with many experts seeking opportunities abroad due to better pay, career growth, and stability.

This “Japa syndrome” has left businesses scrambling to find skilled professionals to secure their operations against growing cyber threats.

Forward-thinking organisations are now focusing on nurturing homegrown experts by investing in local capacity-building initiatives. Cybersecurity training programs, partnerships with universities, and in-house mentorship schemes are becoming common as companies work to develop talent from within.

As we look ahead to 2025, there is likely to be a greater emphasis on building sustainable talent pipelines. Businesses will need to double down on strategies that nurture and retain local expertise, while also exploring ways to attract Nigerian professionals in the diaspora back home. This would be a positive as we build the next gen cyber work force.

Businesses will need to double down on strategies that nurture and retain local expertise

Conclusion

The risk of cyber attacks reaching pandemic-like proportions is no longer hypothetical—it is an urgent reality. The rapid evolution of threats, fueled by AI advancements and the increasing complexity of digital ecosystems, demands immediate, coordinated action. Governments, businesses, and individuals must rise to the challenge, building resilient digital infrastructures capable of withstanding sophisticated cyber threats.

2025 cannot be a year of complacency. It must be a year defined by intentionality in cybersecurity. This means adopting proactive measures such as zero-trust frameworks, investing in AI-driven defenses, and fostering collaboration across regulatory bodies, private organisations, and global partners. Only through vigilance, innovation, and shared responsibility can we combat escalating cyber risks and unlock the promise of a secure, interconnected, and prosperous digital future.

Have a cyber-secure 2025!

Contacts

Tope Aladenusi

Risk Advisory Leader,
Deloitte West Africa
+234 (02) 1 9041730
taladenusi@deloitte.com.ng

Funmilola Odumuboni

Partner Risk Advisory,
Deloitte West Africa
+234 (02) 19041882
fodumuboni@deloitte.com.ng

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte & Touche, a member firm of Deloitte Touche Tohmatsu Limited, is a professional services organisation that provides audit, tax, consulting, business process solutions, financial advisory and risk advisory services.
Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 457,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

www.facebook.com/DeloitteNigeria www.twitter.com/DeloitteNigeria