Deloitte.

Together makes progress

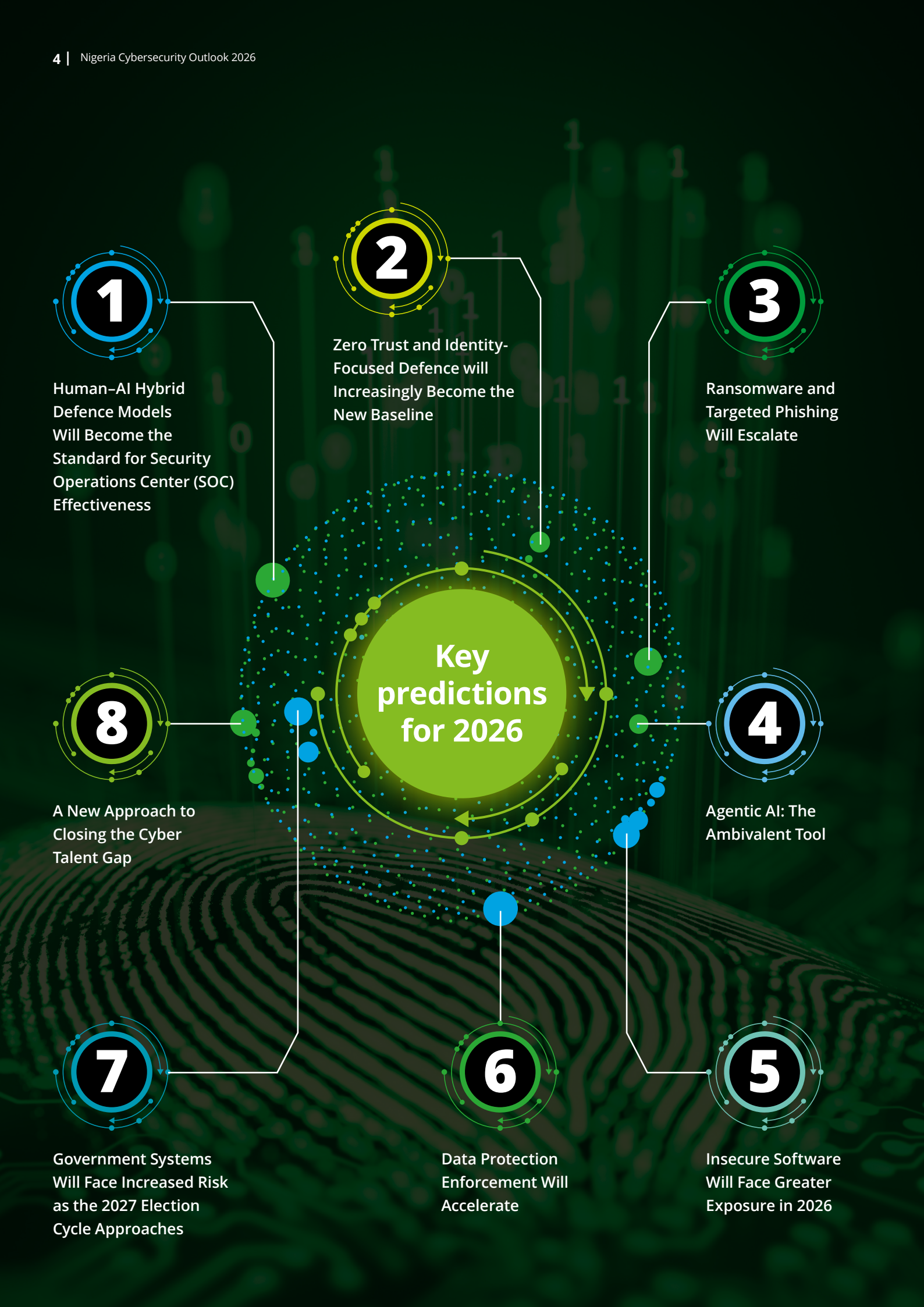
Nigeria Cybersecurity Outlook 2026

January 2026

Introduction

In 2025, Nigeria's digital economy grew at remarkable speed — and cybercrime kept pace. Organisations across sectors dealt with a noticeable increase in attacks, ranging from AI-powered scams and ransomware incidents to identity fraud affecting everyday users. Over the course of the year, a clear pattern emerged: attackers were becoming more sophisticated and faster-moving, while regulators were signalling that leniency was coming to an end. The introduction of the Nigeria Data Protection Act (NDPA) General Application Implementation Directives (GAID) reflected this shift, moving the conversation from intention and awareness to accountability and enforcement.

Looking ahead to 2026, these pressures are unlikely to ease. Cybercriminals are expected to rely more heavily on automation and AI-driven tools, while regulators place greater emphasis on enforcement rather than guidance. Cybersecurity will increasingly be viewed as more than a technical concern — it will shape national security, public trust, and organisations' ability to operate without disruption. Key developments expected in 2026 include closer collaboration between people and AI in defence, a shift toward zero-trust and identity-focused security, heightened ransomware and election-related risks, and a growing need for clearer AI governance and ongoing development of cybersecurity skills. Below are the details of some of the events that will shape cybersecurity in Nigeria in 2026.


Key predictions for 2026
1
Human–AI Hybrid Defence Models Will Become the Standard for Security Operations Center (SOC) Effectiveness
2
Zero Trust and Identity-Focused Defence will Increasingly Become the New Baseline
3
Ransomware and Targeted Phishing Will Escalate
4
Agentic AI: The Ambivalent Tool
5
Insecure Software Will Face Greater Exposure in 2026
6
Data Protection Enforcement Will Accelerate
7
Government Systems Will Face Increased Risk as the 2027 Election Cycle Approaches
8
A New Approach to Closing the Cyber Talent Gap

Human–AI Hybrid Defence Models Will Become the Standard for Security Operations Center (SOC) Effectiveness

In the 2025 Nigeria Cybersecurity Outlook, we predicted the growing competition between AI-driven attacks and AI-enabled defences. Since then, it has become increasingly clear that the pace and complexity of modern threats exceed what either humans or machines can manage alone. Many organisations are only beginning to recognise this reality. Today's attackers already use AI to gather intelligence, evade detection, and execute attacks at scale, often overwhelming traditional security teams.

At the same time, techniques such as highly realistic fake voices, videos (deep fakes), and messages have made it harder to rely on static rules or legacy detection methods. Attackers now use AI to automate reconnaissance, avoid detection, and launch attacks much faster than before. In 2026, the most effective security operations will be those that deliberately combine human expertise with machine capability. AI will take on continuous monitoring, anomaly detection, and alert prioritisation, while human professionals provide judgment, context, and informed decision-making based on business realities.

Deloitte's Future of Cyber survey 2024 notes that AI works best when it supports SOC analysts instead of replacing them. By reducing alert fatigue and background noise, AI allows security teams to focus on what truly matters. Ultimately, the advantage will not come from technology alone, but from how well organisations integrate it with human insight. When balanced correctly, this partnership enables faster responses without sacrificing control or understanding.

2

Zero Trust and Identity-Focused Defence will Increasingly Become the New Baseline

Cyber attackers are increasingly targeting people's identity (user access) rather than technical system flaws. Instead of forcing their way through technical defences and controls, they focus on stealing credentials, manipulating employees, and abusing legitimate access. As predicted in the 2025 Nigeria Cybersecurity Outlook we saw a sharp rise in identity theft and fraud fueled by social engineering, account takeovers, and more convincing forms of digital deception. As a result, security models built around protecting a network's perimeter are proving insufficient since "authorised access" is now seen to be used to perform malicious activities.

In response, more organisations are moving toward a "Zero Trust" approach, where no user or system is automatically trusted — even when operating inside the network. This shift was already becoming evident in 2025 and will continue to gain momentum.

In 2026, Zero Trust and identity-based controls are expected to move from strategic roadmaps into day-to-day operational lifelines. Every access request will need to be assessed based on identity, intent, and behaviour. Permissions will be tightly scoped and adjusted dynamically as risk changes. Strong authentication, behavioural monitoring, and disciplined privilege management will become foundational rather than optional as attackers increasingly gain entry by compromising legitimate users rather than breaching network boundaries.

Rising insider risk, credential theft, and the expanding role of human and machine identities also show that Zero Trust with identity-centric defense will increasingly become the baseline for robust cybersecurity in 2026. Organisations that move early will be better positioned to reduce fraud and misuse. Those that delay are likely to find themselves increasingly exposed as identity becomes the primary attack vector.

Ransomware and Targeted Phishing Will Escalate

In 2026, ransomware and phishing attacks are likely to increase across Nigeria as more services, payments, and records continue to move online. This shift creates greater opportunities for financial crime and disruption. At the same time, the new tax requirements such as e-invoicing and real-time transaction reporting will push more businesses to digitize how they operate and monitor their activities. Tools and techniques that were once used only by cyber criminals are now widely available, making it easier for less experienced attackers to launch effective campaigns and expanding the risk well beyond just large organisations.

Phishing campaigns, in particular, are becoming more convincing. With the help of AI, attackers can generate emails, messages, and voice notes that closely resemble communication from trusted colleagues, banks, suppliers, or regulators. Once attackers gain access to a user's account, ransomware operators can move quickly — not just to lock systems but to quietly steal customer data, threaten exposure, and pressure organisations into paying ransoms. Recent incidents in banks, fintech firms, and government agencies demonstrate that this pattern is already emerging locally, often spreading faster than teams can respond.

Crucially, these threats are no longer confined to large organisations. Small and medium-sized businesses, schools, hospitals, and government agencies are increasingly targeted, especially where security resources/budget is limited. Building resilience does not always require complex solutions. Consistent staff awareness, stronger account protection, basic monitoring for unusual activity, and clear recovery plans can significantly reduce impact. Organisations that prepare early are far more likely to recover quickly. Those that assume they are unlikely targets may find that a single convincing message is enough to cause serious disruption.

4

Agentic AI: The Ambivalent Tool

A new class of artificial intelligence, often referred to as Agentic AI, is beginning to reshape the technology landscape. Unlike earlier systems designed to support specific tasks, these tools can operate more independently — breaking down objectives, making decisions, and taking actions with limited human input.

The increased autonomy of Agentic AI means it can be used in both beneficial and malicious ways. Agentic AI can be highly valuable and potentially dangerous (in the wrong hands). On the defensive side, it can monitor environments continuously, identify unusual behaviour in real time, and respond far more quickly than traditional processes allow. Used well, this can significantly improve detection accuracy and response speed by learning from evolving threat patterns and adapting controls dynamically. However, the same capabilities can also be exploited. Attackers could deploy autonomous AI to identify weaknesses, generate convincing fake content, and execute multi-stage intrusions with minimal human oversight and speeds that outpace conventional defences.

In 2026, Agentic AI is likely to become a decisive factor in determining whether digital systems are resilient or dangerously exposed. The way organisations deploy and govern Agentic AI will have a direct impact on their security posture. The difference will lie in oversight, control, and intent. In some cases, autonomous AI will prevent incidents that human teams could not manage alone. In others, poor governance could enable breaches that unfold too quickly to contain. For Nigerian organisations, the challenge will be adopting this technology carefully — strengthening defences without inadvertently increasing risk.

Insecure Software Will Face Greater Exposure in 2026

We live in a fast-paced world where businesses are under constant pressure to build the best app or deliver the most compelling solution in order to capture an increasingly distracted customer base. Under this pressure, we have seen several high-profile missteps, where applications and services were rushed into deployment with little or no security testing, only to be withdrawn shortly after because attackers were able to exploit basic security flaws.

At the same time, the continued proliferation of technology systems has driven a sharp rise in the use of APIs, cloud platforms, and other shared services that support business growth and economic development. While these technologies enable speed and scale, they also expand the attack surface when security is not treated as a core requirement.

As this pressure intensifies in 2026, organisations that fail to prioritise basic secure software development practices may pay a high price. Application hacking is not new and, on its own, may not warrant special attention. However, the introduction of AI and the widespread use of APIs, coupled with the speed, precision, and scale of recent attacks, point to a clear escalation of these risks in 2026 and beyond.

The response does not require exotic solutions; it requires a return to fundamentals. Security must be considered at the design stage, not added as an afterthought. Applications should undergo proper security testing before deployment. Test and production environments must be strictly separated and protected with strong access controls. Version control should be carefully managed to ensure that the correct, remediated code is what ultimately goes live. Finally, live environments should be tested regularly, with remediation actions tracked and closed out diligently.These may seem like basic practices, but in 2026 and beyond, they will increasingly become the true differentiator between organisations that remain resilient and those that repeatedly find themselves exposed.

6

Data Protection Enforcement Will Accelerate

In 2025, many organisations acknowledged the new data protection requirements and the need for stronger controls, but practical implementation often lagged behind policy statements. Documentation was produced, assessments were planned, Data Protection Impact Assessments (DPIAs) appeared on project checklists and compliance was discussed, yet meaningful operational change was uneven. At the same time, the EU Artificial Intelligence Act sent a strong global signal that the use of AI will not remain unregulated. Other global developments have also made it clear that governments are growing more concerned about how AI systems affect individuals and decision-making.

In 2026, enforcement is expected to intensify. Regulators are likely to move beyond awareness campaigns and begin asking more detailed and demanding questions. Organisations using AI to process personal data or influence outcomes for individuals will face closer scrutiny, particularly in sectors such as finance, telecommunications, and healthcare. Organisations depending largely on cloud AI platforms or third-party AI services would also be in the radar. Assertions of compliance will no longer be sufficient — evidence will be required.

As a result, data privacy and AI governance will need to be embedded into everyday operations. Organisations will need a clear understanding of how personal data is collected, used, and shared along their value chain. Automated decisions must be transparent, documented, and defensible. Boards and executives will require better visibility and clearer accountability. Those that invest early in robust governance will be better positioned to innovate with confidence. Those that delay risk enforcement action, reputational harm, and loss of trust.

Government Systems Will Face Increased Risk as the 2027 Election Cycle Approaches

As Nigeria approaches the 2027 elections, government digital systems are likely to attract increased attention from cyber attackers. Election periods tend to heighten political and social tension, making Government and public services appealing targets for disruption or interference. With more public services now being delivered digitally, the attack surface has expanded significantly.

This risk is compounded by the continued reliance on older technologies in parts of the public sector and uneven security controls across institutions. Attackers may focus on voter records, identity databases, or other critical government systems to push their political ideologies. In many cases, the objective may not be a complete shutdown, but confusion, delays, or doubt around official information during a sensitive period.

Protecting critical digital infrastructure will therefore become a matter of national priority. Keeping essential services running, protecting the election process, and maintaining public trust will require better cooperation and stronger, more reliable systems across government. The period leading up to 2027 will be a crucial test of Nigeria's ability to protect and manage its digital systems effectively.

8

A New Approach to Closing the Cyber Talent Gap

The shortage of cybersecurity professionals has moved beyond a recruitment challenge to become a broader economic and national security concern. With about 4.8 million jobs unfilled worldwide, according to the 2025 ISC2 Cybersecurity Workforce study, there has been a big challenge filling critical cybersecurity role in Nigeria especially with the increased search for greener pastures abroad by citizens. This shortage affects organisations' cyber incident response efforts, weakens resilience, and increases the likelihood of serious disruption.

Traditional solutions have proven insufficient. Universities struggle to keep pace with industry needs, certifications often focus on fundamentals rather than real-world application, and competition on salaries simply redistribute talent among large organisations. Smaller institutions are frequently left without viable options.

To close this gap, we need to explore new, scalable solutions and everyone has a part to play. Organisations need to play the long-term game by investing in education and skills development through partnerships with tertiary institutions and tech hubs to co-create industry-relevant curricula, sponsor certifications, run bootcamps and graduate trainee programmes. Building strong local talent pipelines via internships to identify and recruit early-stage talent and supporting continuous learning through structured mentorship to grow junior professionals into experts, will need to be done proactively. At the same time, organisations need to rethink how they attract and deploy talent by adopting flexible hiring practices that focus on "potential" rather than solely on experience or certifications.

In the short term, outsourcing and partnerships can help bridge gaps, while automation and AI take on routine tasks and support leaner teams. Together, these measures offer a more sustainable path toward building capability and resilience. It is no longer a case of waiting for someone else to do it everybody needs to proactively take on this task for the national good.

Conclusion

2026 should not be approached as a simple continuation of past practices. It represents a turning point — a year in which cybersecurity must be fully integrated into business strategy, workforce planning, technology investment, and public policy. Organisations that act with urgency and clarity will be better positioned to reduce risk and strengthen confidence in Nigeria's digital economy. In an environment where trust is increasingly digital, cybersecurity will remain central to resilience, business growth, and national progress.

Have a cyber-resilient 2026.

Contacts

Tope Aladenusi
Africa Cyber Leader,
Deloitte Africa
+234 1 9041730
taladenusi@deloitte.com.ng

Funmilola Odumuboni
Partner, Cyber
Deloitte Africa
+234 1 9041882
fodumuboni@deloitte.com.ng

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845