CYBER RISK BRIEF

Nigeria's cyber threat picture 2026: what leaders should prioritise

Nigeria's national incident-response authority has warned of rising high-impact attacks driven by phishing, ransomware, business-email compromise and data breaches. Leadership attention should now move from awareness to evidence of control and recovery.

Foxtrot Shield Intelligence Team 27 June 2026 7 minute read

> **EXECUTIVE ASSESSMENT**
>
> The threat picture is shaped by scalable criminal services, AI-assisted deception and persistent control weaknesses. Most organisations do not need a more dramatic threat forecast; they need confidence that identity, payment, patching, backup, incident-response and third-party controls work under pressure. Cyber resilience is an operating capability, not a technology purchase.

What the national warning highlights

ngCERT rated the observed risk and potential damage as high and identified financial services, telecommunications, government, healthcare and other critical infrastructure among the particularly exposed sectors. The warning also notes that cybercrime-as-a-service and AI-enabled techniques allow attackers to operate at greater scale.

Phishing and credential theft

Deceptive messages and sign-in pages remain an efficient route into email, cloud, payment and business systems.

Business-email compromise

Attackers exploit trusted accounts, executive impersonation and payment-process weakness to redirect funds or sensitive information.

Ransomware and extortion

Criminal groups combine system disruption with data theft, increasing operational, legal, reputational and recovery pressure.

Data breaches

Weak access control, unpatched systems, third parties and misconfiguration can expose personal, commercial and operational information.

The regulatory direction is also becoming clearer

In March 2026, the Central Bank of Nigeria deployed a Cybersecurity Self-Assessment Tool for regulated institutions. Its scope includes governance, risk management, technology and third-party controls, incident response and operational resilience. Although the tool is sector-specific, those themes provide a useful indication of the evidence mature organisations should expect to produce.

Seven priorities for leadership

01

Make cyber risk an executive responsibility

Assign accountable leadership, define risk appetite and review material exposure, incidents, exceptions and recovery capability at an appropriate governance forum.

02

Protect identity and email

Use strong multifactor authentication, remove dormant accounts, restrict privilege, monitor suspicious sign-ins and strengthen controls around mailbox and payment-rule changes.

03

Harden payment and instruction verification

Require independent confirmation for new beneficiaries, changed bank details, unusual urgency and high-risk instructions—even when the request appears to come from a senior leader.

04

Reduce exploitable exposure

Maintain a current asset inventory, patch internet-facing systems quickly, remove unsupported services and validate security configuration.

05

Prove recovery works

Keep protected backups, define minimum recovery priorities and test restoration under realistic time pressure. A backup that has not been restored is an assumption.

06

Prepare for the first hours

Give technical, legal, communications, leadership and operational teams clear authority, contact routes and decision thresholds for a suspected incident.

07

Manage third-party risk

Identify vendors with privileged access, sensitive data or operational dependency. Set minimum controls, notification expectations and contingency arrangements.

Questions that demand evidence

Which systems and identities would cause the greatest harm if compromised?

Can the organisation detect and contain a compromised email account quickly?

When was a critical backup last restored successfully?

Who can authorise shutdown, isolation, external support and public communication?

Which suppliers could interrupt operations or expose sensitive data?

How are urgent payment changes independently verified?

What evidence supports management's view of cyber readiness?

> **FOXTROT SHIELD PERSPECTIVE**
>
> Leaders should be cautious of maturity claims based only on policies, tools or training completion. Strong assurance comes from tested controls, realistic exercises, recoverable systems and clear evidence that people can make sound decisions during an incident.

PRIMARY SOURCES

ngCERT: Escalating Cybersecurity Threats and Ongoing Attacks Targeting Organisations in Nigeria, 30 April 2026

Central Bank of Nigeria: Cybersecurity Self-Assessment Tool and 2026 regulatory reforms

Nigeria Data Protection Commission: breach reporting and data-controller responsibilities