



Heirs Technologies

2026

INDUSTRY REPORT

AFRICA'S CYBERSECURITY LANDSCAPE

With strategic focus on Nigeria, Kenya and South Africa

Contents

Foreword	3
Executive Summary	4
Introduction	6
1.1 The Cybersecurity Imperative: Sub-Saharan Market	6
1.2 Objectives of the Report	7
1.3 Research Methodology	7
2.0 Threat Landscape	9
2.1 Technical Vectors vs. Criminal Offenses: Deconstructing African Telemetry	10
2.1.1 Technical Entry Vectors	10
2.1.2 Finalised Criminal Case Types	11
2.2 High-Velocity Financial Fraud & Credential Exploitation	12
2.2.1 Key Vectors Shaping the Nigerian Risk Profile	12
2.3 Sector-Specific Vulnerabilities: Banking, Telecoms, and Critical Infrastructure	13
3.0 AI and the Evolving Threat Environment	16
3.1 Weaponisation of AI: Attack Metrics & Vector Breakdown	17
3.2 Generative AI Risks: Shadow IT and Data Exposure	18
3.3. Defender Strategies: AI-Driven Monitoring & SOC Modernisation	18
3.4. Operational SOC Capabilities and Workforce Asymmetry	19
4.0 Ecosystem Maturity & Regulatory Landscape	21
4.1 Nigeria's Institutional Readiness: NDPA, CBN Directives, and Sectoral Mandates	22
4.2. Regional Regulators	24
4.3. National Critical Infrastructure Preparedness Deficit	24
4.4. Enterprise Operational Compliance & Friction Points	26
5.0 The OEM & Global Vendor Gap (Addressing the SME Market)	28
5.1. The SME Operational Gap: Realigning Enterprise Security Tools for Local Realities	28
5.2. Supply Chain Cyber Risk & Procurement Integration	29
5.3. The Local Managed Solution Opportunity: The Case for SOC-as-a-Service	31

6.0 Technology, Infrastructure & Managed Services Opportunity	33
6.1. Enterprise IT Trends & the Multi-Cloud Threat Surface	34
6.2 Market Opportunity	34
6.3. The Transition from Point Solutions to Unified SOC-as-a-Service	35
7.0 Talent, Capacity & Workforce Pipeline	37
7.1. Structural Drivers of the African Cyber Talent Deficit	38
7.2. Bridging the Pipeline: Public Initiatives vs. Private-Sector Academies	38
7.3. Enterprise Retention Strategies and the Hybrid Talent Operating Model	39
8.0 Strategic Outlook & Recommendations	41
8.1 Forward Projections (2027–2028)	41
8.2 Grouped Actionable Roadmap	41
8.2.1 Action Plan for Enterprise Leaders & Chief Information Security Officers (CISOs)	41
8.2.2 Action Plan for Policymakers & Regulatory Authorities	42
8.2.3 Action Plan for Technology Investors & Infrastructure Developers	42
8.3 Conclusion	43
References	44
Contributors	46
About Heirs Technologies	46

Foreword

Every time an institution goes digital, it expands what is possible. It also expands what is at risk.

Africa's digital economy is no longer emerging. It is here. Instant payment rails are processing millions of transactions daily. Mobile money platforms are reaching populations that formal banking never could. Cloud infrastructure is enabling institutions to scale at a pace that would have been unthinkable a decade ago, and this digital leap has fundamentally redefined our risk exposure. As economic value moves online, so does the urgency to protect it.

Cybersecurity is now one of the core determinants of national economic sovereignty, financial stability, and institutional trust. Over 55% of cybercrime cases across Africa now incorporate artificial intelligence. Ransomware groups are targeting port logistics and payment switches. Deepfake fraud surged sevenfold in a single year. The same infrastructure powering Africa's growth has become its most consequential vulnerability.

The response cannot simply be imported from foreign playbooks. Global security tools often struggle against local macroeconomic volatility,

currency fluctuations, and regional attack vectors that require context they were not built for. Building lasting resilience means designing, deploying, and scaling local solutions such as carrier-neutral data centres, domestic SOC-as-a-Service architectures, and identity-centric defence frameworks built for how African institutions actually operate.

Realising that vision demands deliberate, unified leadership. Regulators must enforce clear, harmonised standards. Enterprise leaders must embed continuous security operations into the fabric of their organisations, and we must invest boldly in our human capital, closing the continent's skills deficit through practical, hands-on training that produces analysts, not certificates.

At Heirs Technologies, we believe Africa's digital expansion must be built on an unshakeable foundation of trust and resilience. Defending Africa's digital gains is not separate from building them. It is the condition on which they last.



Obong Idiong
CEO, Heirs Technologies

Executive Summary

Africa's rapid digital economic expansion has made cybersecurity a critical determinant of financial stability and national economic sovereignty. Focusing on Sub-Saharan Africa as the primary growth engine, this analysis zones in on Nigeria as the continental anchor market alongside comparative benchmarks in South Africa and Kenya. Across these hubs, over 55% of observed cybercrime cases incorporate artificial intelligence to power hyper-personalised phishing, deepfake impersonation, and automated session token theft. Global research indicates that AI-crafted phishing lures achieve click-through rates as high as 54% compared to 12% for manual attacks, creating severe operational exposure across financial institutions and digital infrastructure.

This threat environment is compounded by macroeconomic headwinds and accelerating regulatory enforcement. Foreign software platforms priced in US Dollars or Euros create extreme budget instability during local currency devaluations, forcing African enterprises to adjust deployment scopes or leave security tools underutilised. Simultaneously, regulators are tightening statutory oversight. In Nigeria, active enforcement under the Nigeria Data Protection Act and the Central Bank of Nigeria directive requiring domestic payment data to be hosted locally by 1 January 2027 is compelling institutions to align hybrid cloud

architectures with strict data sovereignty mandates.

In response to foreign exchange volatility and compliance pressures, African enterprises are consolidating fragmented point solutions into unified, local-currency security frameworks. By pivoting toward carrier-neutral data centers and Managed Detection and Response (MDR) delivered via local Security Operations Center as a Service (SOCaaS) models, organisations obtain round-the-clock threat monitoring, real-time behavioural analytics, and rapid incident response without exposing procurement budgets to foreign currency risk.

Sustaining this transition requires resolving the continent's severe human capital bottleneck. Survey data reveals that 63% of Sub-Saharan African organisations lack critical cybersecurity skills, representing one of the highest technical capacity deficits globally. Closing this gap requires structured collaboration between public skilling initiatives, academic institutions, and private security academies that offer practical cyber range experience. Over the 2027–2028 horizon, resilient African enterprises will insulate operational budgets from currency shocks, deploy localised threat detection engines, and adopt hybrid co-managed security architectures.

01

Introduction



01. Introduction

Africa’s rapid digital transformation is driving a fundamental shift across enterprise commerce, financial systems, and public administration. The expansion of instant payment switches, 5G networks, and hyperscaler cloud regions enables institutions to scale rapidly, but it also broadens the continent's attack surface, making cybersecurity central to economic resilience.

While threat vectors manifest continent-wide, this report focuses on Sub-Saharan Africa as the primary engine of digital financial expansion. Within the region, Nigeria serves as the anchor market due to its position as one of Sub-Saharan Africa's largest fintech and payment processing hub, characterised by high transaction velocity and rapid digital adoption benchmarked against South Africa (legacy enterprise and cloud data centers) and Kenya (East Africa's mobile financial gateway).

Reflecting this expansion, Sub-Saharan Africa's cybersecurity market is projected to grow from \$0.68 billion in 2025 and \$0.76 billion in 2026 to \$1.42 billion by 2031 (13.3% CAGR). Capital flows into the sector are currently being sustained by ongoing commercial digitalisation, regional data center builds, and mandatory privacy enforcement.

1.1 The Cybersecurity Imperative: Sub-Saharan Market

Enterprise connectivity across Sub-Saharan Africa is outpacing traditional perimeter security, compelling institutions to adopt zero-trust architectures and continuous threat monitoring.

Nigeria: Valued at \$230 million in 2025 and \$253 million in 2026, Nigeria’s cybersecurity market is projected to reach \$414 million by 2031 (10.3% CAGR), driven by digital payments adoption, strict NDPA compliance, and 5G network expansion.

South Africa: Growing from \$290 million in 2025 to \$330 million in 2026, South Africa’s cybersecurity market is expected to hit \$590 million by 2031 (12.7% CAGR) as enterprises modernise legacy networks and comply with Protection of Personal Information Act (POPIA) breach reporting.

Kenya: Estimated at \$60 million in 2024 and \$67 million in 2026, Kenya's cybersecurity market is projected to reach \$90 million by 2031 (5.8% CAGR), driven by national framework updates and mobile financial protection.

Sub-Saharan Africa & Regional Focus Markets Overview

Region	2025 Market Size	2026 Market Size	2031 Forecast (CAGR)
Africa	\$0.68 Billion	\$0.76 Billion	\$1.42 Billion (13.26% CAGR)
South Africa	\$290 Million	\$330 Million	\$590 Million (12.71% CAGR)
Nigeria	\$230 Million	\$253 Million	\$414 Million (10.32% CAGR)
Kenya	\$60 Million (2024)	\$67 Million (Est.)	\$90 Million (5.81% CAGR)

Source: [Mordor Intelligence](#) and [Bluewave Consulting](#)

1.2 Objectives of the Report

This report delivers an evidence-based evaluation of Africa's cybersecurity ecosystem, combining a primary analytical focus on Nigeria with comparative benchmarks from Kenya and South Africa.

Specifically, this report aims to:

- Analyse attack vectors and sector vulnerabilities across Banking, Fintech, Telecoms, Critical Infrastructure, and SMEs.
- Examine how Generative AI and automated attack frameworks alter threat actor workflows.
- Benchmark regulatory enforcement (NDPA, POPIA, DPA 2019) and enterprise compliance postures.
- Highlight operational mismatches with foreign security tools and the opportunity for local Managed Security Services (MSSPs)
- growth trajectories across cloud security and workforce development pipelines.
- Deliver actionable roadmaps for enterprise leaders, CISOs, policymakers, and investors.

1.3 Research Methodology

This study deploys a dual quantitative and qualitative research framework to assess the Sub-Saharan African cybersecurity landscape. The methodology evaluates core operational domains, including threat telemetry, AI weaponisation and defense, regulatory maturity, infrastructure opportunities, OEM software dynamics, and the talent pipeline, serving as an executive resource for security leaders, policymakers, and enterprise decision-makers.

The quantitative component relies on secondary source data to identify structural trends and multi-year changes across the continent's threat landscape. Global and regional threat telemetry was synthesised from industry publications and threat intelligence reports, including those from Kaspersky, Mastercard, Microsoft, Check Point, INTERPOL, Deloitte, and PwC.

The qualitative component gathered expert perspectives through structured interviews with key stakeholders across the ecosystem, including Chief Information Security Officers, technology directors, legal counsel, managed security service providers, and workforce leads. These qualitative insights provided operational context to explain underlying telemetry, validate quantitative findings, and detail enterprise responses to regulatory directives, foreign-currency software constraints, and talent retention challenges across Africa.

02

Threat Landscape



02. Threat Landscape

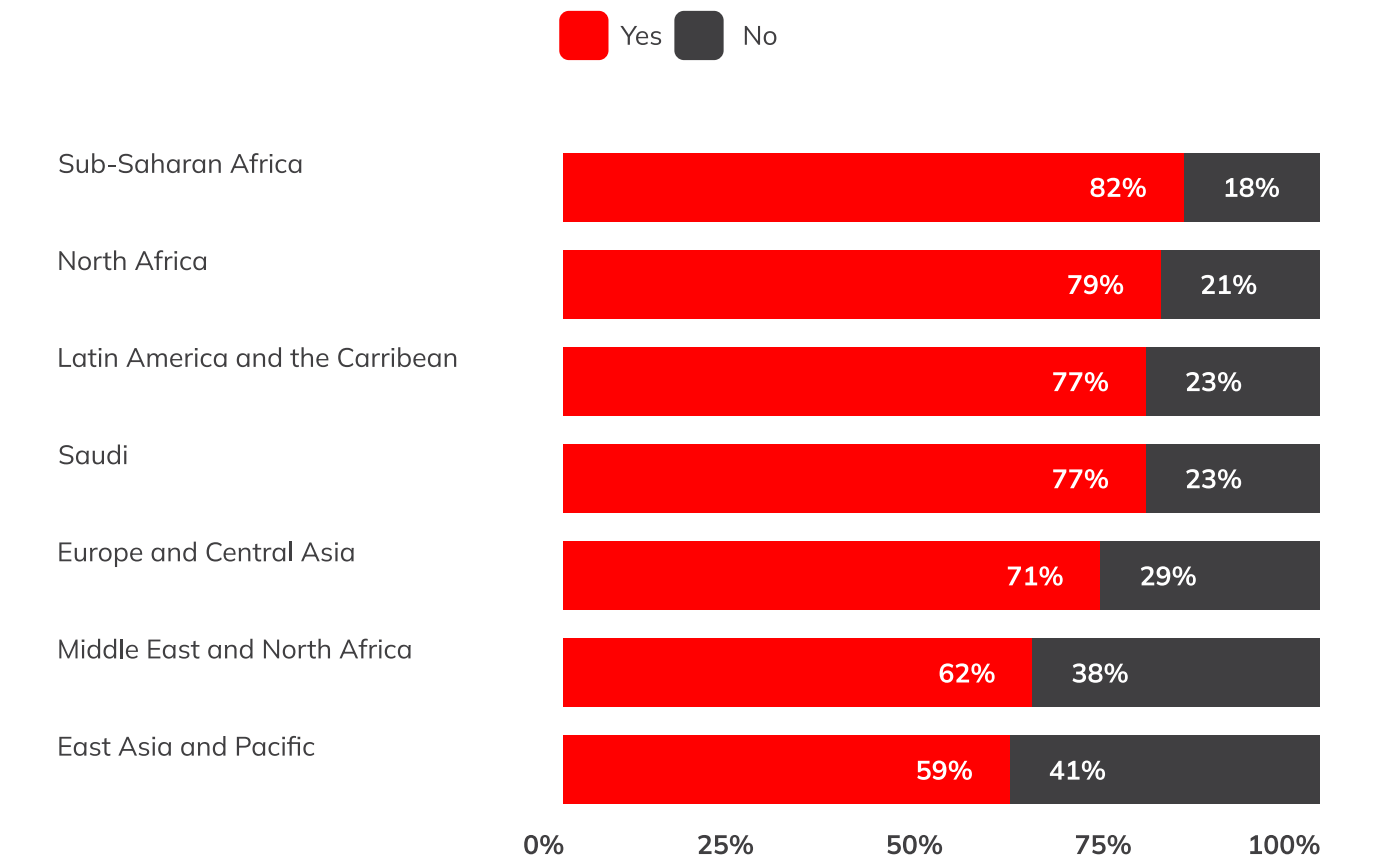
Africa’s digital ecosystem is currently operating at the unique intersection of rapid digital adoption and high structural vulnerability. While digital financial inclusion, mobile money platforms, and cloud infrastructure continue to scale across Sub-Saharan Africa, threat actors have adapted their tactics to exploit operational gaps, legacy technologies, and identity verification weaknesses.

Between 2023 and 2026, these systemic vulnerabilities manifested in high-profile attacks across the continent. In West Africa, threat actors increasingly bypassed traditional network perimeters to target payment switches and fintech API integrations, as evidenced by multi-million-Naira unauthorised transaction exploits at major

payment gateways such as Flutterwave and cryptocurrency platforms such as Patricia. Concurrently, East and Southern African financial networks faced severe surges in mobile app manipulation, SIM-swapping, and credential-stuffing attacks, while ransomware groups expanded operations to target cloud-hosted micro-lenders and credit databases.

The systemic impact of this threat environment is ubiquitous across Sub-Saharan Africa, where 82% of enterprise and consumer stakeholders report that they or someone in their direct network have been directly impacted by cyber-enabled fraud within the last 12 months, representing the highest regional exposure rate globally.

Have you or anyone in your professional/personal network been affected by cyber-enabled fraud in the past 12 months?



Source: World Economic Forum



People often ask me whether West Africa is under a different kind of attack. Honestly, no. The attacks look more or less the same everywhere. What is different is what the attacker wants at the end of it. In Southern Africa, the usual play is to lock up your systems and demand a ransom. In East Africa, the big story has been stealing passwords at scale, in bulk. In West Africa, and Nigeria particularly, the attacker wants the money. Not your files. Not your database. The money. He is going after the rail that moves value, not the server that stores records.



Obiora Awogu, Chief Information Security Officer
(CISO), MoMo from MTN



2.1 Technical Vectors vs. Criminal Offenses: Deconstructing African Telemetry

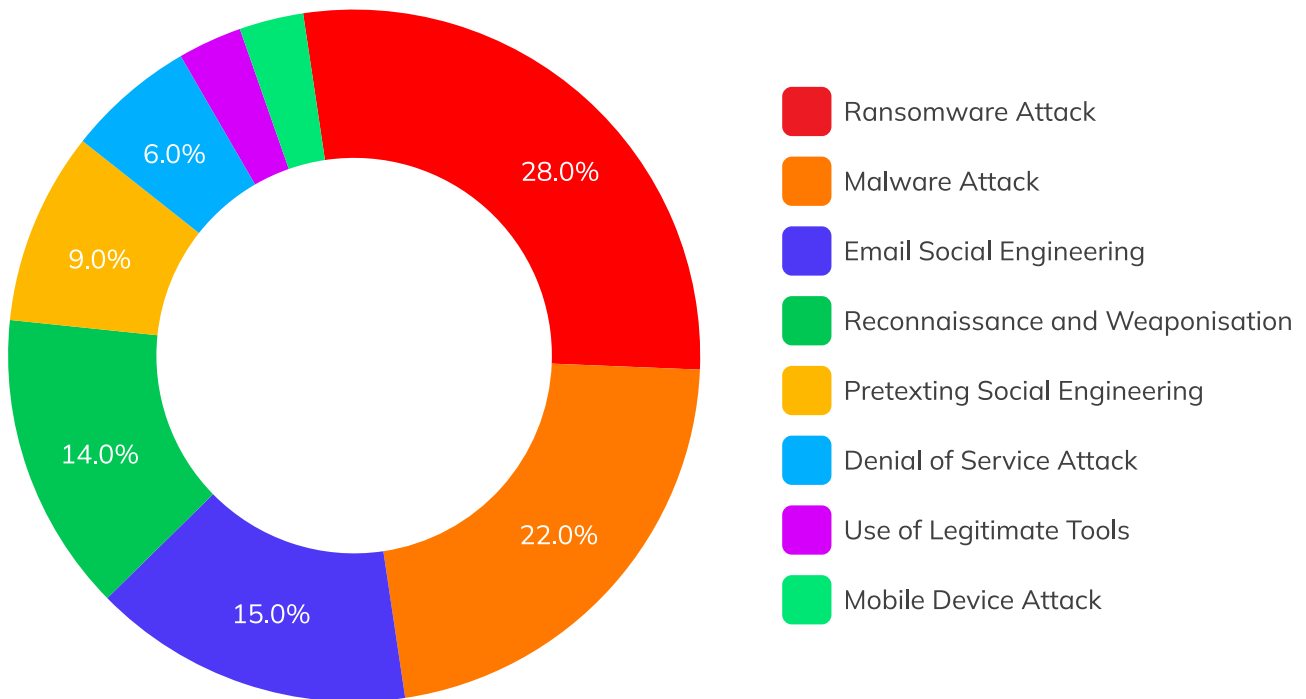
A dual evaluation of African threat telemetry reveals a critical distinction between technical attack vectors (how threat actors enter networks) and reported criminal offenses (how those attacks are monetised).

2.1.1 Technical Entry Vectors:

According to enterprise telemetry captured across African networks by Mastercard, automated exploitation and initial access vectors are dominated by destructive malware, social engineering, and active network probing:

- **Ransomware Attacks (28%):** Represents the single largest technical attack vector attempting network intrusions targeting critical enterprise databases and server infrastructure.
- **Malware Attacks (22%):** Password stealers, spyware, and keyloggers deployed to harvest administrative and customer credentials.
- **Email & Pretexting Social Engineering (24% combined):** High-volume email phishing (15%) and targeted pretexting (9%) serve as the primary human entry points.
- **Reconnaissance & Weaponisation (14%):** Active scanning, port probing, and vulnerability mapping prior to execution.

Cyberthreat Events by Attack Vector in Africa (2025)



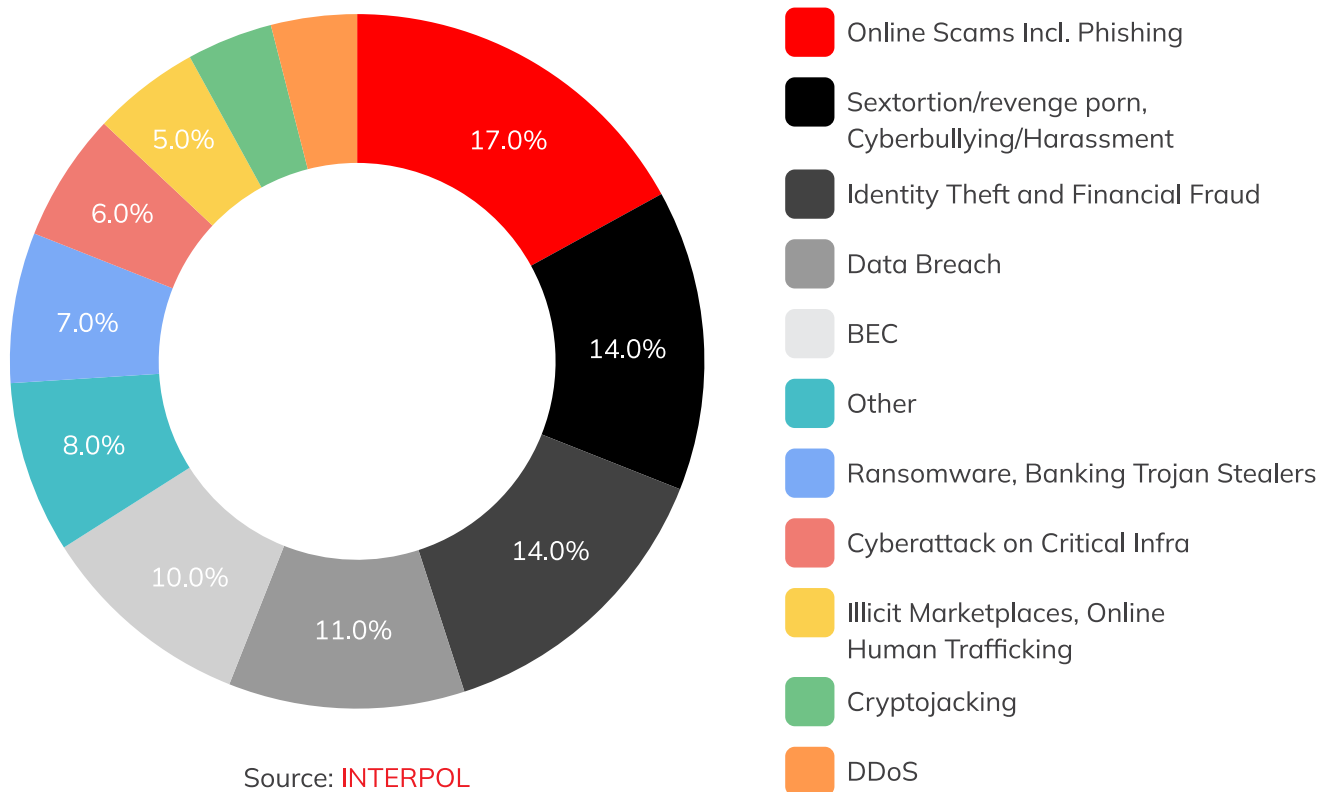
Source: INTERPOL

2.1.2 Finalised Criminal Case Types:

Conversely, official law enforcement filings from INTERPOL member countries demonstrate that technical entry vectors are overwhelmingly deployed to execute direct financial fraud and extortion:

- **Online Scams & Phishing (17%):** The leading reported cybercrime type across the continent.
- **Identity Theft & Financial Fraud (14%):** Direct exploitation of synthetic identities, compromised accounts, and card fraud.
- **Sextortion, Cyberbullying & Harassment (14%):** Consumer-facing extortion campaigns leveraging harvested personal data.
- **Data Breaches (11%) & BEC (10%):** Exfiltration of corporate databases and executive impersonation to divert high-value payments.

Reported Cybercrime Cases Across Africa by Type (2025)



2.2 High-Velocity Financial Fraud & Credential Exploitation

Nigeria sits in a complex position as both a primary target and an operational source of regional cyber-enabled financial crime. Driven by massive digital payment volumes across NIBSS, USSD, and instant switching rails alongside rapid mobile banking adoption, threat actors prioritise immediate payment manipulation over traditional file encryption.

According to Kaspersky threat detection telemetry, 1.6 million online attacks targeting Nigerian users were blocked in H1 2026 alone, with 18.4% of all internet users in the country targeted by web-borne threats. While South Africa logged higher raw attack volumes (5.7 million) due to its larger legacy endpoint footprint, Nigeria's threat profile is characterised by unmatched attack velocity and rapid financial conversion.

2.2.1 Key Vectors Shaping the Nigerian Risk Profile:

- **Multichannel Social Engineering & Account Takeover (ATO):** Phishing in Nigeria has evolved from generic email lures into highly

coordinated, multichannel campaigns spanning WhatsApp, SMS (smishing), USSD, and voice phishing (vishing). Threat actors manipulate customer service channels and account-recovery processes to intercept One-Time Passwords (OTPs) and execute account takeovers on mobile payment wallets and digital banking applications.

- **Identity Monetisation & Mule Networks:** Stolen credentials harvested across Nigerian networks are plugged into mature, well-financed cash-out infrastructure. Mule account networks, compromised POS agent terminals, and peer-to-peer cryptocurrency off-ramps enable attackers to clean and exfiltrate stolen funds within minutes of an intrusion.
- **Data Exfiltration over System Encryption (The ByteToBreach Campaign):** Pure extortion ransomware models face limited commercial success in Nigeria, as local institutions frequently prioritise service restoration over paying ransom demands. In campaigns such as ByteToBreach, threat actors have adapted their economic strategy, focusing primarily on bulk database exfiltration, credential theft, and public disclosure threats rather than pure system locking.



Between 2021 and 2025, phishing, business email compromise (BEC), and social engineering across Nigeria's, Kenya's, and South Africa's financial sectors shifted from largely high-volume, credential-harvesting campaigns towards more targeted, multichannel, identity-focused attacks. Threat actors now increasingly work through compromised accounts, impersonate executives, customers, and trusted third parties, and manipulate legitimate payment and account-recovery processes. As a result, internal defence are under the greatest strain at the intersection of identity assurance, transaction authorisation, customer-service channels, and human decision-making.

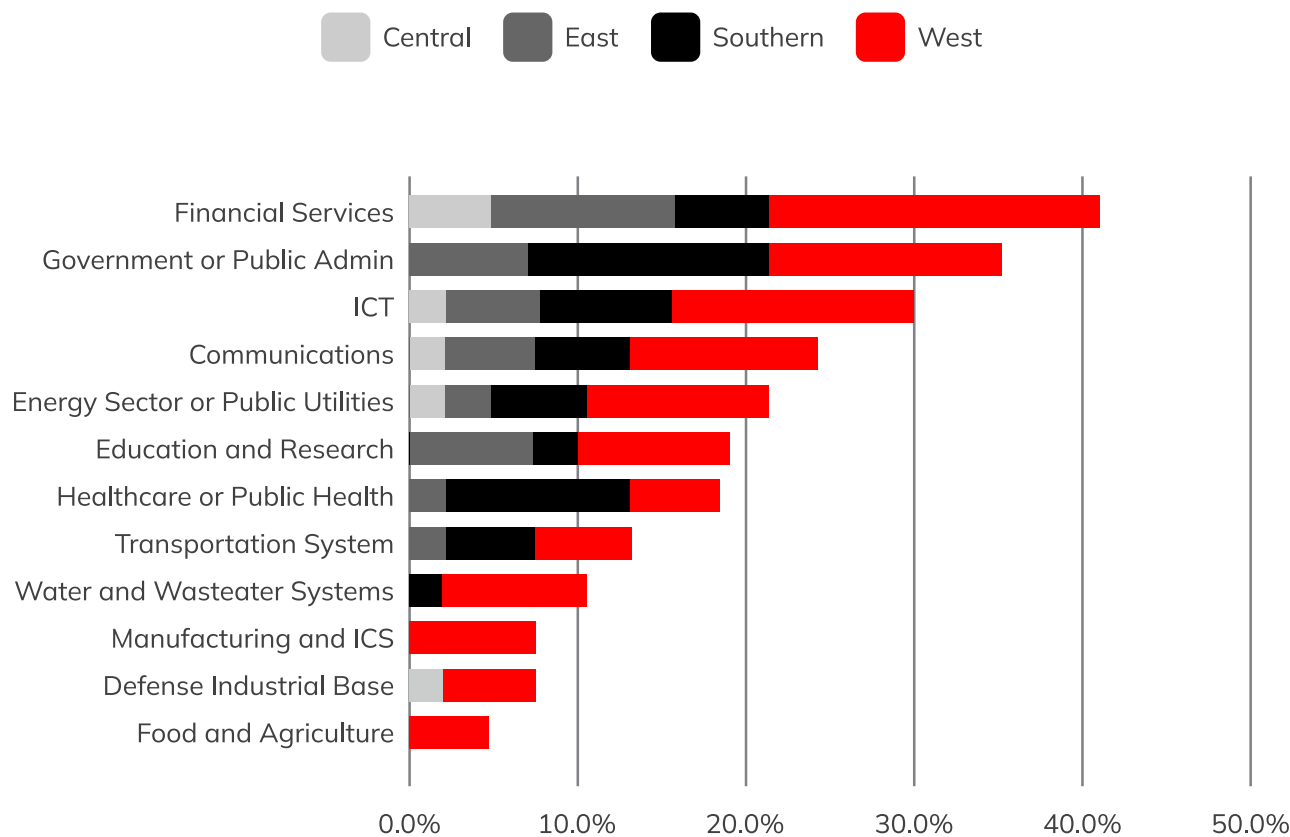


Olusegun Adeniyi, Chief Digital Officer, Wema Bank

2.3 Sector-Specific Vulnerabilities: Banking, Telecoms, and Critical Infrastructure

Nigeria's critical infrastructure, spanning Banking, Telecoms, and Energy or Public Utilities, faces elevated operational risk driven by unpatched edge devices, legacy operational technology (OT), and high-velocity financial payment rails. In Banking and Telecoms, which process USSD transactions and identity-bound OTPs, breaches represent a multi-dimensional crisis combining subscriber data exfiltration with automated payment manipulation.

Targeted Enterprise Sectors by African Region (2025)



Source: INTERPOL

This operational risk extends directly into critical trade logistics and utility networks. This was highlighted in August 2025 when the Nigeria Customs Service ICT platform was targeted by a cyberattack that paralysed cargo clearance operations at major ports, resulting in an **estimated \$18 million** in storage fees, port demurrage costs, and significant import delays.

By comparison, regional benchmarks highlight distinct operational exposures across the continent. South Africa leads continental system-lockup and

double-extortion ransomware losses due to its dense concentration of legacy enterprise networks, with single enterprise incidents costing between **\$10,000 and \$20 million** according to PwC's Global Digital Trust Insights Survey. Meanwhile, Kenya exhibits East Africa's highest web-threat exposure rate (**21.2% of internet users targeted in H1 2026 according to Kaspersky telemetry**), driven by bulk credential harvesting aimed at mobile payment platforms and digital micro-lenders.

03

AI and the Evolving Threat Environment

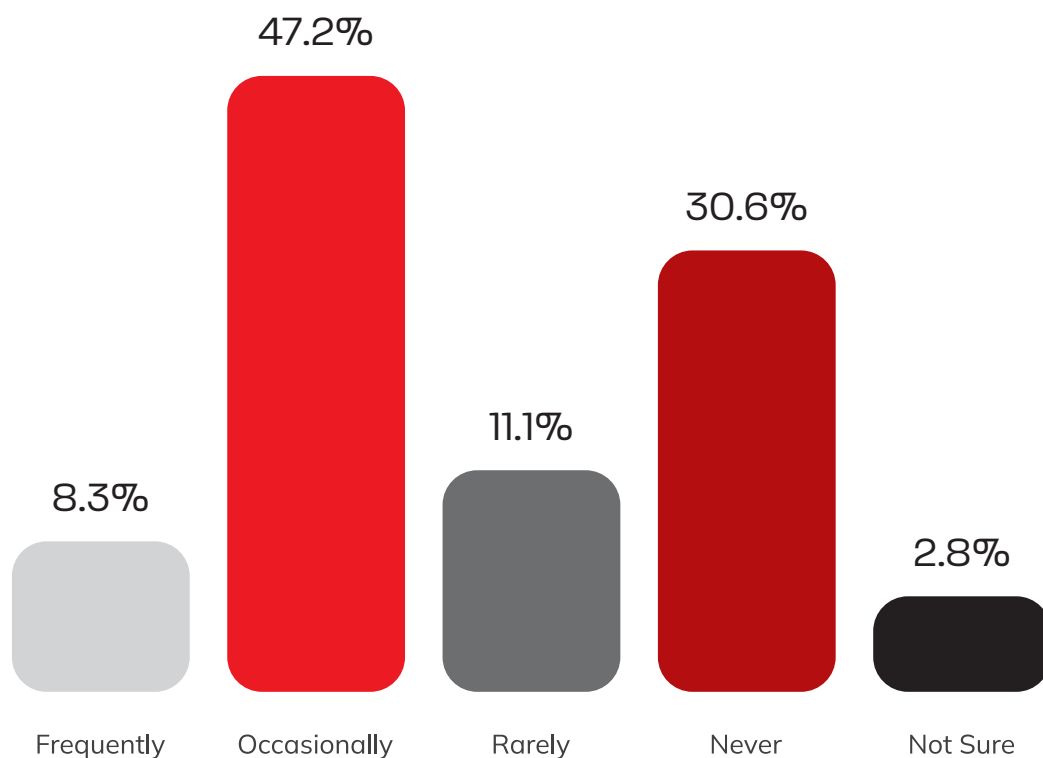


03. AI and the Evolving Threat Environment

Artificial intelligence has transitioned from an emerging technology into a central operational battleground across Africa's digital ecosystem. Cybercriminals and automated crime syndicates are actively leveraging Generative AI, Large Language Models (LLMs), and automated attack frameworks to scale their operations and lower execution costs in bypassing traditional perimeter defenses. Concurrently, enterprise defenders and Security Operations Centers (SOCs) are adopting AI-driven monitoring, User and Entity Behaviour Analytics (UEBA), and automated response playbooks to detect threats at machine speed.

The operational prevalence of AI in cybercrime across the continent is no longer hypothetical. According to law enforcement data published in the INTERPOL African Cyberthreat Assessment Report 2026, over 55% of observed cybercrime cases across member countries utilise AI technology to some degree, with 8.3% of cases frequently employing AI tools and 47.2% incorporating them occasionally.

Cybercrime Cases Observed Utilising AI Technology



Source: [INTERPOL](#)



Generative AI and automation allow criminals to personalise scams and target organisations at machine speed. By imitating familiar voices, crafting culturally fluent messages, and deploying AI chatbots to build trust over time, attackers are making social engineering indistinguishable from legitimate business communication.



Dr. Krishnan Ranganath (Krish), Chief Executive Officer,
UniCloudAfrica

3.1 Weaponisation of AI: Attack Metrics & Vector Breakdown

Threat actors targeting Nigerian and regional African markets exploit AI across automated attack workflows, driving higher conversion rates and faster execution times:

- **Phishing Lure Efficiency:** Global telemetry from Microsoft Threat Intelligence indicates that AI-crafted phishing lures achieve click-through rates as high as **54% compared to 12%** for traditional human-written lures, a capability heavily weaponised across African digital banking and mobile money channels.
- **Business Email Compromise (BEC) Impact Density:** According to Microsoft Threat Intelligence, while Business Email Compromise accounts for approximately 2% of total observed threat volume globally, it drives 21% of successful cyberattack outcomes. This high impact makes executive impersonation a leading vector for high-value invoice fraud and illegal wire transfers across enterprise networks in West, East, and Southern Africa.
- **Deepfake Escalation:** According to data from Sumsb and INTERPOL, deepfake fraud incidents across Africa surged sevenfold between the second and fourth quarters of 2024, continuing to escalate through 2025 and 2026. Attackers primarily target voice and video identity verification channels during high-value wire transfers and remote customer onboarding workflows.
- **CAPTCHA-Protected Phishing Volume:** Globally, Microsoft recorded **11.9 million** CAPTCHA-protected phishing attacks in a single month, representing a **125%** month-over-month increase designed specifically to defeat automated security scanners and deliver malicious payloads to end-users.
- **Macro-Economic Loss Trajectory:** Officially reported cybercrime losses filed with INTERPOL in Africa reached **\$484 million in 2025 (up from \$192 million in 2024)**. However, due to widespread underreporting and varying regional reporting methods, aggregated estimates indicate that cybercrime inflicted at least **\$5 billion** in direct economic damage across Africa in 2025, compared to total continental cybersecurity expenditure of **\$15.3 billion**.



Foundational AI models trained predominantly on Western datasets create dangerous blind spots in Africa. When executive impersonation and automated social engineering drive nearly a quarter of successful breaches locally, effective defence requires AI models grounded in regional transaction behaviours, local languages, and African financial workflows.



Sunday Mgbogu, Head of Engineering, Datamellon



3.2 Generative AI Risks: Shadow IT and Data Exposure

While enterprise teams experiment with Generative AI tools to boost productivity, unmonitored usage has introduced severe corporate data leakage risks:

- **High-Risk Prompt Exposure:** According to the Check Point AI Exposure Index, 90% of Sub-Saharan African organisations utilising Generative AI tools exhibit high-risk prompt activity. Telemetry shows that 1 in every 31 prompts risks exfiltrating sensitive business data, proprietary source code, or customer personally identifiable information (PII) to external cloud LLMs

- **Pre-Deployment Audit Deficits:** Survey data from PwC reveals that while data leaks rank as the top Generative AI concern for 45% of Sub-Saharan African organisations, an identical 45% operate without formal pre-deployment security assessment procedures for AI tools, significantly higher than the global average of 29%.

3.3 Defender Strategies: AI-Driven Monitoring & SOC Modernisation

To counter automated attacks, Security Operations Centers (SOCs) across Nigeria, Kenya, and South Africa are shifting from manual alert triaging toward AI-native security operations:

- **User and Entity Behaviour Analytics (UEBA):** UEBA algorithms establish dynamic baselines for normal network behaviour. These systems flag operational anomalies, such as an administrative account accessing sensitive payment databases at 3 a.m. from an unrecognised IP address, without relying solely on static threat signatures.
- **AI-Assisted Triage & RAG Frameworks:** Modern Security Information and Event Management (SIEM) platforms, which collect and aggregate security log data, and Security Orchestration, Automation, and Response (SOAR) platforms, which automate incident response workflows, leverage AI agents to correlate disparate security alerts and filter false positives. SOC analysts utilise Retrieval-Augmented Generation (RAG) systems to query internal playbooks and threat intelligence feeds instantly.
- **Synthetic Media Verification:** Multimodal verification tools analyse facial pixel consistency, frame alignment, and audio frequency artifacts to detect voice clones and manipulated video feeds during remote customer verification and executive authorisation checks.
- **Automated Response Playbooks:** Machine learning models monitor internal data flows to identify unusual outbound transfers. When anomalous behaviour crosses pre-set risk thresholds, automated SOAR playbooks isolate endpoints or revoke active session tokens while awaiting human analyst confirmation.

3.4 Operational SOC Capabilities and Workforce Asymmetry

The operational race between automated attacks and defender capabilities reveals a clear technical skills bottleneck across African enterprise SOC's:

- **Expertise Gap in Forensic Units:** While 55% of cybercrime cases in Africa involve AI, INTERPOL telemetry reveals that only 8% of intelligence analysts and 22% of digital forensic units across the continent possess advanced operational knowledge of AI threat vectors.
- **Resource and Financial Constraints:** Global survey data from the World Economic Forum shows that 62% of Sub-Saharan African organisations cite a lack of specialised skills as the primary barrier to effective AI-enabled security, while 56% point to financial limitations.
- **Resilience Self-Assessments:** While 76% of Sub-Saharan African organisations have implemented some form of AI-enabled security tooling, only 8% assess their overall cyber resilience posture as exceeding requirements. Meanwhile, 60% report meeting only minimum requirements, and 32% rate their current posture as insufficient.

This operational capability deficit directly underpins the necessity for managed security services and local SOC-as-a-Service architectures.

04

Ecosystem Maturity & Regulatory Landscape

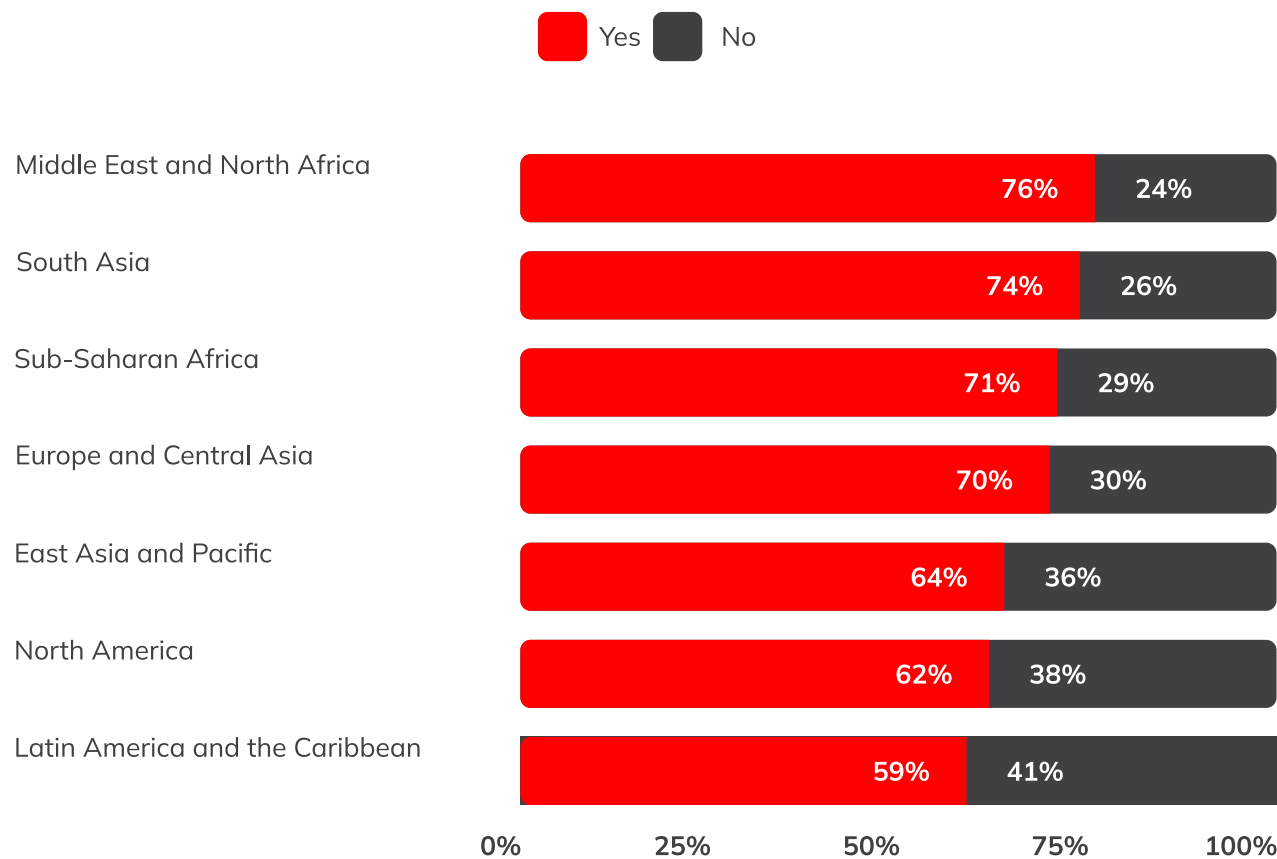


04. Ecosystem Maturity & Regulatory Landscape

Sub-Saharan Africa's cybersecurity regulatory framework is undergoing a rapid transition from passive policy guidance to aggressive enforcement. Driven by statutory mandates and rising geopolitical volatility, compliance has evolved into a board-level operational imperative.

This institutional evolution is heavily influenced by global conditions. World Economic Forum risk surveys indicate that 71% of organisations in Sub-Saharan Africa have adapted their cybersecurity strategy due to geopolitical volatility, slightly outpacing Europe (70%), North America (62%), and Latin America (59%).

Has your organisation's cybersecurity strategy evolved because of geopolitical volatility?



Source: [World Economic Forum](#)

Concurrently, 78% of Sub-Saharan African enterprise leaders view cyber regulations as effective in strengthening overall security postures, rising to **92% in East Africa** according to PwC survey data.

4.1 Nigeria's Institutional Readiness: NDPA, CBN Directives, and Sectoral Mandates

Nigeria's data regulatory ecosystem is anchored by the Nigeria Data Protection Act and operationalised

through the Nigeria Data Protection Commission (NDPC). The NDPC operates as an independent supervisory authority backed by statutory powers to conduct sector investigations, halt non-compliant processing, and issue administrative penalties.

Under the NDPA, statutory sanctions for Data Controllers and Data Processors of Major Importance (DCPMIs) can reach up to ₦10 million or 2% of annual gross revenue, whichever is higher. Regulatory enforcement has intensified, with multi-million-Naira sanctions levied across non-compliant institutions and media firms for processing data without consent or executing unauthorised cross-border transfers.

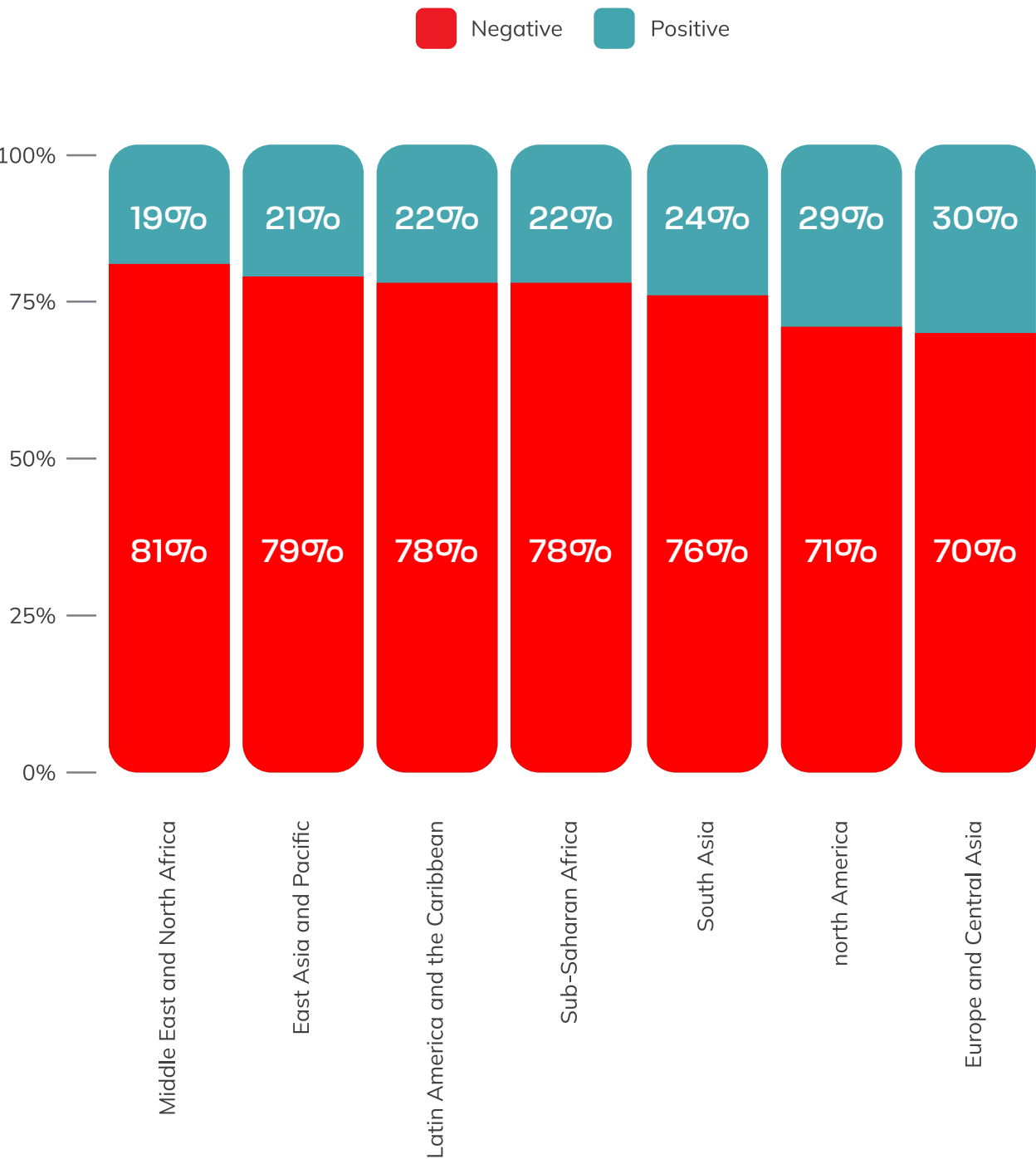


Enforcement under the Nigeria Data Protection Act is designed to create a culture of accountability rather than simply impose penalties. The Commission's regulatory approach balances firm statutory enforcement with active stakeholder engagement, ensuring that organisations move beyond superficial tick-box compliance to establish demonstrable, technical data safeguards across the entire processing lifecycle.



**Ibukunoluwa Owa, Head of Regulations Unit,
Nigeria Data Protection Commission (NDPC)**

What is your view about the effectiveness of cyber-related regulations?



Source: World Economic Forum

Key Statutory Pillars Governing Nigerian Enterprises:

1. The NDPA 2023 & Cross-Border Mandates:

While the NDPA does not impose a blanket data localisation mandate, Part VIII of the act strictly regulates cross-border personal data transfers, requiring adequacy assessments, Standard Contractual Clauses (SCCs), or global privacy frameworks.

2. The Central Bank of Nigeria (CBN) Payment Data Localisation Directive:

Sector-specific rules are establishing strict data residency requirements. The CBN Circular mandates that all domestic payment transaction data generated within Nigeria must be stored and managed locally, with full mandatory compliance enforced from 1 January 2027.

3. The Cybercrimes Act & ONSA Mandates:

Overseen by the Office of the National Security Adviser (ONSA), the amended Cybercrimes Act establishes a mandatory 72-hour incident-reporting window following breach confirmation, requiring covered entities to report major attacks directly to the National Computer Emergency Response Team (ngCERT).

- **South Africa:** Overseen by the Information Regulator under the Protection of Personal Information Act (POPIA), South Africa enforces mandatory breach notifications, while public sector workloads face increasing data localisation guidance under the National Policy on Data and Cloud.
- **Kenya:** Supervised by the Office of the Data Protection Commissioner (ODPC), Kenya's regulatory framework requires mandatory registration, Data Protection Impact Assessments (DPIAs), and approval for cross-border transfers involving strategic national datasets.

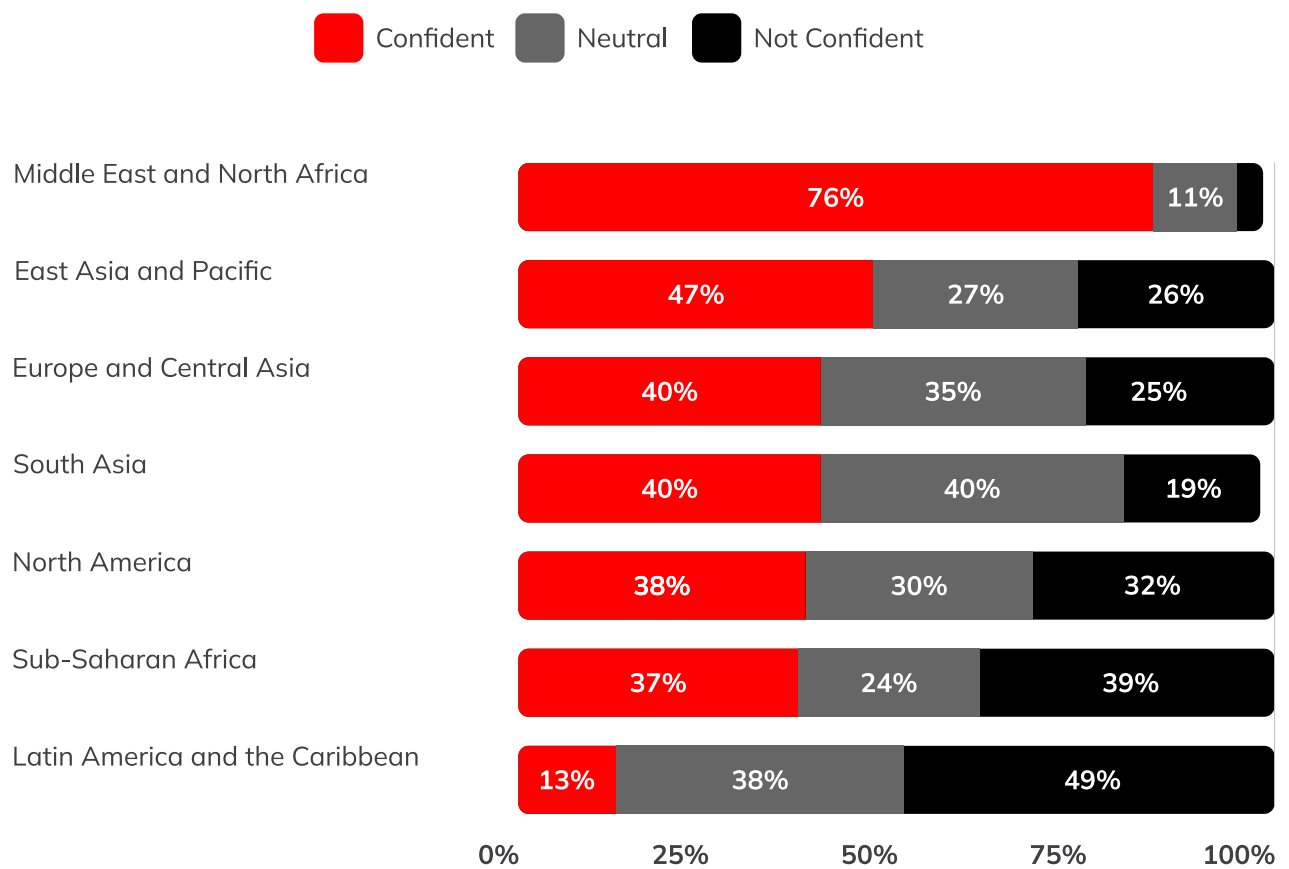
4.3 National Critical Infrastructure Preparedness Deficit

Despite regulatory momentum, enterprise leaders express concern regarding national incident response readiness. World Economic Forum data shows that only 37% of Sub-Saharan African respondents are confident in their country's ability to respond to major critical infrastructure attacks, while 39% lack confidence, and 24% remain neutral.

4.2 Regional Regulators

While regulatory objectives align across Sub-Saharan Africa's three primary digital hubs, enforcement mechanisms, breach-notification rules, and data residency frameworks differ significantly:

How confident are you in the preparedness of the country in which you are based to respond to major cyber incidents targeting critical infrastructure?



Source: [World Economic Forum](#)



Navigating digital infrastructure expansion across West Africa requires a clear understanding of legal and regulatory interplay. While data sovereignty directives like the CBN payment localisation mandate require domestic data hosting, enterprise resilience relies on interconnecting with global digital ecosystems. The challenge for multijurisdictional entities is structuring infrastructure that satisfies local regulatory requirements without sacrificing cloud performance or international connectivity.

Abayomi Adebajo, Director Legal, Equinix

This gap highlights a key structural risk: while Tier-1 banks and telecoms maintain robust internal controls, broader utility, power, and municipal networks remain exposed to systemic operational disruptions.

4.4 Enterprise Operational Compliance & Friction Points

Regulatory Fragmentation & Cross-Border Data

Transfers: Operating across West, East, and Southern Africa requires navigating distinct transfer approvals and breach-notification windows. To mitigate this friction, the NDPC co-chairs the

Network of African Data Protection Authorities (NADPA-RAPDP) Regulatory Harmonisation Working Group, aligning transfer principles with the ECOWAS Supplementary Act and the AU Malabo Convention.

Reconciling Localisation with Cloud Architecture:

The CBN's January 2027 payment data deadline requires financial institutions to restructure hybrid cloud environments, ensuring primary transaction databases and recovery replicas reside within certified local data centers while maintaining encrypted connectivity across regional branches.



Navigating digital infrastructure expansion across West Africa requires a clear understanding of legal and regulatory interplay. While data sovereignty directives like the CBN payment localisation mandate require domestic data hosting, enterprise resilience relies on interconnecting with global digital ecosystems. The challenge for multijurisdictional entities is structuring infrastructure that satisfies local regulatory requirements without sacrificing cloud performance or international connectivity.



Abayomi Adebajo, Director Legal, Equinix

05

The OEM & Global Vendor Gap (Addressing the SME Market)



05. The OEM & Global Vendor Gap (Addressing the SME Market)

The Sub-Saharan African cybersecurity market exhibits a sharp structural divergence. While large corporate institutions commanded 70.69% of regional cybersecurity spending in 2025, Small and Medium Enterprises (SMEs) represent the vast majority of commercial activity across the continent and are projected to record the fastest growth, compounding at a 14.87% CAGR through 2031. However, as mid-sized African enterprises accelerate digital transformation, they encounter operational alignment challenges when adopting global software platforms.

5.1 The SME Operational Gap: Realigning Enterprise Security Tools for Local Realities

Global Original Equipment Manufacturer (OEM) platforms deliver enterprise-grade protection for multinational corporations, but growing African SMEs frequently encounter operational fit gaps when deploying these solutions locally:

1. **Macroeconomic Volatility & Foreign Currency Pricing:** Global OEM platforms are overwhelmingly priced in US Dollars (USD) or Euros (EUR). Sharp local currency devaluations across key African markets create foreign exchange instability, inflating local-currency procurement budgets. These cost pressures force growing organisations to adjust deployment scopes or defer essential module renewals.
2. **Licensing Complexity & Total Cost of Ownership:** Multi-tiered user seat, endpoint, and data ingestion licensing models make long-term expenditure forecasting difficult for mid-market businesses, leading to unexpected operational cost escalations at renewal.
3. **Deployment Complexity & Resource Constraints:** Foreign security platforms often assume access to dedicated, highly specialised in-house engineering teams. In resource-constrained IT environments, lean internal teams face high alert volumes, making complex configurations difficult to manage continuously.
4. **Compliance Framework Mapping:** Global Governance, Risk, and Compliance (GRC) suites are typically calibrated to Western frameworks like GDPR, requiring manual customisation to map controls directly to domestic privacy statutes such as Nigeria's NDPA, Kenya's DPA, or South Africa's POPIA.
5. **Local Threat Context:** Threat activity in African markets frequently focuses on mobile-money API integrations, USSD switching rails, and localized payment channels, requiring threat intelligence tuned to regional transaction behaviours.



SMEs face significant resource and operational hurdles when trying to maintain robust security postures. Automated compliance platforms bridge this gap by streamlining regulatory frameworks into continuous monitoring workflows, allowing growing businesses to achieve demonstrable compliance and reduce operational overhead without requiring massive security budgets.



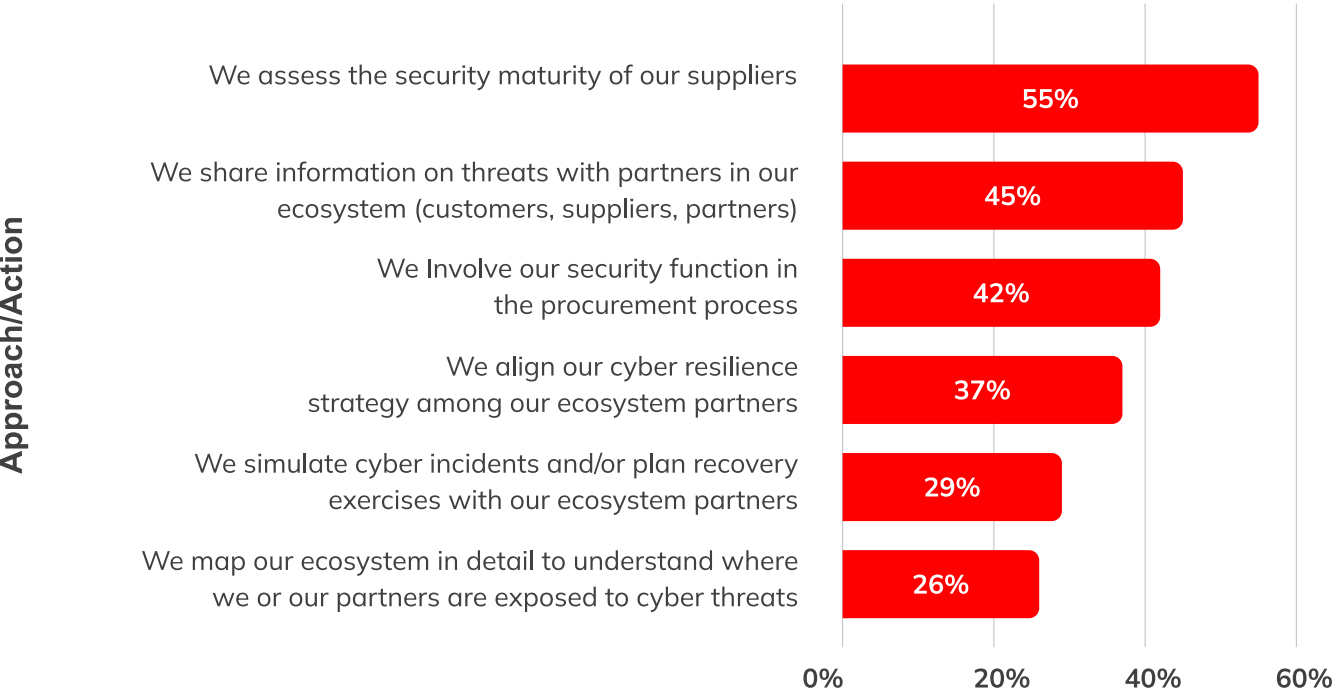
Gbemisola Osunrinde, CEO, Smartcomply

5.2 Supply Chain Cyber Risk & Procurement Integration

The operational friction surrounding global security software is further heightened by expanding third-party supply chain risks across Sub-Saharan Africa. As African enterprises interconnect their payment networks, cloud APIs, and vendor applications, third-party exposures have escalated, making procurement governance a core pillar of cyber resilience.

According to enterprise survey data from the World Economic Forum, Sub-Saharan African organisations actively manage supply chain risk through structured vendor governance:

What is your view about the effectiveness of cyber-related regulations?



Source: [World Economic Forum](#)
Note: Multiple-choice Questions

While 55% of organisations assess supplier security maturity and 42% involve cybersecurity teams in formal procurement, smaller suppliers and SMEs struggle to satisfy complex enterprise audit questionnaires when forced to deploy costly, foreign-denominated security controls.

5.3 The Local Managed Solution Opportunity: The Case for SOC-as-a-Service

To overcome foreign currency friction and management overhead, mid-sized African enterprises are increasingly pivoting toward locally embedded Managed Security Service Providers (MSSPs) delivering Security Operations Center as a Service (SOCaaS).

- **Predictable Local-Currency Expenditure:** Transitioning security procurement from foreign-currency capital expenditure (CapEx) to predictable, local-currency operational expenditure (OpEx) insulates corporate budgets from macroeconomic volatility.
- **Outcome-Based Service Delivery:** Locally managed service models replace complex tool licensing with outcome-driven security, delivering 24/7 Managed Detection and Response (MDR), continuous threat hunting, and automated incident triage through flexible subscription tiers.
- **Shared Specialist Talent:** Rather than competing globally to recruit and retain scarce 24/7 SOC engineering teams, enterprises leverage multi-tenant access to local threat analysts at a reduced total cost of ownership.
- **In-Country Data Sovereignty:** Locally operated SOC infrastructure ensures that primary security telemetry, audit logs, and transaction records remain strictly within domestic regulatory borders, satisfying mandates like the CBN Payment Data Directive and NDPA.



Securing modern financial platforms requires moving beyond reactive perimeter defences to establish continuous, identity-centric visibility across every transaction layer. As payment switches and digital channels scale, institutions must combine real-time threat intelligence with localised monitoring to detect anomalous transaction patterns before fraud occurs.



Ayodeji Jaiyeola, Chief Information Security Officer, Hydrogen Financial

06

Technology, Infrastructure & Managed Services Opportunity

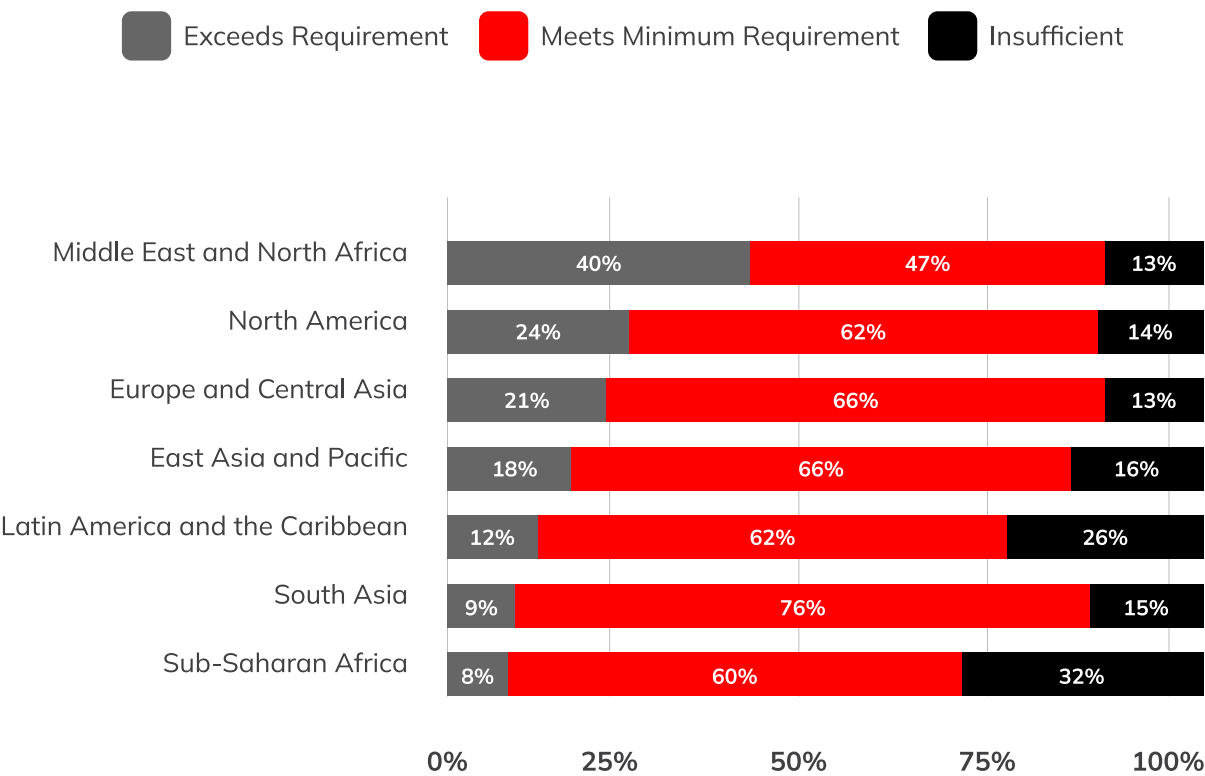


06. Technology, Infrastructure & Managed Services Opportunity

Sub-Saharan Africa’s enterprise IT environment is undergoing a rapid transition toward cloud-native architectures, multi-cloud hosting, and carrier-neutral data center colocation. However, as enterprise perimeters dissolve into hybrid environments, the internal attack surface has expanded significantly.

This infrastructure evolution highlights a clear operational vulnerability across the continent: regional cyber resilience benchmarks indicate that only 8% of Sub-Saharan African organisations rate their cyber resilience as exceeding requirements, while 60% meet minimum requirements, and 32% assess their current posture as insufficient.

Enterprise Self-Assessment of Cyber Resilience Posture



Source: [World Economic Forum](#)



What we are seeing increasingly is that weaknesses are not always sophisticated technical failures. Quite often, they are cloud misconfigurations, excessive access privileges, compromised credentials, poorly governed APIs, and third-party access. In that sense, identity, configuration, and interconnection are becoming just as important as the traditional network perimeter.



Kelechi Ohalete, Head of Governance, Risk and Control, Rack Centre

6.1 Enterprise IT Trends & the Multi-Cloud Threat Surface

As Nigerian and regional African enterprises migrate core workloads to cloud platforms, standalone security perimeters are no longer sufficient to protect distributed data flows:

- **Cloud Adoption Momentum:** Cloud-based cybersecurity spending in Sub-Saharan Africa is projected to expand at a **14.63% CAGR through 2031**, supported by rapid enterprise migration to multi-cloud platforms and local hyperscale data center builds.
- **Expanding Identity and API Attack Surfaces:** Workloads distributed across private clouds, SaaS applications, and third-party vendor integrations make identity governance, zero-trust access control, and API security critical defensive priorities.
- **Physical Infrastructure Interdependence:** Cybersecurity resilience remains directly linked to underlying facility uptime, power redundancy, carrier-neutral interconnectivity, and local hosting reliability.

6.2 Market Opportunity:

The Rise of Managed Services (MSSP & Managed SOC); The economics of enterprise cybersecurity are shifting from standalone software purchases toward continuous operational execution. While cybersecurity solutions represented 67.16% of total regional revenue in 2025, expenditure on cybersecurity services is projected to expand at a **14.54% CAGR through 2031**. This trend reflects strong demand for outsourced Security Operations Centers (SOCs), Managed Detection and Response (MDR), and proactive threat hunting.



Maintaining a genuinely effective 24/7 in-house SOC requires sufficient personnel to cover shifts, leave, attrition, and burnout. Security talent is scarce and expensive, while analysts face severe alert fatigue. The result is a growing business case for SOC-as-a-Service, allowing organisations to access specialist talent, technology, and continuous monitoring without bearing the full cost of building in-house.



**Michael Ojih, Chief Information Security Officer,
Transactworld Digital Services**

6.3 The Transition from Point Solutions to Unified SOC-as-a-Service

Enterprise CISOs are actively consolidating fragmented security tools into unified, cloud-native platforms to streamline operations and satisfy stringent regulatory mandates:

- **Overcoming In-House SOC Overhead:** Operating a 24/7 internal SOC requires a minimum of 8 to 12 dedicated Tier-1 to Tier-3 security analysts to manage shift rotations effectively. Combined with escalating log ingestion costs under traditional security tooling, internal SOC present substantial overhead challenges for mid-market institutions.
- **Adopting Hybrid Operating Models:** Rather than choosing between complete outsourcing or building entirely in-house, enterprises are converging on a hybrid co-management model. Internal leadership retains strategic governance and business risk ownership, while an external SOC-as-a-Service provider manages 24/7 Tier-1 threat monitoring, alert correlation, and incident triage.
- **Integrating Security Operations with Regulatory GRC:** Modern SOC platforms connect real-time threat detection directly into Governance, Risk, and Compliance (GRC) workflows. Security telemetry provides continuous, demonstrable evidence for regulatory audit trails under the NDPA, Central Bank directives, and PCI DSS standards, converting technical detection logs into business-aligned risk intelligence.

07

Talent, Capacity & Workforce Pipeline

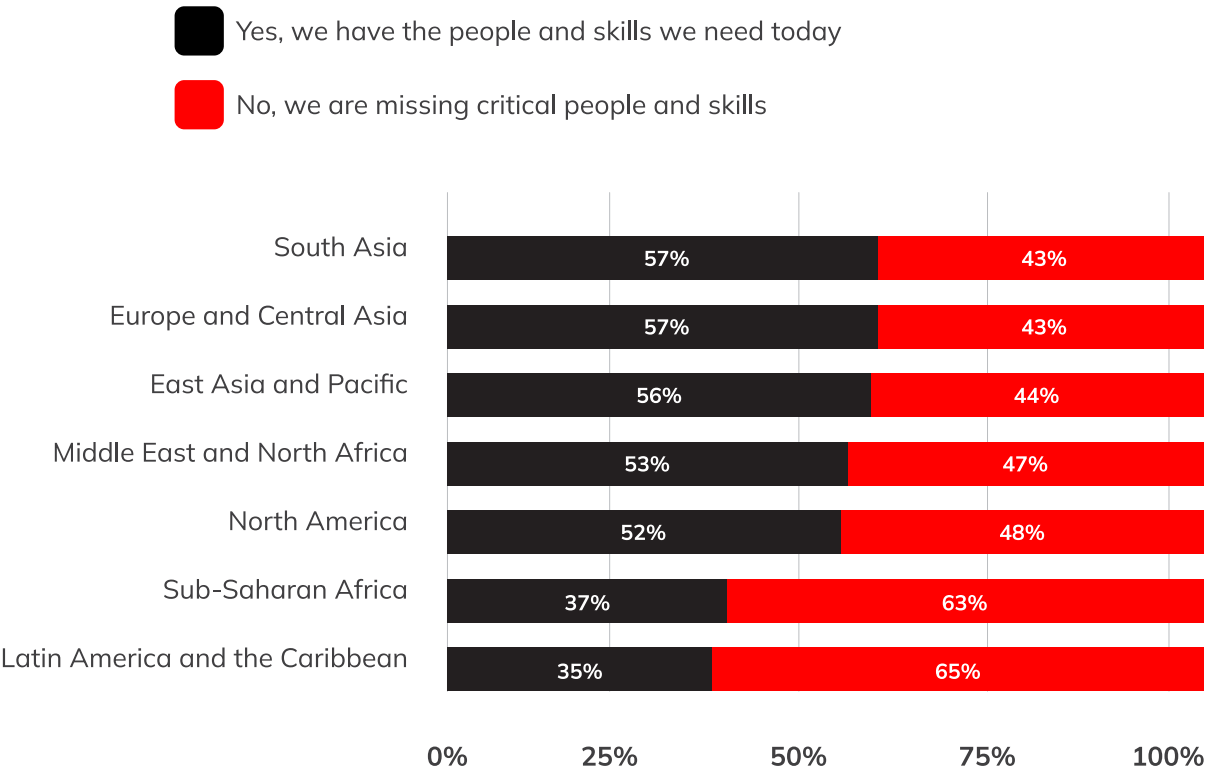


07. Talent, Capacity & Workforce Pipeline

Sub-Saharan Africa faces a critical cybersecurity human capital deficit. While enterprise digital adoption, multi-cloud migration, and financial technology scaling have expanded operational risk environments, the regional pipeline of job-ready security engineering talent requires rapid expansion.

This human capital gap is confirmed by global workforce survey data published by the World Economic Forum: 63% of Sub-Saharan African organisations report that they lack the critical cybersecurity personnel and skills needed to achieve current security objectives, representing one of the highest capacity deficits globally, second only to Latin America (65%).

Does your workforce have the skills needed to achieve current security objectives?



Source: [World Economic Forum](#)



The cybersecurity skills gap in Africa is not a failure of academia, it is an industry-alignment challenge. Traditional academic programmes explain networks and security concepts, but job readiness requires repeated exposure to realistic SOC operating environments: analysing telemetry, working with SIEM and endpoint tools, investigating incidents, and communicating risk under pressure.



Olugbolahan Olusanya, Territory Director (Africa), TeKnowledge

7.1 Structural Drivers of the African Cyber Talent Deficit

The regional cybersecurity skills shortage is structural, driven by three converging operational pressures across West, East, and Southern Africa:

- **Hyper-Specialisation vs. General IT Pipelines:**
The deployment of cloud platforms, digital payment switches, and connected infrastructure demands domain-specific capabilities in cloud security architecture, threat hunting, identity governance, and incident response. Traditional computer science curricula provide foundational theory but often lack practical, hands-on telemetry experience.
- **Global Competition and Remote Talent Drain:**
Skilled African cybersecurity professionals operate in an international talent marketplace. Domestic enterprises face continuous competition from international technology firms offering foreign-currency compensation packages and remote working arrangements.
- **Alert Fatigue and Operational Burnout:**
Understaffing forces small internal security teams into reactive postures. Continuous 24/7 monitoring, unmanaged alert volumes, and repetitive incident pressure contribute to high analyst turnover across enterprise security operations.

7.2 Bridging the Pipeline: Public Initiatives vs. Private-Sector Academies

Closing the workforce gap requires bridging the divide between foundational digital education and operational SOC capability. Public sector capacity-building initiatives, such as Nigeria's 3 Million Technical Talent (3MTT) programme led by the Ministry of Communications, Innovation and Digital Economy, provide essential large-scale foundational training.

Translating foundational digital literacy into job-ready SOC analysts requires structured private-sector enablement. Private-sector academies and Managed Security Service Providers (MSSPs) integrate role-based technical certifications with scenario-based cyber ranges, hackathons, and supervised SOC analyst shadow programmes. This practical approach evaluates real-world capability, assessing whether an analyst can investigate an alert, isolate an endpoint, and document evidence, rather than relying solely on formal course completion.

7.3 Enterprise Retention Strategies and the Hybrid Talent Operating Model

To manage talent turnover and protect institutional knowledge, African enterprise CISOs are adopting structured retention and operational co-management models:

- **Contextual Certification Sponsorship:** Sponsoring advanced industry certifications (such as CISSP, CISM, or CEH) is tied directly to internal career progression frameworks, helping transition junior analysts into specialised disciplines including threat hunting, cloud security engineering, and incident response.
- **Work Redesign & Automation:** Enterprise teams deploy Security Orchestration, Automation, and Response (SOAR) tools to automate repetitive manual alert triaging, reducing operational burnout and allowing analysts to focus on complex threat investigations.
- **Co-Managed MSSP Retention Models:** Rather than attempting to staff an entire 24/7 internal team, enterprises utilise co-managed MSSP models. Internal teams retain institutional context, governance, and business risk ownership, while external MSSPs manage 24/7 Tier-1 shift monitoring and log correlation. This hybrid model insulates organisations from individual staff resignations while allowing internal talent to focus on strategic security initiatives.



Every security operations centre built in Lagos, Nairobi, Casablanca or Johannesburg gives young engineers live incidents to work on, and that experience builds real capability in ways a certificate can't. Over the next three to five years, the countries and organisations that pull ahead will fund cybersecurity as business and national resilience, and they will keep the expertise, and the data, on the continent. That is how Africa moves from importing security to exporting it



Werner Lindemann, Chief Executive Officer, Data Group IT

08

Strategic Outlook & Recommendations



08. Strategic Outlook & Recommendations

The Sub-Saharan African cybersecurity ecosystem stands at a critical turning point. As digital payments expand, cloud migration accelerates, and regulatory authorities enforce stricter compliance rules, enterprise resilience can no longer rely on reactive, piecemeal security tools.

Looking ahead to the 2027–2028 operational horizon, organisational success will depend on an enterprise's ability to protect its procurement budgets from foreign currency volatility, integrate intelligent behavioural threat detection, and align data architectures with regional data sovereignty mandates.

8.1 Forward Projections (2027–2028)

Synthesis of market telemetry, regulatory directives, and CISO insights across Nigeria, Kenya, and South Africa highlights three major structural shifts shaping the continent's threat and operational landscape through 2028:

- **Enforcement of Mandatory Payment Data Localisation:** By 1 January 2027, the Central Bank of Nigeria's directive requiring all domestic payment transaction data to be stored and processed within national borders will come into full force. This mandate, alongside similar critical national infrastructure rules in Kenya and South Africa, will compel financial institutions, payment switches, and cloud providers to host primary databases and disaster recovery replicas inside certified local data centers.
- **Escalation of AI-Driven Automated Financial Fraud:** Threat actors will continue automating attack steps using localized language models and synthetic media. With AI-crafted phishing lures achieving high conversion rates and deepfake fraud expanding, attackers will increasingly target remote identity verification channels and attempt automated session token theft to bypass multi-factor authentication.
- **Mainstream Transition to Local-Currency Managed Security Services:** Faced with foreign exchange illiquidity and local currency devaluations, enterprises will accelerate their departure from foreign-currency software licenses. Organisations will increasingly adopt local-currency SOC-as-a-Service models to secure continuous 24/7 monitoring without exposing procurement budgets to exchange rate shocks.
- **Transition to Local-Currency Managed Services (SOCaaS):** Mitigate foreign exchange risk by shifting from USD-denominated point solutions toward local-currency Managed Security Service Providers (MSSPs). Adopting a hybrid SOC model allows internal teams to retain strategic governance while an external provider manages 24/7 Tier-1 monitoring.
- **Implement Identity-Centric Zero Trust Architecture:** Traditional perimeters are insufficient for distributed cloud environments. CISOs must enforce zero-trust access, mandatory phishing-resistant multi-factor authentication across all endpoints, strict API rate limits, and multi-person authorization workflows for high-value financial transactions.
- **Shift from Post-Incident Freezes to Real-Time Behavioural Holds:** Seeking court orders to freeze bank accounts after fraudulent funds have already been exfiltrated yields low recovery rates. Institutions should deploy User and Entity Behaviour Analytics (UEBA) to identify anomalous transaction velocity and place real-time automated holds on suspicious transfers at the point of initiation.

8.2 Grouped Actionable Roadmap

To navigate these structural shifts, strategic priorities must be aligned across three key stakeholder groups:

8.2.1 Action Plan for Enterprise Leaders & Chief Information Security Officers (CISOs)



• 8.2.2 Action Plan for Policymakers & Regulatory Authorities

- **Harmonise Regional Data Protection & Transfer Frameworks:** Data protection authorities across West, East, and Southern Africa should deepen collaboration through the Network of African Data Protection Authorities (NADPA-RAPDP). Harmonising cross-border transfer rules and breach-notification windows will streamline regional compliance and support cross-border digital trade under the African Continental Free Trade Area (AfCFTA).
- **Establish National Critical Infrastructure Defence Standards:** Regulatory bodies must expand baseline cybersecurity mandates beyond financial institutions to encompass energy grids, port logistics, and municipal utilities, enforcing mandatory 72-hour incident reporting to national Computer Emergency Response Teams (such as ngCERT in Nigeria).
- **Fund Public-Private Cyber Skilling & Cyber Range Academies:** Government ministries should partner with private industry and academic institutions to expand capacity-building initiatives, providing subsidised access to hands-on cyber range training to bridge the regional workforce gap.

8.2.3 Action Plan for Technology Investors & Infrastructure Developers

- **Capitalise on Carrier-Neutral Data Centres & In-Country SOC:** Localisation mandates (such as the CBN payment data directive) create strong commercial opportunities for infrastructure investment. Capital should be targeted toward expanding tier-rated, carrier-neutral data centers and local-currency SOC-as-a-Service platforms across key regional hubs.
- **Develop AI Threat Engines Trained on Local Datasets:** Global security tools trained on Western telemetry frequently miss localized attack patterns. Venture capital and technology investors should prioritize funding threat intelligence platforms tuned specifically to African mobile-money API workflows, USSD switching rails, and regional social engineering tactics.
- **Support Scalable Cybersecurity Talent Academies:** Investment in specialized technical training centers that offer practical SOC analyst certifications and managed shadow programs provides high commercial returns while expanding the regional pipeline of job-ready security engineering talent.



African organisations must move beyond compliance-driven cybersecurity towards measurable cyber resilience. This means understanding their exposure, strengthening identity and payment security, improving continuous threat monitoring, and building the capacity to respond and recover quickly from incidents. Ultimately, cybersecurity investment must translate into tangible outcomes: reduced financial losses, protected customer data, uninterrupted critical services and sustained public trust in Africa's growing digital economy.



William Makatiani, Chief Executive Officer, Serianu Limited.

8.3 Conclusion

Defending Sub-Saharan Africa's digital ecosystem requires a fundamental shift in how leadership views cybersecurity. It is not an isolated IT expense or a passive regulatory exercise; it is an active operational discipline that directly underpins financial system stability, investor trust, and regional growth.

As threat tactics shift toward automated financial fraud and deepfake exploitation, enterprise resilience will depend on pragmatic infrastructure choices rather than defensive posture. Organisations that replace foreign-currency vendor complexity with predictable local managed services, enforce strict identity controls across payment rails, and align their architectures with emerging data residency rules will establish a distinct operational advantage. By grounding cybersecurity in regional market realities, African institutions can protect their balance sheets, satisfy regulatory mandates, and build an enduring foundation for digital trade across the continent.

References

Adaptive Security. (2026, July 5). AI phishing vs. traditional phishing: How generative AI drives 54% click-through rates and evades detection.

<https://www.adaptivesecurity.com/blog/ai-phishing-vs-traditional-phishing-what-is-the-difference>

Agbetiloye, A. (2024, May 16). Fintech giant Flutterwave loses ₦11 billion to security breach. Business Insider Africa.

<https://africa.businessinsider.com/local/markets/fintech-giant-flutterwave-loses-naira11-billion-to-security-breach/bv1hdev?utm>

Aviaan Accounting. (2026). Market research and feasibility study for cybersecurity in Africa.

<https://aviaanaccounting.com/market-research-and-feasibility-study-for-cybersecurity-in-africa/>

Ayua, J. (2024, December 24). Patricia recommit to refunding affected users over cyber breach. Crypto Asset Buyer.

<https://cryptoassetbuyer.com/patricia-refunding-affected-users-cyber-breach/>

Bade, A. M., Babate, A. I., & Bara, M. W. (2026). AI-driven cyber threats and defences in Nigeria's digital economy: A literature review. International Journal of Research and Innovation in Applied Science, 11(2), 1505-1511.

BlueWeave Consulting. (2019). Kenya cybersecurity market report, trend analysis, competitive landscape & forecast (2019–2031).

<https://www.blueweaveconsulting.com/report/kenya-cybersecurity-market>

Check Point Research. (2026). AI security report 2026.

<https://research.checkpoint.com/2026/ai-security-report-2026/>

CYFIRMA. (2025, September 30). Cyber threat assessment on Nigeria.

<https://www.cyfirma.com/research/cyber-threat-assessment-on-nigeria/>

Daniel, S. (2026, August 4). INTERPOL identifies Nigeria as both origin and target of African cybercrime operations. Nairametrics.

<https://nairametrics.com/2026/08/04/interpol-identifies-nigeria-as-both-origin-and-target-of-african-cybercrime-operations/>

Deloitte. (2025). Nigeria's cybersecurity landscape in 2025.

<https://www.deloitte.com/ng/en/services/consulting-risk/perspectives/Nigerias-cybersecurity-landscape-in-2025.html>

Fortinet. (2026). 2026 cybersecurity skills gap global research report.

<https://www.fortinet.com/content/dam/fortinet/assets/reports/2026-cybersecurity-skills-gap-report.pdf>

Ibeh, R. (2026, July 30). Nigeria battles 1.6m online cyberattacks in H1 2026 as AI threats escalate. BusinessDay.

<https://businessday.ng/technology/article/nigeria-battles-1-6m-online-cyberattacks-in-h1-2026-as-ai-threats-escalate/>

INTERPOL. (2026). INTERPOL report finds AI linked to more than half of cybercrime in Africa.

<https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-finds-AI-linked-to-more-than-half-of-cybercrime-in-Africa>

Kanali, N. (2026, July 30). Kaspersky says Kenya among top targets for web attacks in H1 2026. Africa Business Communities.

<https://africabusinesscommunities.com/tech-24/kaspersky-says-kenya-among-top-targets-for-web-attacks-in-h1-2026/>

Mastercard. (2026). The cyber pulse report 2026.

<https://www.mastercard.com/content/dam/mccomshared/business/cybersecurity-fraud-prevention/images/cyber-pulse-report-2026/Mastercard%20Cyber%20Pulse%20-%20EEMEA.pdf>

Microsoft. (n.d.). What is business email compromise (BEC)?
<https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec>

Microsoft. (2026, November 17–20). Advanced threat detection with User and Entity Behavior Analytics (UEBA) [Conference presentation]. Microsoft Ignite, Atlanta, GA, United States.
<https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics>

Microsoft Threat Intelligence & Microsoft Defender Security Research Team. (2026, April 30). Email threat landscape: Q1 2026 trends and insights. Microsoft Security Blog.
<https://www.microsoft.com/en-us/security/blog/2026/04/30/email-threat-landscape-q1-2026-trends-and-insights/>

Mordor Intelligence. (2025a). Africa cybersecurity market size, share analysis: Growth trends and forecast (2026–2031).
<https://www.mordorintelligence.com/industry-reports/africa-cybersecurity-market>

Mordor Intelligence. (2025b). Nigeria cybersecurity market size, share analysis: Growth trends and forecast (2026–2031).
<https://www.mordorintelligence.com/industry-reports/nigeria-cybersecurity-market>

Mordor Intelligence. (2025c). South Africa cybersecurity market size, share analysis: Growth trends and forecast (2026–2031).
<https://www.mordorintelligence.com/industry-reports/south-africa-cybersecurity-market>

PwC. (2024a, October). Strengthening cyber defences: The road to resilience in East Africa – 2025 East Africa digital trust insights survey.
<https://www.pwc.com/mu/en/east-africa-dti/2025-East-Africa-DTI-Survey-Insights.pdf>

PwC. (2024b, November 20). Global digital trust insights survey 2025: South Africa report.
<https://www.pwc.co.za/en/press-room/global-digital-trust-insights-survey-2025-south-africa-report.html>

Serianu. (2025). Africa cybersecurity report – Kenya 2024/2025: From risk to resilience: AI and the future of cyber risk management.
<https://www.serianu.com/downloads/Africa%20Cybersecurity%20Report%20-%20Kenya.pdf>

World Economic Forum. (2026a). Global cybersecurity outlook 2026.
<https://www.weforum.org/publications/global-cybersecurity-outlook-2026/>

World Economic Forum. (2026b, January 12). Global cybersecurity outlook 2026: Regional analysis – Sub-Saharan Africa.
<https://www.weforum.org/publications/global-cybersecurity-outlook-2026/regional-analyses/>

Contributors

This report draws directly on primary research, technical insights, and operational expertise from key leaders across the African cybersecurity, technology, and regulatory ecosystem. We express our gratitude to the following contributors for their invaluable time, perspectives, and industry leadership in shaping this work:

- Olusegun Adeniyi - Chief Digital Officer, Wema Bank
- Obiora Awogu - Chief Information Security Officer (CISO), MoMo from MTN
- Dr. Krishnan Ranganath (Krish) - Chief Executive Officer, UniCloudAfrica
- Sunday Mgbogu - Head of Engineering, Datamellon
- Abayomi Adebajo - Director Legal, Equinix
- Ibukunoluwa Owa - Head, Regulations Unit, Nigeria Data Protection Commission (NDPC)
- Kelechi Ohaleté - Head of Governance, Risk and Control, Rack Centre
- Michael Ojih - Chief Information Security Officer, Transactworld Digital Services
- Ayodeji Jaiyeola - Chief Information Security Officer, Hydrogen Financial
- Gbemisola Osunrinde - Chief Executive Officer, Smartcomply
- Olugbolahan Olusanya - Territory Director (Africa), TeKnowledge
- Werner Lindemann - Chief Executive Officer, Data Group IT
- William Makatiani - Chief Executive Officer, Serianu Limited

About Heirs Technologies

Heirs Technologies is Africa's digital transformation partner empowering businesses through the delivery of innovative solutions crafted for the African context while adhering to global standards. We specialise in delivering world-class solutions in Cybersecurity & Digital Trust, Data & AI, Cloud & Infrastructure, Managed Services and Enterprise Products.

As a subsidiary of Heirs Holdings, the leading pan-African investment company with investments across 24 countries and four continents, Heirs Technologies is committed to the principles of Africapitalism and is strategically positioned to accelerate digital transformation across Africa.

