Africa Cybersecurity Threat Outlook 2026

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

About this report

This report is designed for executive and strategic decision-makers, including board members, Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), Chief Technology Officers (CTOs), Chief Risk Officers (CROs) and policy advisers who must decide their strategy and roadmap investment based on the current-state evolution of the cyber threat landscape.

Each section translates complex technical intelligence into accessible, strategic insights. The EY Africa team breaks down actor behaviours, sector-specific highlights, as well as policy and other implications that will shape cyber decision-making in 2026 and beyond.

It synthesises findings from EY Global Cybersecurity Threat Outlook 2026 and complements them with observed patterns drawn from the experience of EY member firm professionals in Africa across various sectors. It is written at a regional level – the intent is to reflect patterns and implications for Africa as a whole, not to describe any one country or institution.

Where the EY global report provides quantified global indicators, we quote those metrics directly. Where Africa-specific figures are not available, we translate the global trends into Africa-relevant implications and clearly frame them as regional observations rather than statistical claims.

Contacts:

Ritesh Guttoo
Tech Transformation Leader (Southern Africa) and Cybersecurity Leader (Africa)
ritesh.guttoo1@mu.ey.com

Jan Nel
Cybersecurity Leader, South Africa
jan.j.nel@za.ey.com

Pramod Potharaju
Cybersecurity Managed Service Leader, Africa
pramod.potharaju@mu.ey.com

Shameem Goolamun
Cyber GRC and Data Privacy Leader, Africa
shameem.goolamun@mu.ey.com

> "Across Africa, the number of successful cyber breaches is accelerating, marking a shift from theoretical risk to lived operational reality. As organisations have rapidly adopted cloud platforms, digital channels, automation and new technologies, many have discovered - often through painful experience - that their security posture has not evolved at the same pace.
>
> Too many environments remain designed to protect the perimeter of yesterday, while today's threat landscape exploits identity, connectivity and complexity at scale. As attacks continue to grow in frequency and sophistication through 2026 and beyond, CISOs and CIOs must resist the temptation of short-term, reactive solutions and instead reassess their cyber architecture, prior investments and resilience strategy to defend, withstand and recover in a persistently hostile environment.
>
> **Ritesh Guttoo**

Executive Summary

Executive summary

Across Africa, cyber risk has shifted from episodic IT events to systemic, business-compromising threats. The year 2025 marked a structural inflection point: cyber attack accelerated in speed, scale and coordination; identity, data and digital trust overtook infrastructure as the primary attack surfaces; and regulators moved decisively from guidance to enforcement, materially increasing board and executive accountability for cyber resilience outcomes.

Against this backdrop, this report examines 12 key cyber trends emerging across Africa, which are reshaping the threat landscape and will directly influence the cyber posture, risk exposure and resilience priorities of organisations operating across the region.

Cyber risk is a major concern, with some countries and sectors more impacted than others

As African governments and enterprises accelerate digital transformation, automation and data-driven service delivery, the impact of cyber attacks has become significantly more damaging. Increased reliance on digital identity platforms, integrated payment systems, real-time operations technology and interconnected third-party ecosystems means that cyber incidents now propagate rapidly across services, value chains and national borders. As a result, cyber attacks increasingly translate into service outages, economic disruption, regulatory exposure and loss of public trust.

Between 2024 and 2025, organisations across Africa experienced a series of high-impact cyber incidents affecting government services, financial institutions, telecommunications networks, mining and infrastructure operators. In South Africa, cyber attacks targeting digitally enabled government and logistics platforms disrupted critical public services and transport operations, demonstrating how operational resilience is increasingly dependent on cyber resilience. In the mining sector, the growing digitisation of production systems and remote operations has heightened exposure, with attacks resulting in halted production, safety concerns and supply chain delays with direct economic impact.

The financial services sector has seen particularly severe consequences as mobile banking, digital payments and application programming interface (API)-based integrations expand across markets. Banks and financial institutions in countries like Nigeria, Kenya, South Africa and Mauritius experienced ransomware, phishing and account-takeover attacks during 2024 to 2025, leading to customer access disruption, attempted fraud and the potential exposure of sensitive financial and identity data. These incidents highlight how trust, rather than infrastructure, has become the primary attack surface for Africa's digital financial ecosystem.

Similarly, telecommunications operators, which underpin digital government, mobile financial services and critical communications, have emerged as high-value targets. Cyber intrusions affecting telecom environments in many countries across Africa resulted in unauthorised access to large volumes of customer personal information, amplifying regulatory, privacy and reputational risk across multiple downstream sectors.

In Mauritius, cyber attacks against highly digitised public and private sector environments illustrate how smaller, connected jurisdictions are increasingly exposed to sophisticated, cross-border threat actors.

Taken together, these incidents demonstrate that as digital agendas mature across Africa, cyber risk is no longer confined to individual organisations or systems. Instead, it represents a systemic, cross-sector and cross-border risk, with material operational, financial, regulatory and societal consequences for governments, industries and economies as a whole.

Summary of key threats shaping Africa's outlook

- Identity-led compromise (credential theft, token/session hijacking, OAuth abuse) is outpacing exploit-driven malware as the most reliable access path across African organisations.
- Operational disruption is becoming the dominant strategic risk: ransomware, destructive attacks and precautionary shutdowns are translating directly into downtime, revenue loss and systemic service impact.
- Cybercrime and geopolitics are converging, with state-aligned operations, influence campaigns and criminal ecosystems increasingly sharing infrastructure, tooling and techniques.
- Critical sectors — financial services, telecommunications, energy, transport and government — face systemic exposure due to high interdependency and complex third-party ecosystems.
- Supply-chain and fourth-party risk are expanding the blast radius of incidents; software bill of materials (SBOM), vendor access governance and continuous assurance are now board-level priorities.
- Skills shortages and uneven cyber maturity are accelerating reliance on outsourcing, automation and AI-assisted detection and response.
- AI is compressing decision cycles, accelerating both offence (deepfakes, agentic campaigns, automated reconnaissance) and defence (behavioural analytics, automated triage and response).

This table summarises the cyber threat types most frequently observed across the Africa region in recent months, highlighting the primary threat actors, attack patterns, impacted sectors, and areas of highest geographic visibility.

Threat Actor	Incident Type	Key Impacted Sectors	Most Seen (Geographic Visibility)
Cybercriminal syndicates (financially motivated)	Ransomware	All	Across Africa
Cybercriminal syndicates/Initial Access Brokers	Data Leakage/Data Exfiltration	Telecommunications Financial Services Healthcare	Southern Africa, West Africa, North Africa
Organised fraud groups	Financial Fraud (BEC, SIM-swap, payment diversion)	Financial Services	West Africa, Southern Africa, East Africa
Hacktivist groups/ politically motivated actors	Denial of Service (DDoS)	Internet banking Government portals E-commerce sites	Southern Africa, North Africa, during periods of political tension
Cybercriminals (credential harvesters)	Credential Compromise (leading initial access vector; ~160% year-over-year (YoY) exposure increase)	All	Southern Africa, West Africa
Cybercriminals/Social-engineering actors	Phishing and Social Engineering	Financial services Government Telecommunications	Pan-African, with highest reporting in West and Southern Africa
Cybercriminal syndicates/Data brokers	Data Breach (unauthorised access to systems)	Government Financial services Healthcare	Southern Africa, East Africa, North Africa
Cybercriminals targeting critical infrastructure	Operational Disruption (cyber impact on operational technology (OT)/logistics)	Ports Energy Transport	Southern Africa, West Africa (major trade and logistics hubs)
AI-enabled fraud actors/impersonators	Deepfake and AI-enabled Impersonation	Financial services Government Public figures	Southern Africa, East Africa; rapidly emerging Pan-African
Opportunistic attackers/global exploit campaigns	Exploitation of Unpatched Systems and Platforms	Government Large enterprises Regulated sectors	Southern Africa, North Africa (legacy and on prem environments)

Note: For the purposes of this report, the Southern Africa region includes **South Africa, Namibia and Mauritius**, alongside other countries within the Southern African sub region.

Trend 01

Africa is increasingly exposed to identity-led attacks, not "classic malware"

As organisations digitise at speed, cyber risk is shifting from malware to identities, access and trust. In Africa, rapid cloud adoption and fragmented identity controls are making identity a critical determinant of resilience.

Trend 1

Africa is increasingly exposed to identity-led attacks, not "classic malware"

The most consequential intrusions increasingly begin with identity rather than malware. The EY Global Cybersecurity Threat Outlook 2026 observes that identity systems will surpass endpoints and networks as the dominant attack surface; credential abuse, token theft, session hijacking and federation misuse are expected to continue to outpace exploit-driven malware because they are lower cost and yield higher success rates.

In Africa, this global shift has outsized impact for three reasons. First, rapid digital growth has expanded cloud and software as a service (SaaS) adoption faster than identity governance maturity. Second, organisations often operate complex group structures (subsidiaries, joint ventures, outsourced operations) with fragmented directories and inconsistent multi-factor authentication (MFA) enforcement. Third, ecosystems such as mobile money, agency banking and shared service call centres create large populations of high-risk identities and privileged operational accounts.

Africa-relevant attack patterns

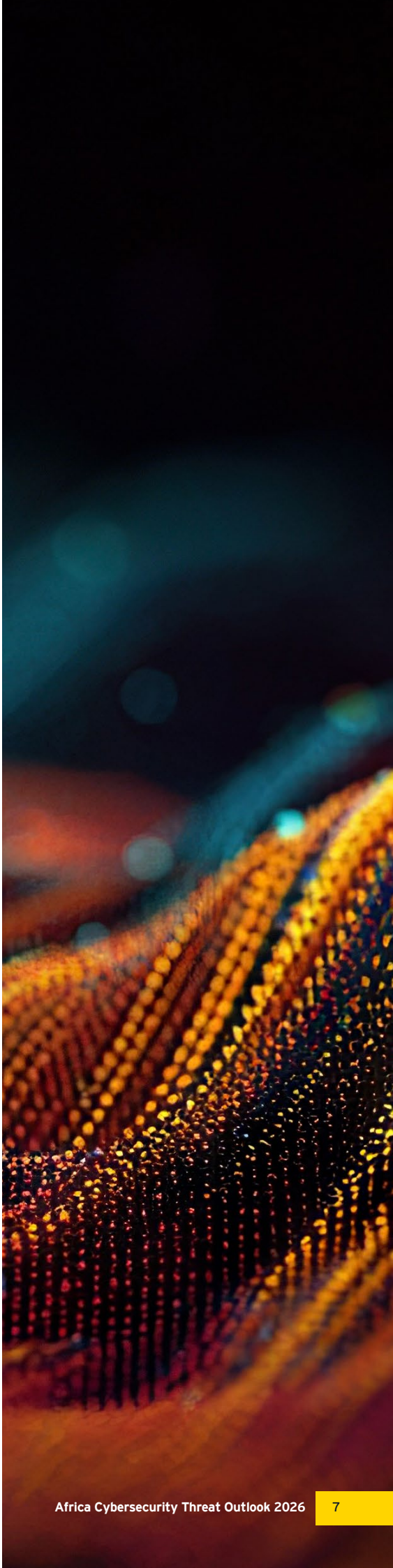
- Credential compromise and session hijacking leading to email and collaboration account takeover (business email compromise (BEC), invoice diversion and executive impersonation).
- Token abuse (OAuth consent grants, refresh-token theft) enabling 'malware-optional' persistence and API-level data exfiltration.
- Privileged access sprawl and stale accounts across hybrid environments, creating lateral movement paths.
- Identity compromise via third-party access (support vendors, integrators, managed services) where the attacker leverages legitimate remote tooling.

Illustrative incident example of identity-led cloud takeover

- A regional financial institution experienced a major security incident after the identity of a privileged cloud administrator was compromised through a phishing led credential and session token theft. Rather than deploying malware, the threat actor authenticated legitimately into the organisation's cloud identity platform and escalated permissions within the tenant control plane.
- Within hours, the attacker created additional administrative accounts, granted persistent OAuth application access, disabled selected security controls and redirected email and audit logs to evade detection. This enabled full takeover of the cloud tenant, access to core applications integrated via single sign on, and the staging of downstream fraud and data exfiltration activity — all without triggering traditional endpoint or network based security alerts.

Board-level implications

Boards should treat identity as critical infrastructure. The relevant performance question isn't 'do we have MFA?' but 'is identity continuously defended and monitored as a Security Operations Centre (SOC) function?' Executive oversight should focus on phishing-resistant MFA for privileged roles, token/session protection, rapid access revocation, and measurable reduction in privileged pathways.



Trend 02

Cybercrime and geopolitics are converging, with Africa in the blast radius.

As state-linked and criminal cyber activity converge, Africa's concentrated telecom, payments and cloud dependencies increase exposure, turning geopolitical shocks elsewhere into local disruption, surveillance risk and operational consequences across sectors and borders.

Trend 2

Cybercrime and geopolitics are converging, with Africa in the blast radius

EY Global Cybersecurity Threat Outlook 2026 notes that state-sponsored cyber operations have matured into a visible instrument of national power, alongside diplomatic and economic tools, and that attribution is becoming harder as state-aligned actors blend espionage, disruption and influence operations. The Middle East and Africa (MEA) section further highlights that cyber activity in the region is often an extension of political influence and state competition, with disruptive intent outweighing pure data theft.

For African organisations, 'blast radius' is amplified by the concentration of national services and cross-border dependencies: regional payment rails, shared telecom backbones, cloud tenancy consolidation, and reliance on a limited set of infrastructure vendors. This means geopolitical activity elsewhere can translate into local operational risk through supply chain compromise, botnet-driven disruption, and credential markets.

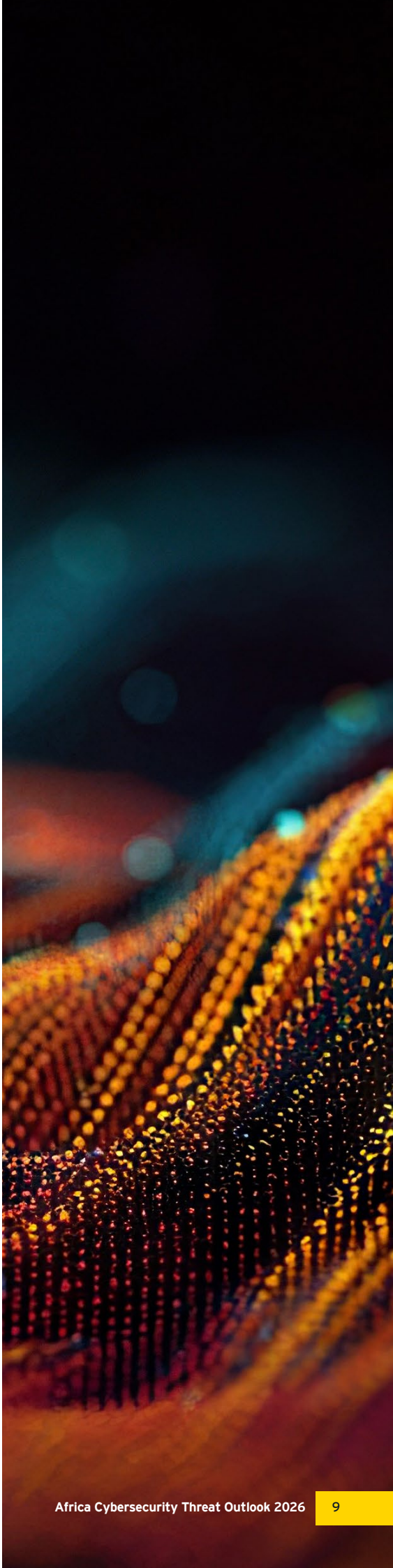
Mass-surveillance and lawful-intercept risk (HNDL-style threats)

A growing concern for governments and financial institutions is surveillance-oriented compromise of communications infrastructure. Telecom networks are increasingly treated as intelligence targets, and the EY global report references campaigns focused on persistent access to telecom backbones for surveillance and traffic insight. In parallel, EY Global Cybersecurity Threat Outlook 2026 flags satellite communication weaknesses that exposed sensitive data.

In this environment, boards should assume that fibre routes, subsea links, satellite backhaul and legacy microwave may be monitored or intercepted by capable adversaries. Independent research has highlighted that many satellite systems historically transmitted command links without encryption, leaving data susceptible to interception at scale. For high-risk sectors (government and financial institutions), this elevates requirements for strong encryption-by-default, frequent key rotation, secure key management, and an explicit 'communications assurance' control framework aligned to national security expectations.

Priority actions for boards

- Treat telecom and connectivity as a critical dependency: mandate joint incident scenarios that assume national-level disruption and surveillance exposure.
- Review encryption posture across high-risk communications paths (satellite, backhaul, cross-border links) and adopt key-rotation and crypto-agility practices.
- Align cyber crisis governance with geopolitical risk governance — define escalation thresholds, comms strategy, and regulator engagement plans.



Trend 03

Critical sectors in Africa mirror the high-impact targets identified by the global EY organisation

Across Africa, the sectors most essential to national stability, telecom, energy, finance, transport and public platforms, are also the most exposed, making cyber resilience inseparable from service continuity, safety and economic stability.

Trend 3

Critical sectors in Africa mirror the high-impact targets identified by the global EY organisation

EY Global Cybersecurity Threat Outlook 2026, identifies critical sectors as the operational front lines of modern cyber risk because of their role in national stability: telecommunications, infrastructure, utilities, healthcare, finance, transportation and aviation. In Africa, the same sectors tend to be more tightly coupled to national service delivery (payments, identification, connectivity, energy and logistics), increasing the systemic consequences of disruption.

National digital platforms and "single points of failure"

Many countries rely on a small number of national platforms: national ID and civil registries, payment switches, tax and customs systems, and integrated e-government portals. When these are disrupted, the economic and societal impact often exceeds the direct IT recovery cost.

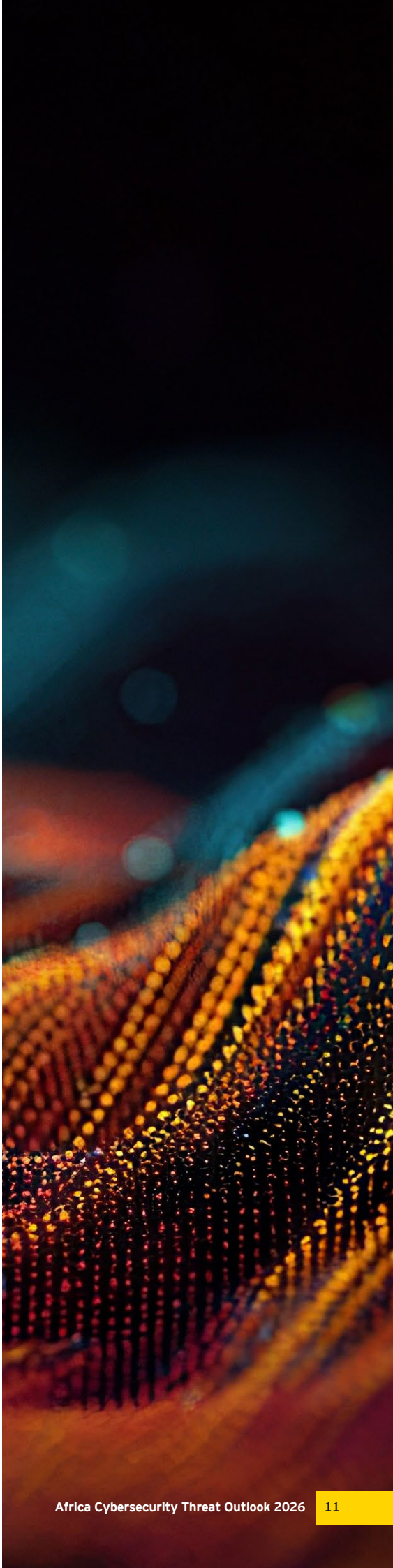
Beyond IT: OT as the leverage point (energy, aviation, mining, metro)

EY Global Cybersecurity Threat Outlook 2026 highlights increasing focus on operational technology (OT) and critical infrastructure, noting that cyber incidents now threaten physical safety and operational continuity and that OT will remain a preferred leverage point. For Africa, OT exposure is particularly material in power generation and grids, oil and gas logistics, aviation operations, mining processing plants, and urban rail/metro systems.

- **Energy grid operations:** precautionary isolation and conservative shutdowns can trigger load shedding, market instability and political scrutiny.
- **Aviation and airports:** ransomware and outages can disrupt ticketing, baggage, cargo and safety-related coordination, with cascading delays.
- **Mining:** IT-to-OT pivot can halt extraction and processing; safety visibility (ventilation, monitoring) becomes a risk dimension.
- **Metro and rail:** disruption of signalling, dispatch or passenger systems can create both safety and public-order implications.

Board-level observation

In these sectors, the correct resilience question is not 'can we restore systems?' but 'can we continue delivering critical service safely while systems are degraded?'. Boards should require OT-aware incident response playbooks, segmentation validation and recovery exercises that include safety, regulatory and public communications decisions.



Trend 04

Ransomware in Africa is more about service disruption, than ransom payments

Across Africa, ransomware is primarily a disruption threat: attackers aim to halt essential services, weaken recovery options and force crisis decisions, making operational resilience and recoverability more important than ransom economics.

Trend 4

Ransomware in Africa is about service disruption, not ransom payments

Ransomware remains the most disruptive threat class. Research by EY teams, cited in EY Global Cybersecurity Threat Outlook 2026, found ransomware accounted for 25.9% of all reported incidents in 2025, and the report emphasises that operational disruption is now the dominant strategic risk. In Africa, ransomware campaigns frequently aim to halt operations and force crisis decisions, especially in logistics, healthcare, municipalities, utilities and financial administration.

Illustrative Africa incidents

Publicly reported incidents across Africa show ransomware increasingly being used as a tool for operational disruption rather than purely data encryption. Attacks have targeted logistics networks, public-sector and government-linked entities, and large pension and benefits administration environments, resulting in sustained service outages and systemic impact. In many cases, ransom demands were driven less by the threat of data exposure and more by the urgency to restore critical services and operational continuity.

Pre-encryption reconnaissance and backup compromise

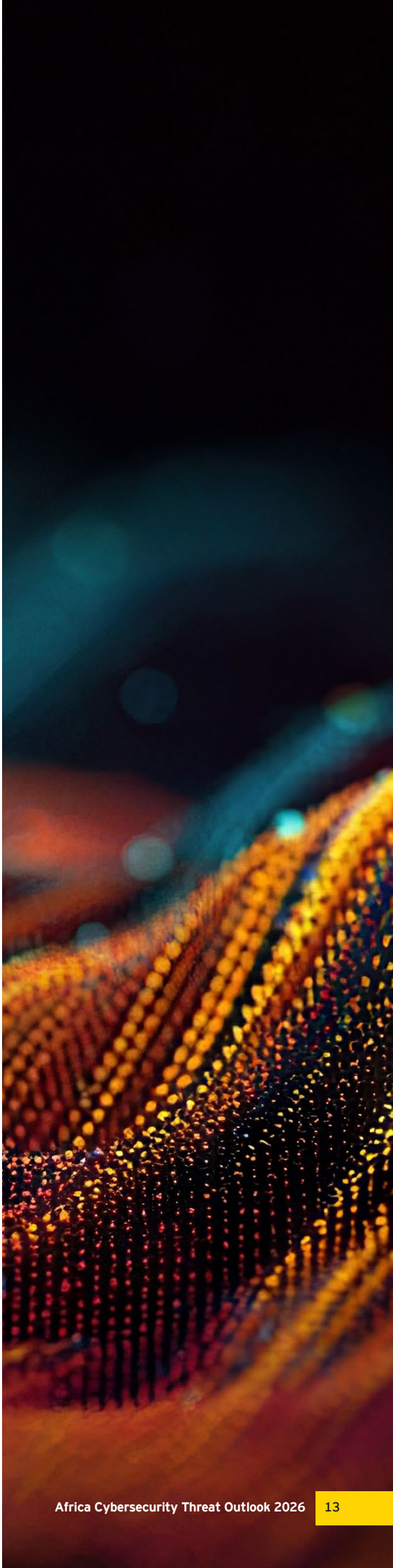
Modern ransomware operations increasingly include extended reconnaissance and deliberate targeting of backups and disaster recovery (DR) capabilities prior to encryption. EY Global Cybersecurity Threat Outlook 2026, highlights 'pre-encryption reconnaissance' and the need to validate backup resilience and run recovery simulations. From our Africa delivery experience, it is common to find adversaries maintaining persistence for extended periods (often months) to map the environment, harvest credentials, and sabotage recovery pathways.

Many organisations are changing backup systems

A growing number of organisations are redesigning backup architectures in response: shifting to immutable backups, offline and air-gapped copies, hardened backup identity controls, and frequent restore testing. This aligns with EY Global Cybersecurity Threat Outlook 2026 observation that organisations that fared best had rehearsed incident command structures and immutable backups.

Board questions to ask

- Can we restore critical services without negotiating with attackers, and have we proven it through recent full restore tests?
- Are backups protected by separate identities and segmented networks, with immutable storage and tamper detection?
- Do we monitor for early-stage attacker behaviour (credential theft, privilege escalation, backup deletion attempts) rather than waiting for encryption?
- Is our DR site architected to avoid 'shared fate' with production (identity, admin tooling, monitoring and backup planes)?



Trend 05

Third-party and ecosystem risk is a major blind spot in Africa

Across Africa, cyber exposure increasingly sits beyond the enterprise boundary, as dense vendor ecosystems and hidden fourth-party dependencies create pathways for disruption, data compromise and regulatory fallout, making ecosystem assurance a core resilience priority.

Trend 5

Third-party and ecosystem risk is a major blind spot in Africa

Ecosystem exposure is now the new perimeter. EY Global Cybersecurity Threat Outlook 2026, emphasises third-party oversight and highlights supply chain risk, SBOM requirements, and vendor scoring as strategic priorities. African organisations often operate with dense vendor ecosystems: fintechs, mobile money partners, systems integrators, outsourced call centres, shared data centres, and cloud/SaaS providers.

Third-party and fourth-party risk

Third-party incidents are increasingly driven by fourth-party dependencies (your vendor's vendor). In practice, vulnerabilities in widely deployed software components, managed services tooling, and shared hosting platforms can cascade across multiple institutions. Boards should require mapping of critical service chains and explicit controls for access, logging, and incident notification across tiers.

Regulatory exposure and breach consequences

Regulatory expectations are tightening both globally and across African markets, with a clear shift from guidance to enforcement and increasing executive accountability. In the African context, recent incidents involving the potential compromise of personal and financial information at scale have highlighted the downstream risks of identity fraud, large-scale notification obligations and regulatory scrutiny, underscoring the material impact of identity-driven breaches beyond the initial cyber event.

Contractors as an extended attack surface

The increasing reliance on contractors and temporary resources for software development and IT administration is materially expanding organisational risk. These roles often require elevated or persistent access to source code repositories, cloud administration platforms and sensitive environments, yet vetting, validation and oversight processes are frequently inconsistent across jurisdictions and delivery models. Where contractor identities are insufficiently vetted, over privileged, or not tightly scoped to time-bound tasks, they become a high-value target for compromise or misuse. In complex ecosystems, a single contractor account can provide indirect access to multiple systems, tenants or clients, amplifying blast radius well beyond the immediate engagement. Without rigorous identity assurance, access lifecycle management and continuous monitoring, organisations risk introducing systemic exposure through the very resources intended to accelerate delivery and reduce skills gaps.

Board priorities

- Adopt continuous third-party assurance for critical vendors (not annual questionnaires): access governance, telemetry, and incident response integration.
- Mandate least-privilege vendor access with time-bound approvals, monitored sessions, and rapid revocation.
- Require contractual right-to-audit and defined breach notification timelines, including fourth-party disclosure obligations.

> "Organisations increasingly operate through complex ecosystems where exposure is driven not just by direct vendors, but by extended supply chains that remain poorly understood and insufficiently governed.
>
> Effective risk management now requires GRC functions to continuously discover external parties, classify them based on risk, and automate monitoring across cyber, data and operational dimensions—enabling timely visibility of exposures and informed actions before risks materialise.
>
> **Shameem Goolamun**

Trend 06

Skills gaps and response readiness remain structural constraints

Across Africa, cyber resilience is still constrained by scarce experienced capacity and uneven preparedness, driving greater reliance on managed services, automation and AI to strengthen detection, accelerate response and improve operational readiness.

Trend 6

Skills gaps and response readiness remain structural constraints

EY Global Cybersecurity Threat Outlook 2026, notes that skills gaps persisted even where resilience improved, and emphasises intelligence-driven detection and automated triage for machine-speed attacks. The latest Africa Cyberthreat Assessment Report from, INTERPOL, similarly observes that while African countries have taken steps to improve cyber resilience, significant investigative challenges remain, and insufficient cyber hygiene continues to undermine preparedness.

New risk dynamics emerging from cyber skills gaps

Beyond capacity constraints, sustained shortages in experienced cyber professionals are introducing new categories of risk. Limited depth in security engineering, incident response and threat analysis increases the likelihood of misconfigurations, delayed decision making during live incidents, and over reliance on default tooling or external guidance. In high-pressure scenarios, organisations may struggle to distinguish signal from noise, validate automated alerts, or challenge vendor-driven recommendations—leading to either over reaction, such as precautionary shutdowns, or under reaction where early indicators are missed. This skills asymmetry also weakens governance over privileged access, cloud configurations and identity controls, creating conditions where sophisticated identity led attacks can persist undetected. As a result, skills gaps are no longer just an efficiency issue; they have become a structural risk factor that directly affects response quality, containment speed and executive confidence during cyber crises.

Africa trends: outsourcing, automation and AI-assisted operations

A visible regional pattern is the increase in organisations outsourcing cyber functions (SOC operations, threat hunting, vulnerability management and incident response) to managed security providers, and investing in automation and AI to compensate for scarce experienced capacity. The goal isn't to replace human knowledge, but to compress detection and response timelines and to standardise evidence generation for regulators and auditors.

Board-level operating model signals

- Shift from tool accumulation to outcome-focused operations: fewer tools, better telemetry, faster triage.
- Adoption of extended detection and response (XDR)/security information and event management (SIEM) modernisation, identity threat detection and response (ITDR) and automated containment playbooks.
- Regular crisis simulations that assume material disruption and test executive decision authority.
- Evidence-by-design: operational dashboards that produce audit-ready artefacts as a byproduct of security operations.

> “Cyber skills gaps are becoming a structural risk - now amplified by AI. Shortages across security engineering, cloud, identity and AI-enabled defence are limiting organisations' ability to secure and operate increasingly automated and complex environments.
>
> For African organisations, this is no longer a talent pipeline issue. As AI raises the speed and sophistication of both attacks and defences, resilience depends on reducing dependency on scarce skills through AI-assisted operations, automation and managed expertise through trusted partners, rather than assuming gaps can be closed through hiring alone.
>
> **Jan Nel**

Trend 07

AI disruption – Mythos, zero-days and the collapse of patch windows

Across Africa, AI is accelerating both deception and exploitation, compressing patch windows beyond what legacy and OT-heavy environments can absorb, making continuous exposure management, compensating controls and faster remediation essential to resilience.

Trend 7

AI disruption – Mythos, zero-days and the collapse of patch windows

AI is reshaping the threat landscape on two fronts: AI-enabled deception (deepfakes, synthetic identities) and AI-accelerated vulnerability discovery with exploitation. Global Cybersecurity Threat Outlook 2026 highlights AI-driven social engineering and notes a median six-day gap between vulnerability disclosure and weaponisation in 2025.

Mythos and automated zero-day discovery

In April 2026, multiple industry sources reported that a leading generative AI (GenAI) model demonstrated autonomous capability to discover and exploit zero-day vulnerabilities at scale, triggering the launch of a defensive initiative to use these capabilities responsibly. Independent evaluations reported the model completing multi-step enterprise attack simulations under controlled conditions. Whether or not such capabilities become broadly accessible, the strategic implication is clear: patch windows will continue to compress, and defenders must design for 'assume exploit' conditions.

Africa's patch management challenge

Across many African organisations, patch governance is constrained by legacy platforms, limited maintenance windows, and OT environments that cannot be patched. As exploit timelines compress, manual patching and spreadsheet-based exception management become untenable. Boards should demand automation and risk-based prioritisation, focusing on Known Exploited Vulnerabilities (KEV) first, with clear accountability for exposure closure and compensating controls where patching is not feasible.

Leading organisations, particularly within the financial services sector, are increasingly testing AI-assisted and autonomous patching approaches to close exposure gaps at both infrastructure and application code levels. Rather than relying solely on periodic patch cycles, these models use continuous vulnerability discovery, exploit intelligence and automated testing to prioritise and deploy fixes at machine speed, with built-in safeguards to reduce operational risk.

AI-enabled deception and deepfake-driven attacks

A growing area of concern is the use of AI enabled impersonation, including voice cloning and synthetic video or messaging, to manipulate trusted business processes. These attacks target executives, finance teams and regulators, bypassing technical controls by exploiting trust and urgency. Traditional indicators of compromise are often absent, requiring organisations to redesign approval workflows and verification processes to assume impersonation rather than exception.

Board actions

- Move to continuous exposure management: asset inventory, vulnerability intelligence and prioritised remediation at cadence.
- Adopt compensating controls for unpatchable systems: virtual patching, segmentation, strong identity controls, and continuous monitoring.
- Set enterprise-wide service-level objectives for critical patching and enforce exception governance.

"AI is changing how vulnerabilities are discovered. Advanced models can now autonomously identify previously unknown weaknesses across code and environments at machine speed, compressing the time between exposure and exploitation.

For African organisations, resilience will not come from adding another security tool. It requires engaging trusted partners that bring AI accelerators, proven models and automated workflows to rapidly uplift vulnerability discovery and remediation within existing environments.

Pramod Potharaju

Trend 08

The CISO accountability gap – responsibility without control

Across Africa, cyber resilience is often weakened by a gap between accountability and authority, as CISOs are expected to deliver outcomes without control over the operational levers needed to reduce risk and respond decisively.

Trend 8

The CISO accountability gap – responsibility without control

Regulators and boards increasingly expect visible executive ownership of cyber resilience. EY Global Cybersecurity Threat Outlook 2026 explicitly positions cybersecurity as a board-level priority and outlines CEO and CISO strategic priorities for 2026. Yet, across many African organisations, the CISO is held accountable for outcomes while lacking operational control over key levers: Security operations, identity administration, change windows, vendor access, and incident response authority.

Why this matters in Africa

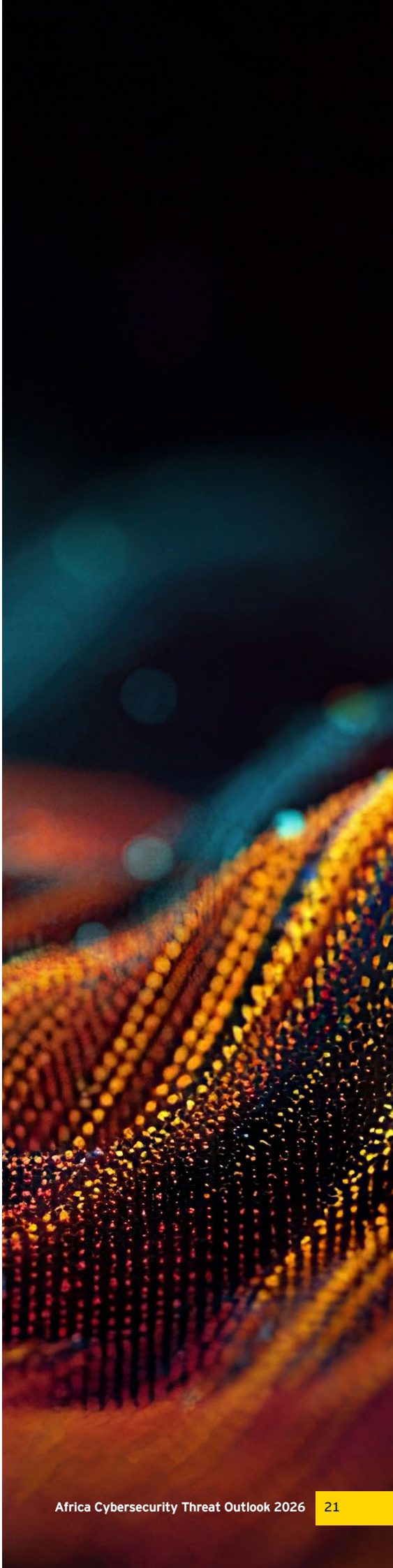
The accountability gap slows response, fragments decision-making, and encourages "policy-only" security functions that cannot move at machine speed. To close this, many organisations are redefining the CISO role beyond policy and risk management toward an operational resilience mandate: integrating cyber operations, crisis governance, and technology risk execution.

Reframing the CISO role: operational influence without loss of independence

To close the accountability gap, leading organisations are adopting hybrid operating models that give the CISO direct influence over security operations and incident response outcomes without assuming first line execution responsibility. In this model, day to day security operations, identity administration and response tooling remain embedded within technology or operations teams, while the CISO retains authority over operating standards, risk prioritisation, escalation thresholds and crisis coordination. This enables the CISO to direct action during cyber events, mandate containment measures, and validate remediation decisions in real time, while preserving the independence required to provide effective second line oversight.

Operating model shifts we see working

- CISO co-ownership of identity and privileged access governance, with authority to enforce baseline controls and emergency revocation.
- Unified cyber-resilience governance (cyber + continuity + operational risk) with clear decision rights during incidents.
- A single accountable operating model for security operations (SOC, incident response, threat intelligence), even where delivery is provided through managed service partners.
- Board dashboards that link cyber key risk indicators (KRIs) to operational outcomes (downtime, recovery time objectives, regulatory exposure).



Trend 09

Fragmented national cyber authorities and uneven regulation

Across Africa, fragmented oversight and uneven regulation create a dual-speed risk environment, allowing threats to move across borders more easily and making collaboration, shared intelligence and minimum resilience standards increasingly essential.

Trend 9
Fragmented national cyber authorities and uneven regulation

EY Global Cybersecurity Threat Outlook 2026 notes that regulatory expectations are becoming more stringent globally, while the MEA section highlights fragmented enforcement across the region. The latest Africa Cyberthreat Assessment Report from, INTERPOL, similarly notes that the absence of specific frameworks in some jurisdictions and uneven collaboration can hinder prevention, detection and disruption of cybercrime.

For Africa, this creates a dual-speed environment: some markets are moving rapidly toward stricter data protection and critical infrastructure requirements, while many organisations remain effectively unregulated or lightly supervised. This unevenness benefits threat actors: they can stage operations in lower-friction environments while targeting higher-value institutions regionally.

A critical reality: no company can defend alone

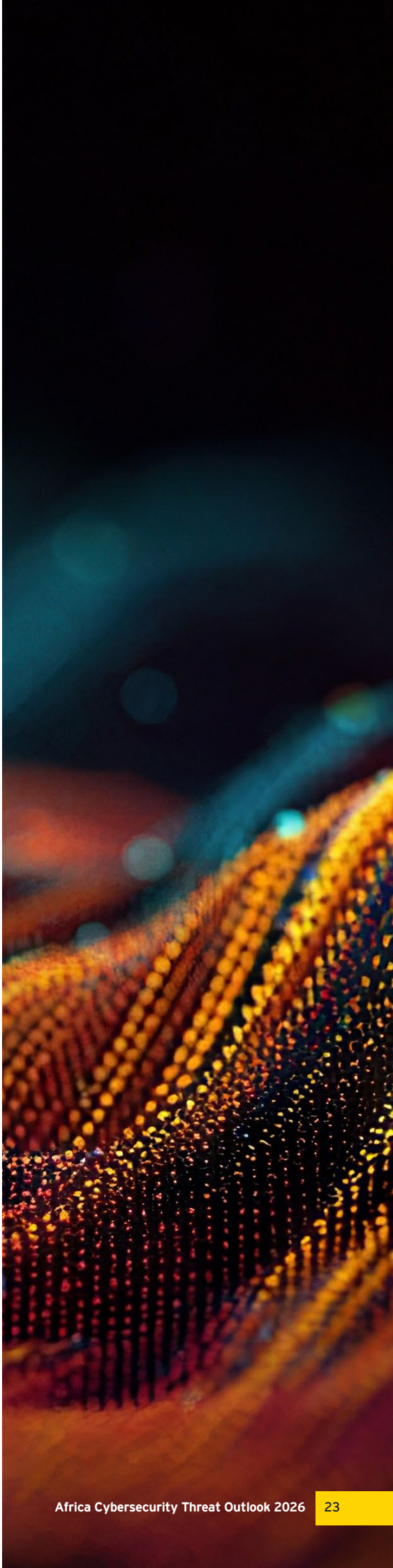
Nation-state and state-tolerated actors can sustain long-term campaigns, exploit cross-border jurisdictional gaps, and reuse shared criminal infrastructure. As a result, company-level controls must be complemented by sector-level and national-level collaboration: intelligence sharing, coordinated exercises, and minimum resilience baselines.

Across Africa, we are increasingly seeing the establishment of dedicated national cybersecurity authorities mandated to coordinate cyber risk at a national level, set minimum security baselines, and act as focal points for incident response, threat intelligence sharing and cross border cooperation. Examples include national authorities established through statute in countries such as Ghana, Rwanda and Morocco, as well as regional coordination mechanisms under initiatives such as the African Network of Cybersecurity Authorities (ANCA) facilitated by Smart Africa. These bodies are beginning to define common expectations for critical sectors, designate critical information infrastructure, and provide structured engagement between government, regulators and industry.

However, the absence of such authorities or effective coordination mechanisms in many African countries means that a significant number of organisations continue to operate without consistent national guidance, limited access to centralised threat intelligence, and little practical support during major cyber incidents. This fragmentation leaves individual institutions—particularly those handling sensitive data or operating critical infrastructure—disproportionately exposed, forced to design and defend in isolation while facing adversaries that operate across borders with shared tools and infrastructure.

Board priorities

- Participate in sector information-sharing (Information Sharing and Analysis Centre (ISAC)-style structures) and require reciprocal sharing with regulators where appropriate.
- Assume cross-border threat: design incident response and communications plans for multi-jurisdiction exposure.
- Advocate for minimum resilience baselines in critical sectors (identity controls, backup resilience, reporting and exercises).



Trend 10

Supply chain risk – software provenance, hardware trust and SBOM

Across Africa, supply chain risk is increasingly systemic, as dependence on globally sourced software, hardware and managed services expands exposure, making procurement, provenance and continuous assurance central to cyber resilience.

Trend 10

Supply chain risk – software provenance, hardware trust and SBOM

Supply chain compromise has become systemic. EY Global Cybersecurity Threat Outlook 2026 notes that supply chain risk surged and highlights SBOM as a regulatory and insurance requirement. It also describes sustained activity by major state-linked actors (including Russian and Chinese operators) targeting telecoms, energy and government, and notes that threats are borderless and ecosystem-driven.

For African organisations, supply chain risk has two layers: (1) software supply chains (open-source libraries, enterprise resource planning (ERP) platforms, managed services tooling) and (2) hardware and network equipment provenance. Given Africa's reliance on globally sourced equipment and outsourced services, boards should treat procurement as a cyber control function: security-by-design requirements, provenance checks, and continuous vulnerability disclosure obligations.

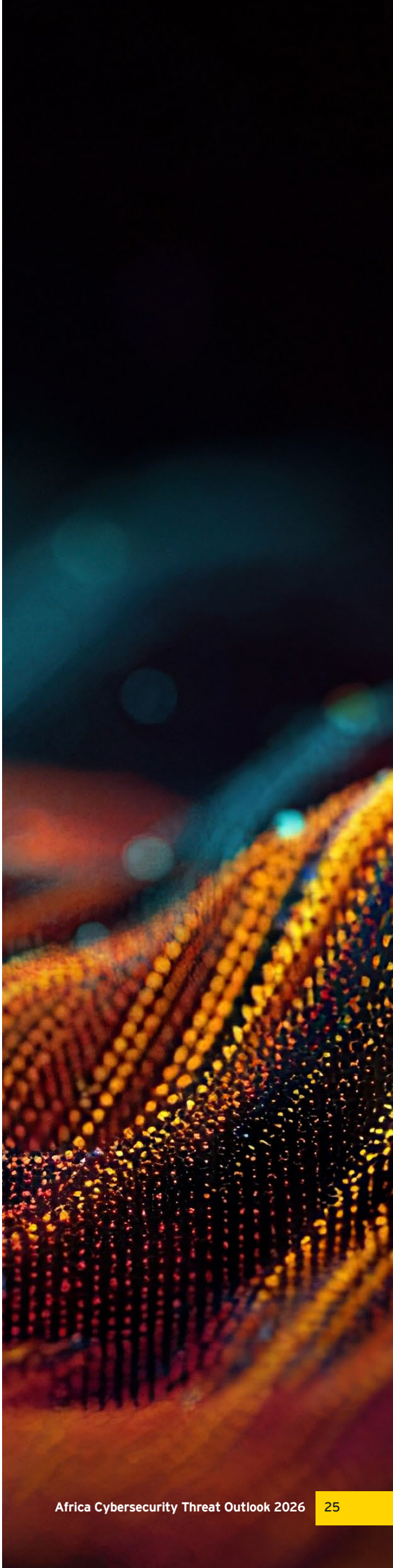
Practical governance controls

- SBOM and vulnerability disclosure requirements for critical software and managed services.
- Vendor access segmentation and monitoring, including remote maintenance accounts for network and OT environments.
- Independent validation for high-risk infrastructure components (routers, firewalls, identity platforms) and rapid patch service level agreements (SLAs).
- Supply chain incident playbooks: how you will operate if a key vendor or platform is compromised.

Example of supply-chain compromise

Incidents affecting African organisations increasingly demonstrate supply chain compromise at the software and infrastructure layer. In several cases, malicious code or backdoored components were introduced upstream through software updates, embedded open-source libraries, or vendor provided infrastructure platforms, and subsequently propagated into operational environments as trusted deployments.

As these components were distributed through legitimate update mechanisms or pre-installed systems, the activity inherited implicit trust, bypassed signature-based detection, and persisted undetected for extended periods. Post-incident analysis commonly revealed limited visibility into component provenance, dependency mapping and inherited vulnerabilities significantly delaying containment, remediation and assurance across the affected ecosystem.



Trend 11

Shadow IT and Shadow AI: invisible accelerants of risk

Across Africa, shadow IT and shadow AI are accelerating cyber exposure, as unsanctioned SaaS, cloud and AI tools bypass governance, obscure data flows and extend trust into unmonitored environments, making continuous discovery, secure enablement and rapid containment essential to resilience.

Trend 11

Shadow IT and Shadow AI: invisible accelerants of risk

The rapid adoption of cloud services and artificial intelligence is driving a surge in unauthorised technology and AI usage across African organisations. Employees, contractors and business units increasingly deploy applications, automation and AI tools outside formal governance processes in pursuit of speed and efficiency. This "shadow" activity frequently bypasses security controls, data classification and audit logging.

Shadow AI significantly amplifies risk by enabling uncontrolled data sharing, automated decision-making and model interaction without oversight. Prompts, training data and outputs may contain sensitive information, while AI-driven workflows can trigger actions at scale. Without visibility and governance, organisations lose control of where data flows, how decisions are made, and how incidents propagate. Boards should treat shadow IT and shadow AI as systemic governance risks, not isolated policy breaches.

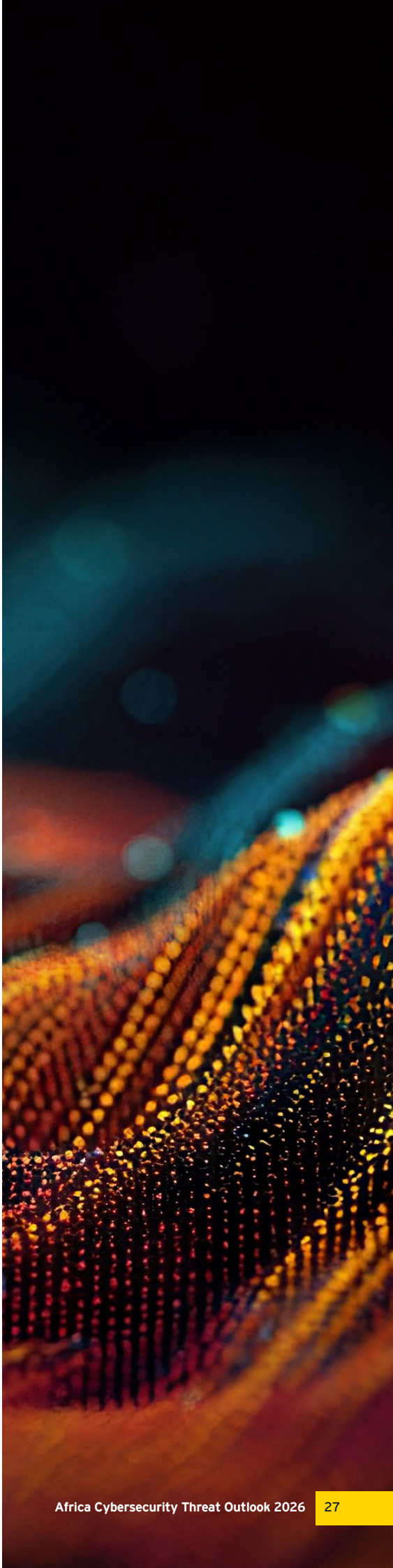
Examples of shadow IT and AI leading to material compromise

In multiple African organisations, cyber incidents have been traced back to unsanctioned SaaS and cloud services introduced by business or development teams. Once credentials associated with these shadow applications were compromised, attackers gained footholds that bypassed monitoring, patching and detection—allowing data access and lateral movement to persist undetected. In several cases, these applications were connected to core environments through shared identities or hard-coded credentials, significantly expanding the blast radius and delaying incident response when the activity was eventually discovered.

As per CISOs in the region, a more recent and distinct risk is now emerging with Shadow AI. As AI tools and development platforms proliferate, users and developers are increasingly adopting unsanctioned AI applications, browser plug-ins and public code repositories. These platforms are being actively targeted by accelerated infostealer campaigns designed to harvest credentials, session tokens and API keys. The malware often operates briefly and cleans up after execution, leaving minimal forensic artefacts. As a result, compromise is frequently identified only after anomalous cloud activity, secondary fraud or misuse of privileged access is detected.

Board priorities

- Establish continuous discovery of unsanctioned SaaS, cloud, AI tools and code repositories, with clear ownership, risk classification and authority to contain or retire high risk shadow assets.
- Move away from policy driven prohibition toward secure by design enablement: fast approval pathways for business and AI tools, embedded security guardrails, and response playbooks that assume compromise may originate from unsanctioned platforms



Trend 12

Cyber insurance as a resilience and risk-transfer lever

Across Africa, cyber insurance is becoming a more viable resilience and risk-transfer lever, as improved control maturity and underwriting discipline expand coverage availability, making policy alignment, exclusion clarity and tested response readiness essential to absorbing residual cyber impact.

Trend 12

Cyber insurance as a resilience and risk-transfer lever

Historically, many African organisations struggled to obtain meaningful cyber insurance due to high premiums, restrictive exclusions and limited capacity. This dynamic is changing. Improved cyber maturity, better underwriting data and stabilised global insurance markets have expanded coverage availability and reduced pricing volatility across the region.

Insurers are increasingly underwriting control maturity rather than geography, rewarding organisations with strong identity controls, tested backups, incident response readiness and third-party risk management. Cyber insurance is now emerging as a complementary risk-transfer mechanism, supporting incident response, legal and forensic costs, notification obligations and certain business interruption impacts. Boards should ensure cyber insurance is aligned with cyber maturity roadmaps, clearly understood exclusions, and integrated incident response planning.

The limits of cyber insurance: what it does not cover

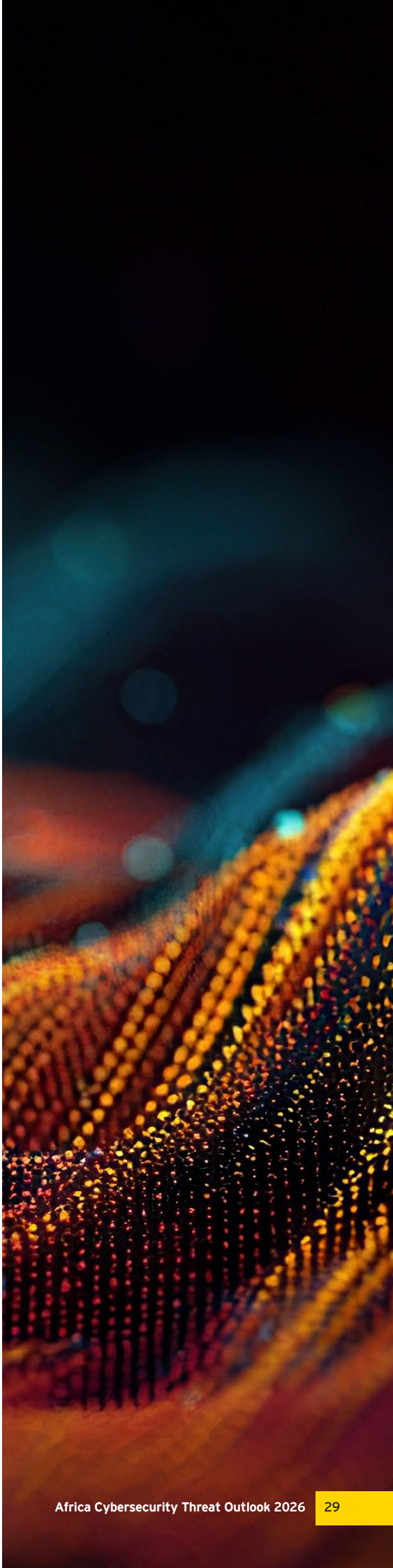
Despite its growing importance, cyber insurance isn't a substitute for cyber resilience. Coverage exclusions for systemic events, nation-state activity, prolonged outages, regulatory fines and widespread data compromise remain common. Even where an incident falls within policy coverage, claim validation and payout timelines may not align with the operational urgency of restoring services. Boards should therefore treat cyber insurance as a risk-transfer mechanism of last resort, designed to absorb residual impact - not as a primary control or a recovery strategy.

Incident response readiness is now an underwriting requirement

Insurers are increasingly underwriting response readiness, not just preventative controls. Evidence of tested incident response plans, crisis governance, executive decision authority and integration with external forensic and legal providers is now material to both coverage and claims outcomes. Organisations that cannot demonstrate response discipline, particularly at executive level, face higher premiums, narrower coverage or coverage denial during disputed claims.

Board priorities

- Regularly review cyber insurance coverage against the current and emerging threat landscape.
- Link cyber maturity improvements to premium optimisation and coverage outcomes.
- Treat cyber insurance as a complement to resilience, not a substitute.



Closing thoughts

As we move deeper into 2026, the cyber threat landscape is already evolving at a pace that outstrips many of the assumptions formed in previous years. While recent incidents and historical trends provide important lessons, organisations must increasingly look ahead - factoring in emerging technologies, geopolitical tensions and rapidly shifting attacker capabilities - to shape their future security posture.

Attackers now operate with unprecedented speed and scale, leveraging automation and AI to industrialise exploitation and compress the time between access, impact and exit. By contrast, many defence models remain slow to adapt, constrained by legacy processes, skills shortages and reactive operating models often responding only after material damage has occurred.

Boards and executives must therefore move beyond visibility to comprehension. Logs, alerts and dashboards have limited value unless they explain why controls are failing, where risk is accumulating and how incidents propagate across ecosystems.

> The organisations that succeed will be those that translate detection into prediction, prediction into prevention and prevention into trust — while resisting the temptation to chase every new technology without a clear architectural rationale.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

Creative Services ref. 1774 Ayanda Mokhethi

ED None

ey.com/za