JIRRS
Journal International Review of Research Studies

Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

REVIEW OF CYBERSECURITY LANDSCAPE IN AFRICAN BUSINESSES

Adedayo Ayomide ADENIRAN [1]; Olanrewaju Tolu OMIGBODUN [2]
[1]Department of Geography and Planning, University of Ibadan, Nigeria;
done@butyglobal.com; https://orcid.org/0009-0001-0241-6232
2 Department of Transport Planning and Logistics, University of Ilesa;
olanrewaju_omigbodun@unilesa.edu.ng; https://orcid.org/0009-0007-4583-1798

Corresponding author: done@butyglobal.com

Abstract

This review synthesises the rapid evolution of the African cybersecurity landscape, transitioning from foundational challenges identified to a state of systemic digital fragility within a USD 2.8 trillion nominal GDP economy. Supporting over 570 million internet users, the continent currently faces a "paradox of progress" characterised by a relentless tempo of 3,153 weekly cyberattacks, 60% higher than the global average, resulting in a "3:1 resilience ratio" where USD 5 billion is lost annually despite a USD 15.3 billion expenditure. The study identifies a radical professionalisation of threat actors through Crime-as-a-Service (CaaS) models, shifting the primary attack surface from traditional networks to identity and critical information infrastructure (CII). Notably, identity-driven intrusions now account for 48% of regional incidents, while the dual-use nature of Artificial Intelligence (AI) facilitates "mainstream deepfake fraud" and "Agentic AI" risks that bypass traditional perimeters. As the regulatory environment moving from theoretical compliance to tangible enforcement and record-breaking fines, the review argues for a fundamental transition to prevention-first resilience. Strategic recommendations for African businesses include implementing Zero Trust Architectures, adopting Human Risk Management (HRM) to close the "overconfidence gap," and leveraging Managed Security Service Providers (MSSPs) to bridge the continent's 200,000-person talent deficit.

Keywords: Artificial Intelligence; Business; Cyberattack; Cyber security

1. Introduction

The outlook of cyber security in African businesses that was conducted by Adeniran et al. (2024), established a foundational understanding of the cybersecurity challenges facing the African corporate sector by highlighting the approximately USD 10 billion annual cost of cybercrime and the continent's significant deficit in certified professionals. However, as the regional digital economy has surpassed USD 2.8 trillion in nominal GDP and supports over 570 million internet users, the

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

"Security Gap" described in the original text has evolved into a trillion-dollar challenge that demands a transition from reactive detection to prevention-first resilience (IT News Africa, 2026). The current threat landscape is defined by a relentless tempo, with African organisations now facing an average of 3,153 cyberattacks per week, a frequency that is 60% higher than the global average (Check Point Software Technologies, 2025).

Recent fiscal data for 2024 and 2025 provides a more granular economic picture than was available during the original study's publication. While the continent allocated USD 15.3 billion toward cybersecurity expenditure (approximately 0.55% of GDP), it still incurred USD 5 billion in reported cybercrime losses (Serianu Limited, 2025). This creates a "3:1 resilience ratio"for every three dollars spent on protection, one dollar is still lost to attackersrevealing a maturity gap where internet penetration and digital adoption are outpacing the implementation of defensive safeguards (CIO Africa, 2025). This economic volatility is further reflected in the 15% decline in Foreign Direct Investment (FDI) inflows into digital sectors in regions where cybersecurity risks are perceived as high (Mordor Intelligence, 2026).

The Table 1 presents the latest cross-country comparison of macro-digital and cyber-resilience indicators across the five in-scope economies, supported by global and regional sources.

Table 1: Key Indicators by Country

Region/Country	Population (2025 est.)	Nominal GDP (USD)	Internet Users (2025)	Aggregate Cybersecurity Expenditure (USD est.)	Estimated Crime Losses (⅓ of Spend)	Qualified Cyber Professionals (2025 est.)	Mobile Data Subscriptions (2025)
Africa (Total)	1.55 B	$ 2.8T	570 M	$ 15.3 B (0.55% GDP)	$ 5.0 B	400 000 (120 000 cert)	855 M
Nigeria	237.5 M	$ 285.93 B	109 M	$ 1.43 B	$ 0.48 B	75 000 (28 000 cert)	150 M
Kenya	57.5 M	$ 136.0 B	29 M	$ 0.68 B	$ 0.23 B	27 000 (9 000 cert)	68.8 M
Uganda	51.4 M	$ 64.99 B	14 M	$ 0.33 B	$ 0.11 B	11 000 (3 500 cert)	38.6 M
Botswana	2.56 M	$ 19.19 B	2.1 M	$ 0.096 B	$ 0.032 B	3 500 (900 cert)	4.21 M
Lesotho	2.36 M	$ 2.09 B	1.1 M	$ 0.010 B	$ 0.003 B	900 (180 cert)	2.07 M

Source: Africa Cybersecurity Report, Kenya (Serianu Limited, 2025)

Artificial Intelligence (AI) has emerged as the defining factor of the current era, representing what global leaders identify as the primary driver of change in 2026

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

(World Economic Forum, 2026). The rise of "Agentic AI"autonomous systems capable of acting without human oversighthas been integrated into African logistics and finance, yet it has created a "governance gap" as private-sector adoption outpaces national strategies in major hubs like Nigeria, Kenya, and South Africa (IT News Africa, 2026; Obakhume, 2026). Concurrently, the rise of hyper-realistic deepfake technology has moved into the mainstream, enabling cloned voice approvals and synthetic interactions that bypass traditional mobile authentication in Africa's mobile-first economy (Check Point Software Technologies, 2025). This "AI vs. AI" battleground requires businesses to manage technology not just for innovation, but for the preservation of digital trust (World Economic Forum, 2026).

Furthermore, the attack surface has shifted from traditional network perimeters to a storm centred on Identity and Critical Infrastructure. Nearly 48% of total incidents in the region now involve identity-related breaches, such as credential theft and valid account abuse, signalling that trust and identity have become the most exploited elements of modern enterprise security (Serianu Limited, 2025). Simultaneously, ransomware has evolved into "data-pressure" operations targeting Critical Information Infrastructure (CII) (IT News Africa, 2026). As industrial digitalization grows, the focus of attackers has shifted from data availability to data integrity, where corrupted datasets in power grids or healthcare systems can trigger cascading real-world disruptions (Check Point Software Technologies, 2025).

As African nations move toward the 2030 goal of a secured Digital Single Market, the regulatory landscape has entered what is described as the "Year of the Teeth" (Digital Policy Alert, 2026). With 44 countries now possessing data protection laws and 38 operational Data Protection Authorities, the region has transitioned from theoretical compliance to tangible enforcement characterized by record-breaking fines and criminal convictions for data negligence (Digital Policy Alert, 2026). In this complex environment, operational resilience is no longer defined by how many attacks are prevented, but by how effectively an organisation can withstand, recover, and adapt to a state of constant digital volatility (African Union, 2024).

2. Literature Review

The original literature review by Adeniran et al. (2024) provided a seminal definition of cybercrime as the unauthorised use, modification, and destruction of digital resources, while correctly identifying the "human element" as the most significant vulnerability in any security architecture. However, in the brief period since its publication, the conceptual and operational nature of cybercrime in Africa has undergone a radical professionalization (Omigbodun & Akinloye, 2026). Current scholarship now views cybercrime not merely as a series of isolated deviant acts, but as a sophisticated Crime-as-a-Service (CaaS) economy that leverages global illicit supply chains to target the continent's rapidly digitising sectors (Interpol, 2025).

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

The Professionalisation of the Threat Landscape

Recent literature identifies a decisive shift from opportunistic, mass-scale attacks toward precise, identity-driven intrusions (Esentry, 2025). While the base article noted the prevalence of malware and phishing, current data reveals that African organisations now face an average of 3,153 cyberattacks per week, a frequency that is 60% higher than the global average (Check Point Software Technologies, 2025). This intensity is driven by the rise of Ransomware-as-a-Service (RaaS) and "data-pressure" operations. Ransomware has evolved from simple data encryption to sophisticated double and triple extortion models, where threat actors exfiltrate sensitive data before encryption to demand ransoms that often exceed regulatory fines (Interpol, 2024; IT News Africa, 2026).

Table 2: Top Threat Scenarios - Africa

Threat Scenario Event Type	Number of Incidents (%)	Magnitude of Loss (%)	Summary Observation
Phishing & Social Engineering	24	18	Primary infection vector; AI-generated content and voice spoofing raise success rates.
Exploitation of Vulnerabilities & Misconfigurations	18	15	Persistent patch-management gaps in cloud and government networks.
Credential Theft & Reuse (Identity Compromise)	14	12	Drives fraud and unauthorized transfers; MFA adoption rising but inconsistent.
Business Email Compromise (BEC)	10	11	High-value fraud via supplier-invoice manipulation and fake approvals.
Ransomware / Data Encryption for Extortion	5	6	Lower frequency, highest per-event losses; downtime costs dominate impact.
Distributed Denial of Service (DDoS)	6	5	Disruptive but transient attacks on telecoms and fintechs.
API & Cloud Exploitation	5	6	Weak authentication and shared-service exposure; API economy expanding.

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

Third-Party / Supply-Chain Compromise	4	8	Vendor and MSP intrusions trigger cascading regional effects.
Malware Deployment & Propagation	8	4	Commodity malware prevalent; relatively low loss per incident.
Insider-Triggered Incidents (Negligent or Malicious)	6	4	Human error remains significant; analytics improving early detection.

Africa Cybersecurity Report, Kenya (Serianu Limited, 2025)

Identity: The New Perimeter

Just as shown in the table 2 above and in most contemporary research has redefined the "weakest link" theory originally discussed by Adeniran et al. (2024). Identity has surpassed the network as the primary attack surface. Nearly 48% of total incidents in the region are now identity-related, involving the theft or misuse of valid login credentials rather than technical system breaches (Serianu Limited, 2025). This "valid account abuse" allows adversaries to move quietly through internal systems and persist longer without triggering traditional detection mechanisms (esentry, 2025). The convergence of mobile financial serviceswhich has seen adoption rise to 85% among connected Africanshas made identity the master key to the continent's digital wealth (KnowBe4, 2025).

The AI Paradox: Synthetic Deception and Agentic Risk

A critical missing element in earlier literature is the role of Artificial Intelligence (AI) as a force multiplier for both defenders and attackers. By 2026, AI is identified by 94% of global leaders as the primary driver of change in the cybersecurity landscape (World Economic Forum, 2026). Generative AI has birthed a new era of "Mainstream Deepfake Fraud," where cloned voices and synthetic interactions bypass traditional multi-factor authentication in Africa's mobile-first economy (Check Point Software Technologies, 2025). Furthermore, the rise of "Agentic AI"autonomous systems capable of acting without human oversight, has created a significant "governance gap" in key hubs like Nigeria and Kenya, where private-sector adoption is significantly outpacing national regulatory frameworks (IT News Africa, 2026; Akinloye, 2026).

IT/OT Convergence and Critical Infrastructure

While the original text focused on general business risks, recent studies highlight a mounting threat to Critical Information Infrastructure (CII). The rapid digitisation of the African energy sector, particularly smart grids and renewable energy, has removed the "air gap" that once protected power and water systems (Kreso, 2025). Legacy systems like SCADA and PLCs, originally built for physical safety rather than digital security, are now interconnected with corporate networks, making them

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

susceptible to malware such as “Industroyer” which can trigger cascading real-world disruptions (Smart Security Solutions, 2026; IT Window, 2024).

Societal Impacts and OIBSA

Finally, the literature has expanded to include the rising social and psychological toll of Online Image-Based Sexual Abuse (OIBSA) and digital sextortion. Over 60% of African countries reported a surge in these crimes in 2024, often involving organized criminal networks that use social media-based coercion to target both adults and minors (Interpol, 2025). This underscores that the “Outlook of Cybersecurity” in African businesses is no longer just a financial concern, but a fundamental pillar of societal stability and the digital social contract (African Union, 2024).

The “Outlook of Cybersecurity” must also account for the fact that internet communication significantly influences the moral, social, and emotional development of the younger generation. Beyond financial loss, exposure to negative online communication, including phishing, cyberbullying, and damaged reputations, can cause users to struggle in real-life contexts and negatively impact their overall mental performance and mood (Akinloye, 2025). This excessive reliance on online platforms can hinder the ability of individuals to communicate their issues effectively, thereby weakening the social fabric required for digital resilience.

3. Theoretical Review

The original theoretical framework provided by Adeniran et al. (2024) utilized classical criminological models to explain cyber-deviance. However, the rapid professionalization of the threat landscape and the emergence of Artificial Intelligence (AI) as a dual-use tool for both offense and defence necessitate a broader theoretical expansion. Modern cybersecurity in Africa is no longer just about preventing deviance; it is about managing systemic digital fragility and establishing a new social contract for data governance (African Union, 2024; IT News Africa, 2026).

Routine Activity Theory and the Modern Attack Surface

Routine Activity Theory posits that a crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge in space and time. In the digital context of 2026, the “suitability” of targets has increased exponentially as African businesses migrate critical functions to the cloud and integrate Internet of Things (IoT) devices into critical infrastructure (Kreso, 2025; IT Window, 2024).

Motivated offenders now operate through Crime-as-a-Service (CaaS) models, lowering the barrier to entry for low-skilled actors to launch sophisticated ransomware or Business Email Compromise (BEC) campaigns (Interpol, 2025; Serianu Limited, 2025). The “guardian” element has shifted from simple firewalls to AI-powered detection systems, yet a “governance gap” remains as private sector

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

adoption outpaces national regulatory preparedness in major hubs like Nigeria and Kenya (IT News Africa, 2026; Deloitte, 2026).

Aker's Social Learning Theory and the CaaS Economy

Aker's theory suggests that criminal behaviour is learned through imitation and differential reinforcement within deviant peer groups. In the modern African landscape, this "learning" occurs within decentralized dark web marketplaces where Ransomware-as-a-Service (RaaS) affiliates share tactics and tools (Interpol, 2024; esentry, 2025).

The rise of Generative AI has accelerated this social learning, providing ready-made phishing kits and deepfake templates that allow novices to mimic the linguistic patterns and writing styles of high-level executives (Interpol, 2025; Deloitte, 2026). This professionalization has turned isolated hackers into coordinated cartels capable of sustained, large-scale operations targeting the financial and energy sectors (esentry, 2025; ESET, 2026).

Situational Crime Prevention and "Secure-by-Design"

Situational Crime Prevention (SCP) focuses on hardening the environment to reduce opportunities for crime. In 2026, the traditional "air gap" that protected industrial production lines and power grids has disappeared due to IT/OT convergence (Kreso, 2025; Smart Security Solutions, 2026).

Consequently, SCP must evolve into a "Secure-by-Design" and "Privacy-by-Design" approach, where security is a foundational pillar of innovation rather than a reactive IT add-on (ESET, 2026; Usercentrics, 2025). This includes segmenting networks to prevent lateral movement and adopting Zero Trust Architecture, which assumes that any user or deviceeven those inside the perimeteris a potential threat until verified (esentry, 2025; Smart Security Solutions, 2026).

The evolution of Situational Crime Prevention (SCP) into a "Privacy-by-Design" approach can be further explained through Communication Privacy Management (CPM) theory. This framework posits that individuals manage their private information through negotiated boundaries and rules for disclosure or concealment. In a post-divorce or complex organizational structure, the use of technology to maintain relationships necessitates clear boundary coordination to prevent information overload or the abuse of personal data (Akinloye, 2024b). By applying these principles, businesses can foster an environment where employees act as active managers of their digital boundaries, reducing the risk of third-party or insider-triggered leaks.

Data as a Public Good and the New Social Contract

A significant theoretical shift presented in recent continental policy is the conceptualization of data as a non-rivalrous public good and the basis for a new social contract (African Union, 2022; World Bank, 2021). Unlike traditional assets,

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

data's value is realized only through processing and combination, leading to a "Datafication" phenomenon (African Union, 2022).

This theory suggests that trust is the core currency of the digital economy; therefore, data governance must move beyond "negative compliance" to "positive enabling regulation" that redresses historical structural inequalities and protects the digital social contract for Africa's 1.5 billion citizens (African Union, 2022; Digital Policy Alert, 2026).

Identity as the New Security Perimeter

Theoretical frameworks have shifted from network-centric models to Identity-Driven Security. With nearly 48% of regional incidents now involving valid account abuse (the misuse of legitimate credentials), identity has become the primary battleground (Serianu Limited, 2025; esentry, 2025). This "Overconfidence Gap"where users feel confident but lack knowledge of specific threats like ransomwareunderscores that the human element remains the most significant vulnerability (KnowBe4, 2025). Theory now emphasizes Human Risk Management (HRM), focusing on digital mindfulness and "second-nature vigilance" to counter sophisticated social engineering and AI-cloned interactions (KnowBe4, 2025; IT News Africa, 2026).

Modern theory must also draw upon Communication Accommodation Theory (CAT) to understand how and why individuals modify their interactions to suit the demands of their partners. In the context of the "Overconfidence Gap", a primary predictor of relational solidarity and trust is the evaluation of a partner's communicative accommodation. Attackers exploit this by mimicking expected communication patterns, thereby bypassing the victim's natural vigilance (Akinloye, 2024a). This professionalisation of synthetic deception requires a deeper understanding of how "non-accommodation" can serve as an early warning sign for identity-driven intrusions.

Operational Resilience and the "AI vs. AI" Tempo

Finally, modern theory adopts an Operational Resilience mindset, which shifts the question from "if" an attack will occur to "how quickly" an organization can recover (CIO Africa, 2025; Check Point Software Technologies, 2025). In 2026, the "AI vs. AI" war defines this tempo: defenders use AI to triage logs and detect anomalies at machine speed, while attackers use the same technology to create polymorphic malware that evades traditional detection (Deloitte, 2026; WEF, 2026). Resilience is thus theorized as a state of strategic agility, requiring organizations to withstand, recover from, and adapt to constant digital volatility (Digital Policy Alert, 2026; African Union, 2024).

4. Result and Discussions

Comprehensive Analysis of the African Cyber-Threat Landscape (2024–2026)

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

The period between 2024 and 2026 marks a defining epoch in Africa's digital evolution, characterized by a profound "paradox of progress." As the continent aggressively pursues the 2030 goal of a secured Digital Single Market under the African Union's Agenda 2063, its digital infrastructure is expanding at a tempo that frequently outpaces the defensive protocols designed to protect it (African Union, 2024; IT News Africa, 2026). This "Security Gap" has matured into a trillion-dollar challenge, as African businesses navigate a landscape where they face an average of 3,153 cyberattacks per weeka frequency 60% higher than the global average (Check Point Software Technologies, 2025; Serianu Limited, 2025).

Spatial and Regional Exposure Patterns

Recent empirical data reveals a highly concentrated threat landscape, with economic hubs serving as the primary targets for sophisticated transnational syndicates.

- **South Africa:** Remains the central hub for cybercrime on the continent, accounting for the highest share of ransomware and phishing incidents (SOCRadar, 2025). Despite having one of the most advanced cybersecurity ecosystems, the region is struggling with a "reporting gap," where only a fraction of incidents are disclosed to the Information Regulator (SA Profile, 2025).

- **Nigeria:** Has experienced a staggering 1,047% increase in data breaches involving national entities in recent fiscal quarters (esentry, 2025). The landscape is increasingly defined by identity-driven intrusions, with Nigeria ranking 34th globally for leaked accounts, recording approximately 6,101 attacks per week in peak periods (esentry, 2025; Interpol, 2025).

- **Egypt and Morocco:** Egypt accounts for roughly 13% of total incidents recorded across Africa, driven by rapid fintech adoption and mega-infrastructure projects like the New Administrative Capital (Mordor Intelligence, 2026). Morocco has emerged as a market leader for Managed Detection and Response (MDR), with its cybersecurity market valued at USD 1.2 billion in 2025 (Ken Research, 2025).

- **East Africa:** Ethiopia was identified as the world's most targeted country for malware detections in 2024, while Kenya recorded over 4.5 billion cyber-threat events in a single quarter of 2025 (Interpol, 2025; Serianu Limited, 2025).

The Economics of Cyber Resilience

The financial implications of cyber-insecurity are no longer peripheral but represent a significant drain on the continent's nominal GDP of USD 2.8 trillion (Serianu Limited, 2025). In 2023 alone, cybercrime cost the continent an estimated USD 10 billion (Ecofin Agency, 2026; TechAfrica News, 2026). The current fiscal climate is defined by the "3:1 Resilience Ratio": while the continent allocated USD 15.3 billion (0.55% of GDP) toward cybersecurity expenditure, it still incurred USD 5 billion in

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

reported losses (Serianu Limited, 2025; CIO Africa, 2025). This economic volatility has a direct impact on the investment climate; for instance, Nigeria saw a 15% decline in Foreign Direct Investment (FDI) inflows into its digital sectors between 2021 and 2023, largely attributed to perceived cybersecurity risks (Zenodo, 2025; Mordor Intelligence, 2026).

Dominant Sectoral Risks and the IT/OT Convergence

The attack surface has shifted toward the pillars of connectivity that underpin modern African society.

- **Financial Services and Fintech:** Account for 70% of total incidents and losses (Serianu Limited, 2025). The surge in "cash-less" policies and the linkage of national identity numbers to banking records has increased the target value of mobile-first users, with 85% of connected Africans now utilizing mobile financial services (Mordor Intelligence, 2026; KnowBe4, 2025).
- **Critical Information Infrastructure (CII):** The "air gap" that once protected energy and water systems is effectively gone due to the rapid convergence of Information Technology (IT) and Operational Technology (OT) (Smart Security Solutions, 2026). Ransomware has evolved into "data-pressure" operations, where the corruption of a dataset in a power grid or renewable energy plant can trigger cascading real-world disruptions (IT News Africa, 2026; Kreso, 2025).
- **Telecommunications:** Remains the primary target for state-linked actors and sophisticated gangs, as no single company can defend its network in isolation (World Finance, 2026; SA Profile, 2025).

The 2025 cyberattack on Ivorian payment processor CinetPay, which resulted in a $1.2 million settlement backlog, serves as a critical case study of how digital fraud can trigger a "liquidity cascade" that threatens the working capital of over 25,000 African businesses (TechCabal, 2026). This incident underscores the fragility of the Francophone West African fintech corridor and tests the robustness of regulatory standards implemented by the Central Bank of West African States (TechCabal, 2026).

Strategic Law Enforcement and Regulatory Response

The year 2025 is historically significant as the "Year of the Teeth," where African nations transitioned from the adoption of laws to the era of consequences (Digital Policy Alert, 2026).

- **Historical Sanctions:** A landmark 2024 case saw the Nigerian government impose a record USD 220 million fine on Meta for violations related to consumer protection and data privacy, signalling a new era of vigilance toward tech giants (Africa Data Protection Report, 2024).

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

- **Operational Success:** Through the AFJOC initiative, Interpol and AFRIPOL have dismantled transnational syndicates. Operation Serengeti (2024) led to over 1,000 arrests and the identification of 35,000 victims, disrupting criminal networks linked to ransomware and multi-million-dollar BEC schemes (Interpol, 2025).

The Overconfidence Gap: Despite 83% of users feeling confident in their security awareness, 53% admit they do not know what ransomware is, highlighting a critical "Human Risk Management" gap that remains the primary enabler for social engineering and AI-cloned deception (KnowBe4, 2025).

---

5. Conclusion

The original synthesis provided by Adeniran et al. (2024) correctly identified that cybersecurity is no longer a peripheral IT issue but a fundamental pillar of business continuity. However, the data from 2025 and projections for 2026 reveal that the continent has entered a phase of "Digital Fragility," where the rapid adoption of AI, cloud, and fintech has outpaced existing security safeguards (Serianu Limited, 2025; IT News Africa, 2026). The conclusion of this review posits that the path forward requires a transition from reactive defense to a state of constant, proactive resilience.

Synthesis of the African Digital Turning Point

Africa's digital economy, now valued at approximately USD 2.8 trillion, is currently defined by the "3:1 Resilience Ratio": for every three dollars spent on cybersecurity (totalling USD 15.3 billion), one dollar is still lost to cybercrime (USD 5 billion) (Serianu Limited, 2025; CIO Africa, 2025). This economic reality underscores a persistent maturity gap where internet penetration is growing faster than defensive investment (CIO Africa, 2025). Furthermore, the shift from opportunistic attacks to precise, identity-driven intrusions, where nearly 60% of investigated incidents involve valid account abuse, indicates that trust and identity are now the most exploited elements of the corporate perimeter (esentry, 2025).

The Regulatory Transition: From Paper to Enforcement

The landscape has transitioned into the "Year of the Teeth," characterized by a decisive shift from the adoption of laws to tangible enforcement (Digital Policy Alert, 2026). With 44 countries now possessing data protection laws and the African Union moving to finalize the Continental Cybersecurity Strategy, the regulatory environment is increasingly punitive (African Union, 2024; Digital Policy Alert, 2026). The record-breaking fines seen in 2024 and 2025, alongside the emergence of personal liability for executives in cases of data negligence, signal that "lack of awareness" is no longer a valid legal defence for African businesses (Digital Policy Alert, 2026; Africa data protection report, 2024).

Strategic Recommendations for African Businesses

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

Human Risk Management and Identity Defence: Since 48% of regional incidents originate through identity-related breaches like phishing and credential theft, businesses must move beyond basic awareness to Human Risk Management (HRM) (Serianu Limited, 2025; KnowBe4, 2025). This includes implementing phishing-resistant Multi-Factor Authentication (MFA) and utilizing AI-driven behavioural analytics to flag anomalous access patterns at machine speed (esentry, 2025; IT News Africa, 2026).

Securing the IT/OT Convergence: As industrial digitalization in Africa grows at 30% annually, the "air gap" protecting critical infrastructure has disappeared (IT News Africa, 2026; Smart Security Solutions, 2026). Organizations in energy, manufacturing, and healthcare must adopt a "Secure-by-Design" approach, utilizing network segmentation and Zero Trust Architecture to prevent lateral movement between corporate IT and sensitive control systems (OT) (ESET, 2026; Smart Security Solutions, 2026).

Democratizing Defence through MSSPs: To address the critical shortage of certified talent, with over 200,000 unfilled roles on the continent, businesses should leverage Managed Security Service Providers (MSSPs) (IT News Africa, 2026; Serianu Limited, 2025). MSSPs act as the resilience engine for the region, allowing SMEs and large enterprises alike to consume advanced AI-assisted detection as-a-service, thereby bridging the talent gap (IT News Africa, 2026; Ken Research, 2025).

Policy and Governance Recommendations

Proactive AI Governance: Governments must urgently close the "governance gap" by enacting binding AI legislation that mandates transparency and human oversight (IT News Africa, 2026; Digital Policy Alert, 2026). National strategies should support Regulatory Sandboxes to test privacy-preserving technologies in real-time, ensuring that the rise of "Agentic AI" does not lead to systemic failures in finance or logistics (Digital Policy Alert, 2026; IT News Africa, 2026).

Harmonization of the Digital Single Market: The African Union should accelerate the implementation of the AU Data Policy Framework to create a unified cross-border data exchange mechanism (African Union, 2022; African Union, 2024). Interoperability between regional Data Protection Authorities (DPAs) is essential to ensure that the Digital Single Market remains secure, competitive, and resilient against transnational criminal syndicates (African Union, 2024; Interpol, 2025).

Summary: Bridging the Maturity Gap in the African Digital Decade

The comprehensive review of "The Outlook of Cyber Security in African Businesses: Issues and Way-Out" (Adeniran et al., 2024) reveals that while the foundational issues of resource constraints and low awareness persist, the context of 2026 has introduced a "digital fragility" that the original study could not have fully anticipated. The African digital economy, now a USD 2.8 trillion engine, has leapfrogged traditional infrastructure through AI, cloud computing, and ubiquitous fintech, yet this

JIRRS
Journal International Review of Research Studies
Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

speed has created a Security Gap that now represents a trillion-dollar systemic risk (African Union, 2024; IT News Africa, 2026). The transition from the 2024 landscape to the current environment is defined by three major shifts: the professionalisation of cybercrime, the "Identity-as-the-New-Perimeter" paradigm, and the regulatory maturation known as the "Year of the Teeth" (Interpol, 2025; Digital Policy Alert, 2026).

The threat landscape in 2026 is no longer characterized by opportunistic hackers but by coordinated, transnational cartels utilizing Crime-as-a-Service (CaaS) models (Interpol, 2024; esentry, 2025). African organisations now face a relentless tempo of 3,153 cyberattacks per week, a frequency 60% higher than the global average (Check Point Software Technologies, 2025). The most critical shift in modus operandi is the move toward identity-driven intrusions, which now account for 48% of all investigated incidents in the region (SerianuLimited, 2025). This "New Normal" of valid account abuse means that trust, rather than technical exploits, is the primary point of failure for modern African enterprises (esentry, 2025; KnowBe4, 2025).

Technology has become a dual-use force in this era. While Artificial Intelligence (AI) is the primary driver of change for 94% of global leaders, it has enabled "Mainstream Deepfake Fraud" that can bypass traditional mobile authentication through cloned voices and synthetic interactions (World Economic Forum, 2026; Check Point Software Technologies, 2025). Simultaneously, the rapid convergence of Information Technology (IT) and Operational Technology (OT) has removed the historical "air gap" protecting power grids and water systems, turning ransomware into "data-pressure" operations that target the integrity of critical information infrastructure (IT News Africa, 2026; Smart Security Solutions, 2026).

Economically, the region is defined by the "3:1 Resilience Ratio": for every three dollars spent on cybersecurity (USD 15.3 billion), one dollar is still surrendered to cybercriminals (USD 5 billion) (Serianu Limited, 2025; CIO Africa, 2025). This indicates a persistent maturity gap where defensive investment is failing to outpace digital adoption. However, the regulatory response has hardened significantly. With 44 countries now possessing data protection laws and 38 operational Data Protection Authorities, the region has moved into an era of criminal liability for executives and record-breaking fines, such as the USD 220 million penalty imposed on Meta in Nigeria (Digital Policy Alert, 2026; Africa data protection report, 2024).

Ultimately, the path forward for African businesses requires a transition from reactive detection to prevention-first resilience. By leveraging Managed Security Service Providers (MSSPs) to bridge the 200,000-person talent gap and adopting Zero Trust architectures that treat identity as the core perimeter, organisations can withstand the constant volatility of the 2026 frontier (IT News Africa, 2026; Serianu Limited, 2025). The success of the Digital Single Market depends on this strategic agility and the ability to embed security into the living rhythm of African innovation (African Union, 2024; IT News Africa, 2026).

JIRRS
Journal International Review of Research Studies

Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

References

Adeniran, A. A., Adeniran, A. O., Familusi, O. B. & Adedayo, O. (2024). The outlook of cyber security in African businesses: issues and way-out. Management Analytics and Social Insights, 1 (2), 260-271. https://doi.org/10.22105/SA.2021.281500.1061

Africa Data Protection Association. (2024). Africa Data Protection Report: Nigeria Fines Meta a Record $220 Million. Douala: Africa Data Protection Association. https://www.africadataprotection.org/report-dec-2024

African Union. (2020). The Digital Transformation Strategy for Africa (2020-2030). Addis Ababa: African Union Commission. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

African Union. (2022). AU Data Policy Framework. Addis Ababa: African Union Commission. https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf

African Union. (2024). African Digital Compact: A Unified Resolve for Africa's Digital Future (V4). Addis Ababa: African Union Commission. https://au.int/sites/default/files/documents/44005-doc-AU_Digital_Compact_V4.pdf

Akinloye, D. N. (2024a). Grandparent-grandchild communication: synthesis of integrative model. Psychology Nexus, 1(1), 1-15

Akinloye, D. (2024b). Communication and online platforms: pitfalls, possibilities, and pressures.ttu-ir.tdl.org.

Akinloye, D. N. (2025). Communication pattern and the influence of social media contents on young adults' wellbeing in Texas, United States of America. Journal of Communication, 6(12), 1-22. https://doi.org/10.46303/ressat.2023.13

Akinloye, D. (2026). Exploring the magnitude of Artificial Intelligence on family communication. Journal International Review of Research Studies, 1(06), 1-21.

JIRRS
Journal International Review of Research Studies

Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

Check Point Software Technologies. (2025). African Perspectives on Cyber Security Report 2025. San Carlos: Check Point Software Technologies Ltd. https://www.checkpoint.com/security-report

CIO Africa. (2025). Africa's Digital Growth Outpacing Cybersecurity. Nairobi: Chief Information Officer Africa Ltd. https://cioafrica.co/africas-digital-growth-outpacing-cybersecurity/

Deloitte. (2026). Nigeria Cybersecurity Outlook 2026. Lagos: Deloitte Nigeria. https://www2.deloitte.com/ng/en/pages/risk/articles/cybersecurity-outlook.html

Digital Policy Alert. (2026). The Year of the Teeth: Data Protection in Africa Roundup 2025 and Projections for 2026. St. Gallen: SGEPT. https://digitalpolicyalert.org/blog/data-protection-in-africa-roundup

Ecofin Agency. (2026). Cyber risks top concerns for African businesses in 2026 report. Geneva: Ecofin Agency. https://www.ecofinagency.com/news-digital/1201-51832-cyber-risks-top-concerns-for-african-businesses-in-2026-report

Esentry. (2025). Eagle's Eyes Q3 2025 Report: Monitoring Data Breaches and Identity Intrusions. Lagos: esentry.io. https://www.esentry.io/reports/q3-2025

ESET. (2026). Cybersecurity for renewable energy: Best practices to protect critical infrastructure. Bratislava: ESET Research. https://www.eset.com/blog/business/renewable-energy-cybersecurity

Interpol. (2024). Interpol African Cyberthreat Assessment Report 2024 Outlook. Lyon: INTERPOL Cybercrime Directorate. https://www.interpol.int/en/Crimes/Cybercrime/Africa-Cyber-Threat-Assessment-Report-2024

Interpol. (2025). Africa Cyberthreat Assessment Report 2025 (4th Edition). Lyon: INTERPOL Cybercrime Directorate. https://www.interpol.int/en/How-we-work/Criminal-Intelligence/Africa-cyberthreat-report-2025

IT News Africa. (2026). 8 Key Trends that will Define Africa's Cyber Security Landscape in 2026. Johannesburg: IT News Africa. https://www.itnewsafrica.com/2026/01/8-key-trends-that-will-define-africas-cyber-security-landscape-in-2026/

Ken Research. (2025). Morocco Cybersecurity (MDR & SOC) Market Analysis. Gurgaon: Ken Research Pvt. Ltd. https://www.kenresearch.com/morocco-cybersecurity-mdr-soc-market

KnowBe4. (2025). African Cybersecurity & Awareness Report 2025. Cape Town: KnowBe4 Africa. https://www.knowbe4.com/hubfs/Africa-Annual-Survey_Whitepaper_US_EN-F.pdf.

JIRRS
Journal International Review of Research Studies

Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

Kreso, I. (2025). Cyber threats and vulnerability mapping in the energy sector: Laying the groundwork for smart grid resilience. Applied Cybersecurity & Internet Governance, 4 (1). https://doi.org/10.60097/ACIG/211124

Makoshi, S. M. (2025). Cybersecurity Challenges in Nigeria: Threat Landscape, Economic Impact, and Strategic Solutions. Zenodo. https://doi.org/10.5281/zenodo.15144077

Mordor Intelligence. (2026). Nigeria Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). Hyderabad: Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/nigeria-cybersecurity-market

Obakhume, K. A. (2026). Local Content Development and the Resource Curse in Nigeria: Comparative Lessons and Policy Reform Pathways. Social Sciences & Humanities Open, 13, 102291. https://doi.org/10.1016/j.ssaho.2025.102291

Oladunmade, M. (2026, February 1). Exclusive: CinetPay customers owed over $1 million months after alleged cyberattack. TechCabal. https://techcabal.com/2026/02/01/cinetpay-cyberattack-settlement-backlog/

Omigbodun, O. T., and Akinloye, D. (2026). Context and Application of Agnew's General Strain Theory to Explain Crime. Journal International Review of Research Studies,1(06), 1-11.

TechAfrica News. (2026). Cybersecurity Tops Risk List for African Businesses in 2026. Accra: TechAfrica News. https://techafricanews.com/2026/01/12/cybersecurity-tops-risk-list-for-african-businesses-in-2026-says-new-report/

SA Profile. (2025). South African Businesses Are Underestimating Cyber Risks. Cape Town: Media Xpose. https://www.saprofilemagazine.co.za/business-news/south-africa-cybersecurity-warning-wwise-2025/

Serianu Limited. (2025). Africa Cybersecurity Report 2024/2025: From Risk to Resilience. Nairobi: Serianu. https://www.serianu.com/downloads/Africa%20Cybersecurity%20Report%20-%20Kenya.pdf

Smart Security Solutions. (2026). Factories, grids, and finance: Critical infrastructure cyber lessons of 2025. Johannesburg: Technews Publishing. https://www.securitysa.com/26388r

SOCRadar. (2025). Africa Threat Landscape Report 2025. Middletown: SOCRadar Extended Threat Intelligence. https://socradar.io/resources/report/africa-threat-landscape-report-2025/

Usercentrics. (2025). Global Data Privacy Laws: Your 2025 Guide (GDPR, CCPA, More). Munich: Usercentrics GmbH. https://usercentrics.com/guides/data-privacy-laws/

JIRRS
Journal International Review of Research Studies

Received: 02/05/2026 - **Accepted:** 23/06/2026
Vol: 01.08
DOI: 10.66104/s28ggf60
Pages: 1-17

World Bank. (2021). Data for Better Lives. Washington, D.C.: World Bank Publications. https://doi.org/10.1596/978-1-4648-1600-0

World Economic Forum. (2026). Global Cybersecurity Outlook 2026. Geneva: World Economic Forum in collaboration with Accenture. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Author Responsibility Statement

AAA: Conceptualization, Writing - original draft, Introduction, Methods, Analysis, Discussion,Conclusion; OTO: Conceptualization, Writing - original draft, Introduction, Conclusion. The authors read and approved the final manuscript.