Telecom Cybersecurity in Sub-Saharan Africa: Securing the Backbone of the Digital Economy

A few months ago, a sophisticated cyberattack quietly rocked the telecom industry in East Asia. The breach infiltrated the core network of a major operator, compromising one of the most sensitive systems in telecom infrastructure: the Home Subscriber Server (HSS). Often called the digital brain of mobile networks, the HSS stores critical user data from Universal Subscriber Identity Modules (USIMs). Once breached, attackers potentially gained access to IMSI numbers, authentication keys, SMS metadata, and contacts.

The fallout was severe. With that level of access, malicious actors could clone SIM cards, commit financial fraud, or launch identity theft campaigns. To contain the damage, the operator had to replace SIM cards for more than 23 million users.

While this incident occurred far from Africa, it should serve as a wake-up call for Sub-Saharan Africa, where telecom is the foundation of financial inclusion, digital governance, and economic transformation.

Rajiv Aggarwal, Head of Sub-Saharan Africa, Cloud and Network Services at Nokia

The Urgent Need for a Security Surge

With over 650 million unique mobile subscribers and mobile money platforms processing over $800 billion annually, Sub-Saharan Africa is the world's most mobile-first region. Telecom networks here do more than connect people—they connect economies. From sending remittances in Ghana to paying for healthcare in Kenya or accessing government services in Nigeria, the mobile phone has become the essential tool for daily life.

But this centrality also makes telecom a prime target for cybercriminals. As more services—from banking to education—are integrated into mobile networks, the volume of sensitive data traveling across these systems grows exponentially. That data is a goldmine for attackers who can exploit it for fraud, identity theft, and even large-scale disruption of essential services.

The Nokia Threat Intelligence Report highlights a steady rise in highly specialised telecom-targeted cyberattacks. In just the last 18 months:

- Salt Typhoon compromised telecom networks to harvest sensitive user data.
- A major telecom breach exposed sensitive customer data, including financial identifiers, for millions.
- Ransomware campaigns targeted telecom operators, aiming to disrupt services and exfiltrate data.
- Multi-year espionage footholds in telecom infrastructure enabled covert data collection.

Why Generic Cybersecurity Tools Won't Protect Telecom

One of the strongest lessons from the East Asian breach is that traditional IT security tools are not enough. Telecom networks are complex, built on specialized systems that demand telco-specific protections.

Next-generation, telco-ready Endpoint Detection and Response (EDR) must include:

- AI-powered, real-time threat detection based on telecom traffic analysis.
- Automated patch and compliance management to minimize vulnerabilities.
- Lightweight, non-disruptive sensors that don't slow down critical services.

As cyberattacks become faster and more automated, often fuelled by AI, Sub-Saharan Africa must move from reactive defence to anticipatory security strategies.

Building Resilient Networks

To counter increasingly sophisticated attacks, African enterprises and telecom operators need to adopt networks

that can defend themselves. This involves embedding intelligence, automation, and continuous verification into the very core of network infrastructure. AI is already making an impact, especially in the realm of 5G security.

An example of this is Nokia's NetGuard Cybersecurity Dome, which incorporates generative AI built on Microsoft Azure OpenAI GPT. This solution showcases how large language models can enhance real-time threat detection and assist teams in making faster, more informed decisions during cyber incidents.

But identifying threats is just the beginning. True cybersecurity demands a 'Zero Trust' approach—where every user, device, and interaction is continuously verified. It also requires automated incident response systems capable of immediate, decisive action, reducing human error and response time. Real-time analytics play a crucial role in identifying vulnerabilities before they can be exploited.

These capabilities are no longer theoretical. They are already being deployed in Africa, helping businesses shift from reactive defence to proactive protection—anticipating and neutralizing threats before they escalate.

Four Priorities for Sub-Saharan Africa

To strengthen resilience, operators and regulators in the region should focus on four critical areas:

1. **24/7 Threat Monitoring with AI-Driven XDR**
   Attackers often strike during weekends or high-traffic events. Always-on monitoring powered by AI/GenAI is now essential.
2. **Protecting Network Functions**
   Detect abnormal infrastructure activity and malware patterns early, before they compromise large portions of the network.
3. **Adopting Zero Trust Principles**
   Enforce strict verification for every user, device, and request. Use segmentation and limit privileged access to reduce insider and external risks.
4. **Strengthening Regulation and SOC Capabilities**
   Align with global standards while developing regional frameworks. Invest in Security Operations Centres (SOCs) to fast-track cyber readiness for 4G and upcoming 5G rollouts.

The East Asian breach shows that the next major telecom cyberattack could come anywhere, anytime. For Sub-Saharan Africa—where mobile connectivity is both a growth engine and a lifeline, the consequences of a large-scale breach would be devastating.

Now is the moment for governments, regulators, operators, and technology providers across the region to act decisively:

- Make cybersecurity a core pillar of telecom strategy.
- Build capacity for regional and cross-border cooperation.
- Invest in telco-specific defences that match Africa's unique digital landscape.

Because in the digital age, resilience isn't just about bouncing back, it's about staying one step ahead. ■

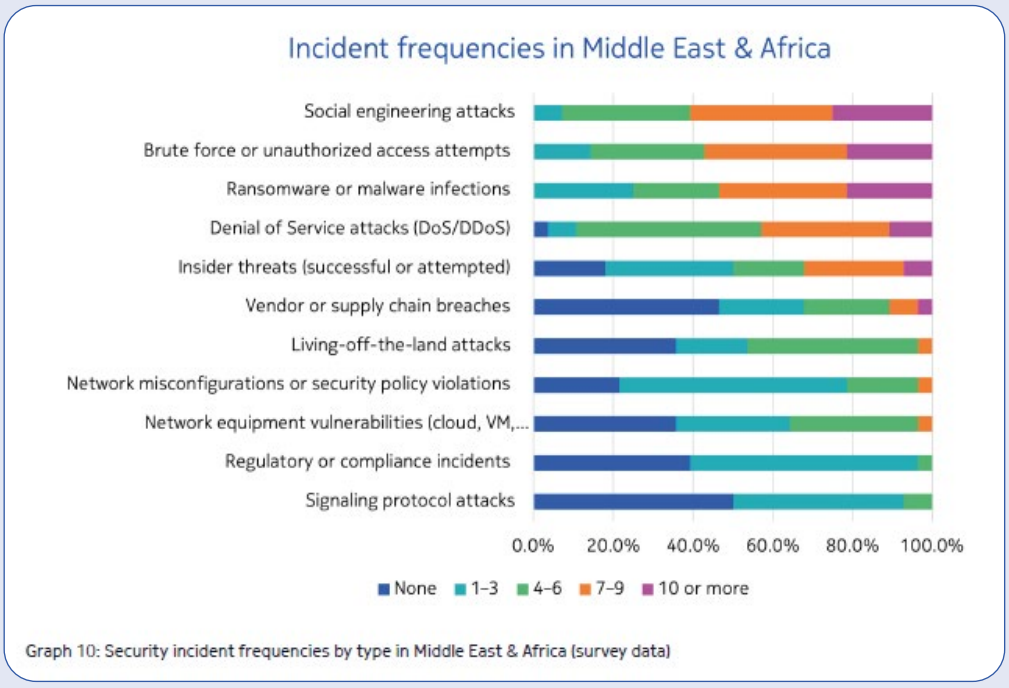
Inside the Nokia Threat Intelligence Report

Drawing on NetGuard and Deepfield insights, Managed Security Services data, Nokia Bell Labs research, and cybersecurity expertise—including quantum-safe networking—the Nokia Threat Intelligence Report offers a clear, evidence-based view of telecom risks.

Insights are enriched with inputs from 160 telecom security professionals worldwide, delivering practical guidance on threat detection, AI integration, DDoS mitigation, regulatory compliance, and quantum readiness.

Key trends in Middle East & Africa:

- 6 in 10 operators faced seven or more brute-force or unauthorised access attempts in the past year
- SIM lifecycle abuse was observed by 36% of security professionals in the past year
- Zero-trust strategies are a priority, with 75% of operators investing in implementation



Graph 10: Security incident frequencies by type in Middle East & Africa (survey data)