Global Cybersecurity Outlook 2026
Regional Analysis

Sub-Saharan Africa

FEBRUARY 2026

WORLD ECONOMIC FORUM

Introduction

Cybersecurity risk in 2026 is accelerating, fuelled by advances in AI, deepening geopolitical fragmentation and the complexity of supply chains. This analysis builds on the Global Cybersecurity Outlook 2026 (GCO 2026) to examine how these global trends are playing out in sub-Saharan Africa, providing a focused view of the region's evolving cybersecurity landscape.[1]

Key takeaways on sub-Saharan Africa

- 76% of organizations in sub-Saharan Africa already implemented AI enabled tools to fulfil their cybersecurity objectives (globally 77%).
- 71% of businesses in this region reported adjusting their cybersecurity strategy due to geopolitical volatility (globally 66%).
- 37% of organisations in sub-Saharan Africa express confidence in their country's ability to respond to a major cyber incident affecting critical infrastructure, while 39% explicitly state they are not confident (31% globally).
- 84% of respondents in the region reported an increase in cyber-enabled fraud and phishing attacks in the past year (globally 77%).
- 63% of respondents based in sub-Saharan Africa reported their organizations is lacking the talent and skills required to meet their current cybersecurity objectives (globally 50%).
- 8% of organizations in sub-Saharan Africa rate their cyber resilience as exceeding requirements (globally 19%), while around 32% assess it to be insufficient (globally 17%).

AI Security

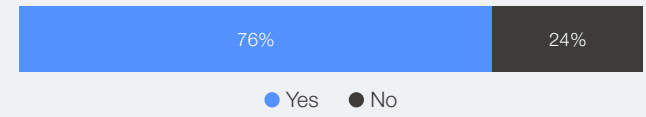
AI risk perception

- According to the GCO 2026 survey, 87% of organizations in the region believe AI and machine learning will have the greatest impact on cybersecurity in the next 12 months (globally 94%) and 82% report that AI-related risks have increased (globally 87%).
- Data leaks are considered the most pressing cybersecurity issue linked to generative AI in this region, cited by 45% of respondents (globally 34%).
- This heightened concern is not unique to sub-Saharan Africa, but the region faces additional challenges. According to the GCO 2026 survey, 45% of organizations report not having processes in place to assess the security of AI tools before deployment, compared to 29% globally.

AI for security

- Organizations in sub-Saharan Africa are actively adopting AI-enabled tools to strengthen their cybersecurity posture. Survey data indicates that 76% have already implemented such solutions – signalling strong momentum towards AI-driven security (globally 77%).

Has your organization implemented any AI-enabled tools to fulfil its cybersecurity objectives?



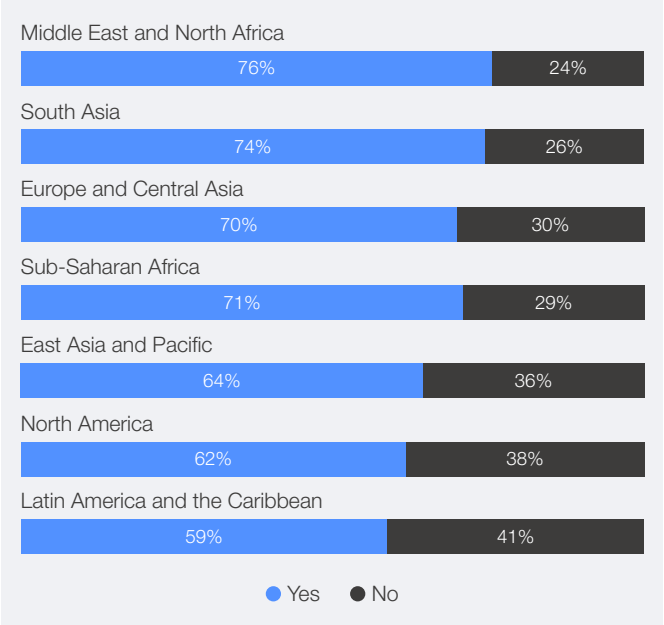
- Despite this progress, 62% of organizations cite insufficient skills as a key hurdle, while 56% point to insufficient funds as a major barrier to embracing AI for cybersecurity.

1. The number of respondents from this region in the GCO 2026 survey is lower than in other regions. As a result, the findings may have reduced statistical robustness and should be interpreted with due caution.

Geopolitics

– 71% of organizations report adjusting their cybersecurity strategy due to geopolitical volatility – which is slightly higher than the overall average of 66%. Additionally, 61% of respondents report incorporating geopolitically motivated cyberattacks into risk mitigation plans – global average 64%.

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



– Preparedness challenges are accompanied by relatively low confidence in national resilience, 39% of respondents state they are not confident (globally 31%).

Cybercrime

– The GCO 2026 survey reveals that cyber-enabled fraud as well as AI vulnerabilities are the top two cyber risks in the region.

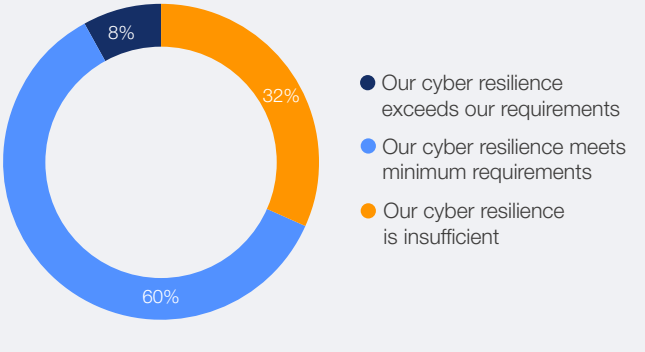
Rank	Which cyber risks concern you most for your organization?
1	Cyber-enabled fraud and phishing
2	AI vulnerabilities
3	Exploitation of software vulnerabilities

– Additionally, 84% of organizations in the region report an increase in cyber fraud and phishing attacks in the past year.

Resilience

– In sub-Saharan Africa only 8% of organizations rate their cyber resilience as exceeding requirements (globally 19%), while around 32% assess it to be insufficient (globally 17%), resulting in the lowest resilience levels across regions, according to the GCO 2026 survey.

How would you rate your organization's cyber resilience?



– The top three challenges to achieving cyber resilience in the region are:

1. Shortage of cybersecurity skills and expertise (61%)
2. Rapidly evolving threat landscape and emerging technologies (47%)
3. Lack of funds (45%)

Supply chain

- The top three cyber risks related to supply chain security reported by organizations in sub-Saharan Africa are:

    1. External factors: Uncertainty of impact of external factors (e.g., geopolitics, regulations)

    2. Inheritance risk: Inability to assure integrity of third-party software, hardware and services

    3. Concentration risk: A high degree of dependence on critical third-party suppliers

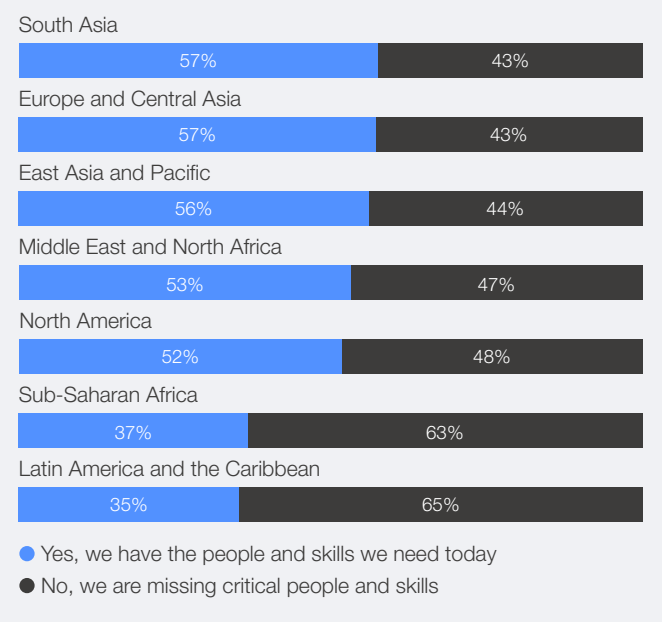
- To mitigate these risks, 55% assess their supplier maturity, while 45% share information on threats with their ecosystem partners (customers, suppliers, etc.).

How does your organization address supply chain cyber risk?

Cyber skills

- 63% of respondents report their organizations lack the workforce skills required to meet current cybersecurity objectives. Sub-Saharan Africa has the second-widest cybersecurity skills gap among the regions after Latin America and the Caribbean (65%).

Does your organization's workforce have the skills needed to achieve its current cybersecurity objectives?



- The most critical missing roles are:
    - Threat intelligence analyst
    - DevSecOps engineer
    - Identity and access management specialist

**Some graphs may show percentages exceeding 100% due to multiple-choice questions and rounding.*

To read the full report Global Cybersecurity Outlook 2026 on cybersecurity risks and trends at a global scale, please visit wef.ch/cybersecurity26. Explore the data deeper with our accompanying Data Explorer.