Global Cybersecurity Outlook 2026
Regional Analysis

South Asia

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 South Asia, providing a focused view of the region's evolving cybersecurity landscape.[1]

Key takeaways on South Asia

- 89% of organizations in South Asia believe AI and machine learning will have the greatest impact on cybersecurity in the next 12 months (globally 94%).
- 81% of businesses in the region have implemented AI-enabled tools to meet their cybersecurity objectives (globally 77%).
- 74% of organizations surveyed have changed their cybersecurity strategies due to geopolitical volatility (globally 66%).
- Ransomware and cyber-enabled fraud and phishing are the top two perceived cyber risks in the region.
- 43% of South Asian organizations reported missing critical people and skills to meet their cybersecurity objectives (globally 50%).
- 8% of organizations in South Asia rate their cyber resilience as exceeding requirements (globally 19%), while around 77% assess their cyber resilience as meeting minimum requirements (globally 64%).

AI Security

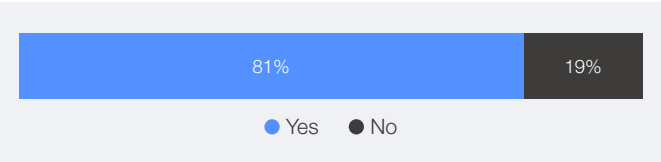
AI risk perception

- According to the survey, 89% of organizations in the region believe AI and machine learning will have the greatest impact on cybersecurity in the next 12 months, and 87% report that AI-related risks have increased.
- 62% of organizations in South Asia report they assess the security of AI tools before deployment at least once or periodically (globally 64%). Furthermore, data leaks are the most pressing cybersecurity issue linked to generative AI in this region.

AI for security

- Organizations in South Asia are actively adopting AI-enabled tools to strengthen their cybersecurity posture, but significant barriers remain.
- The GCO 2026 survey shows that 81% of organizations in the region have implemented AI-enabled tools to meet their cybersecurity objectives (globally 77%), signalling strong momentum towards AI-driven security solutions.

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



- Despite this progress, insufficient knowledge and skills (62%), along with the need for human validation of AI-generated security responses (45%), remain the top challenges to adopting 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

– Geopolitical volatility is influencing cybersecurity strategies globally and organizations in South Asia are no exception. Some 74% of organizations surveyed have changed their cybersecurity strategies due to geopolitical volatility (globally 66%).

– In response, 70% incorporate geopolitically motivated cyberattacks into their risk mitigation plans – among the highest across regions (globally 64%).

Cybercrime

– Ransomware and cyber-enabled fraud are the top two perceived cyber risks in South Asia, mirroring trends in other regions.

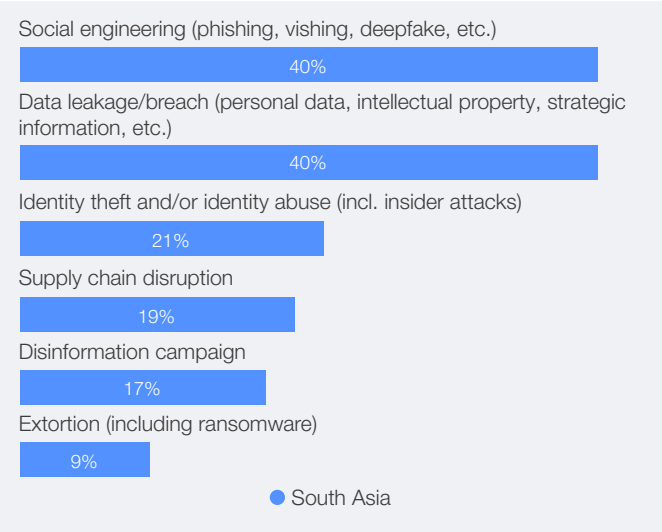
Rank	Which cyber risks concern you most for your organization?
1	Ransomware attack
2	Cyber-enabled fraud and phishing
3	Exploitation of software vulnerabilities

– Additionally, 85% of organizations in South Asia believe that the risks of cyber-enabled fraud and phishing attacks have increased.

– 60% of organizations perceive risk of ransomware attacks to have increased.

– 66% of businesses in the region report experiencing a significant cyber incident in the past 12 months, with 40% of these cases involving social engineering techniques such as phishing, vishing, or deepfakes.

Which cyber incidents (e.g., significant financial damage, major operational disruption, etc.) have affected your organization in the past 12 months?

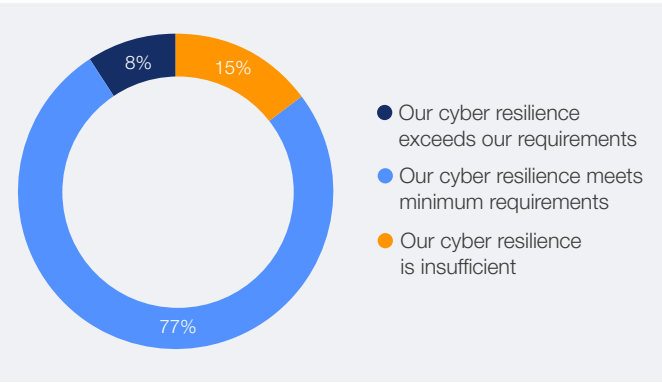


Resilience

– In South Asia, 8% of organizations rate their cyber resilience as exceeding requirements, while around 77% assess their cyber resilience as meeting minimum requirements. Around 15% assess their resilience as insufficient.

– Globally, 17% of all surveyed organizations across the world indicate insufficient resilience, 65% report minimum resilience and 19% say their cyber resilience exceeds requirements.

How would you rate your organization's cyber resilience?



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

1. Rapidly evolving threat landscape and emerging technologies, *tied with* Cybersecurity skills and expertise (64%)

2. Third party and supply chain vulnerabilities, *tied with* Lack of funds (32%)

Supply chain

- The top three cyber risks related to supply chain security reported by organizations in the region are:

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

    2. Visibility: Lack of visibility into own organization's extended supply chain

    3. Procurement risk: Inability to apply security controls to third party suppliers

- To mitigate these risks, according to survey respondents from South Asia, organizations primarily focus on involving the security function in procurement processes (64%) and assessing supplier maturity (60%). These approaches align closely with practices observed in other regions.

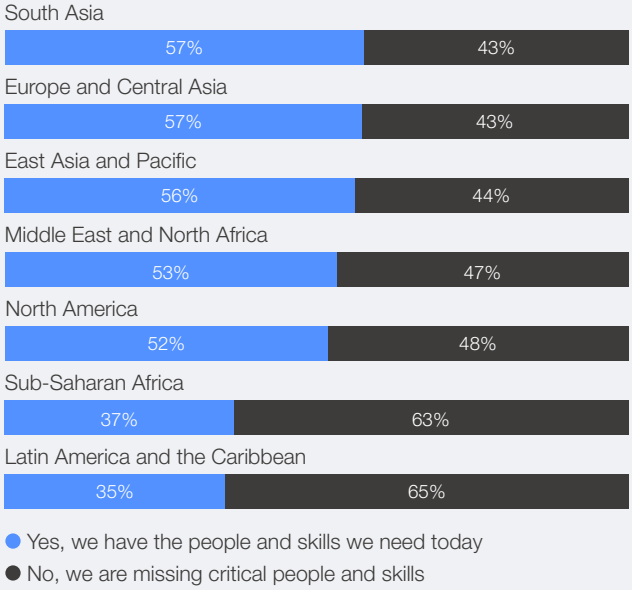
How does your organization address supply chain cyber risk?

Cyber skills

- Regarding the cybersecurity skills gap, the picture in South Asia is mixed: 57% of respondents report having the necessary people and skills to meet their cybersecurity objectives (the highest across all regions with Europe and Central Asia), while 43% report that they lack sufficient capabilities.

- Moreover, 64% of organizations in the region identify shortages in cybersecurity skills and expertise as one of the biggest obstacles to becoming cyber resilient.

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

    - Incident responder

**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.