

Europe and Central Asia

FEBRUARY 2026

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 Europe and Central Asia, providing a focused view of the region's evolving cybersecurity landscape.

Key takeaways on Europe and Central Asia

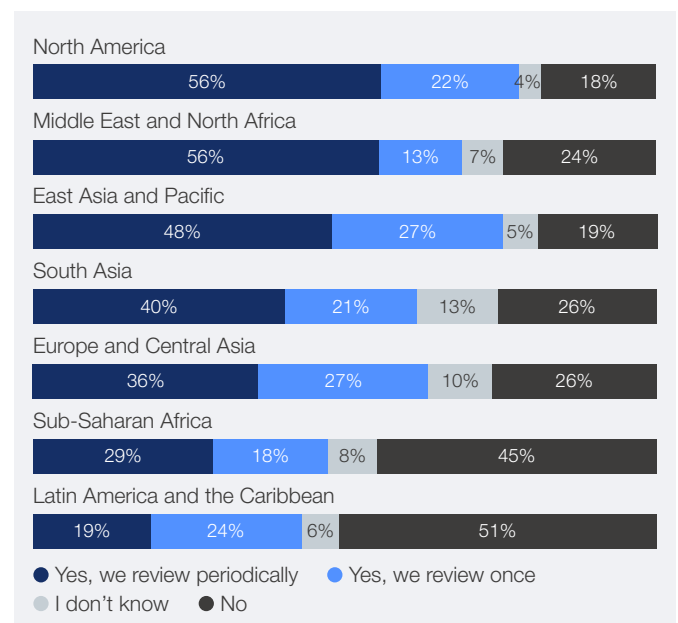
- 88% of respondents from Europe and Central Asia reported that risks related to AI vulnerabilities have increased in the past year. The global perception of AI risk is slightly lower at 87%.
- 27% of organizations reported not having any processes in place to assess the security of AI tools before deploying them. However, 75% of organizations from this region (globally 77%) reported having implemented AI for cybersecurity.
- Ransomware is the number one concern in the region, followed by cyber-enabled fraud. Some 71% of respondents reported that they themselves or someone in their network has been affected by cyber-enabled fraud. Globally, this figure is higher at 73%.
- 70% of organizations based in Europe and Central Asia reported their cybersecurity strategies have evolved because of geopolitical volatility. This percentage is lower at 66% across all respondents.
- 66% of respondents declared their cyber resilience meets minimum requirements (globally 64%), and 40% of respondents from this region reported some level of confidence in the national ability to respond to a major cyber incident affecting critical infrastructure (globally 37%).
- 43% of organizations in Europe and Central Asia report missing critical people and skills to meet current cybersecurity objectives. This is marginally better than the global average, which is 49%.

AI security

AI risk perception

- According to the GCO 2026 survey, 93% 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 88% report that AI-related risks have increased.
- Furthermore, data leaks are considered the most pressing cybersecurity issue linked to generative AI in this region, cited by 30% of respondents (globally 34%).
- This heightened concern is not unique to Europe and Central Asia, but the region appears better prepared compared with other regions. Some 63% of organizations in this region report they assess the security of AI tools before deployment at least once or periodically, close to the global average of 64%.

Does your organization have a process in place to assess the security of AI tools before deploying them?



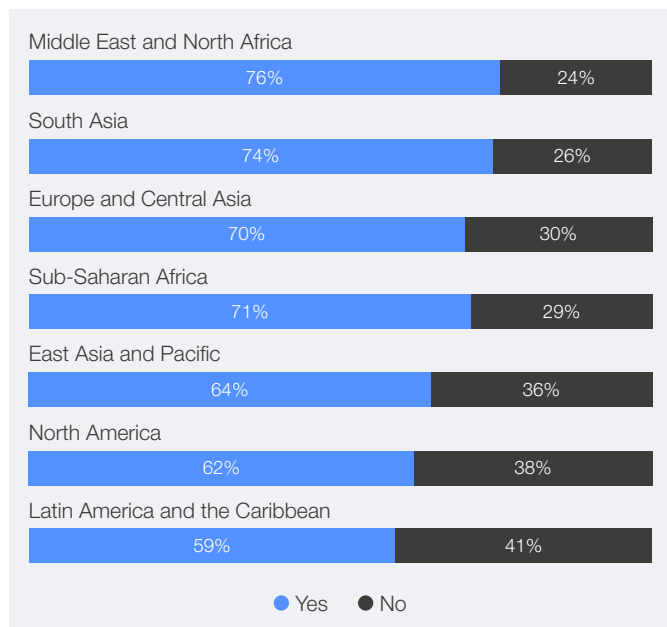
AI for security

- Organizations in Europe and Central Asia are actively adopting AI-enabled tools to strengthen their cybersecurity posture, with the GCO 2026 survey indicating that 75% have already implemented such solutions (globally 77%). This signals strong momentum towards AI-driven security even if barriers remain.
- Despite this progress, organizations in the region report several key hurdles in adopting AI for cybersecurity:
 - Insufficient skills (48%)
 - Human validation required for AI-generated security responses (38%)
 - Uncertainty about risk (38%)

Geopolitics

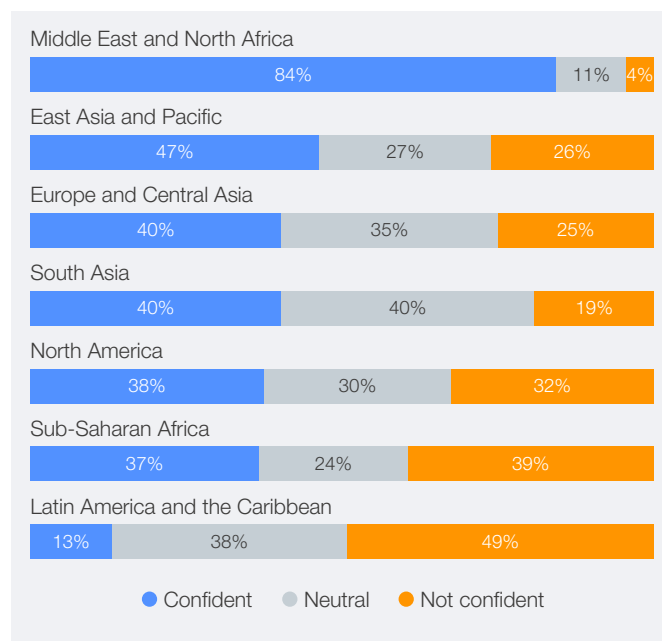
- 70% of organizations in Europe and Central Asia report adjusting their cybersecurity strategies due to geopolitical volatility – slightly higher than the global average of 66%. Additionally, 72% report incorporating geopolitically motivated cyberattacks into risk mitigation plans – the highest proportion among all other regions (64% global average).

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



- Approximately 40% of organizations in Europe and Central Asia show confidence in their country's ability to respond to major cyber incidents targeting critical infrastructure, while nearly 25% explicitly state they are not confident. These figures broadly reflect the trends reported in other regions.

How confident are you in the preparedness of the country in which you are based to respond to major cyber incidents targeting critical infrastructure?



Cybercrime

- The GCO 2026 survey reveals that ransomware and cyber-enabled fraud are respondents' top two cyber risks in the region, mirroring trends seen in Latin America and the Caribbean as well as in South Asia.

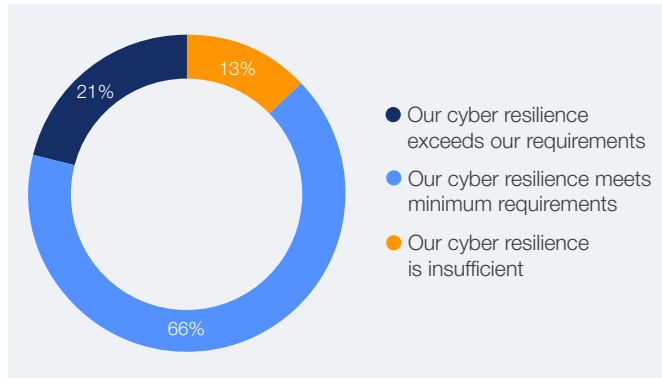


- Additionally, 72% of organizations in this region report an increase in cyber fraud and phishing attacks (globally 77%), marking the second-highest surge in this category after AI-related vulnerabilities.

Resilience

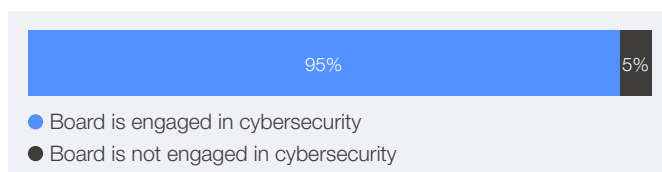
- In Europe and Central Asia, 21% of organizations rate their cyber resilience as exceeding requirements (globally 19%), while around 13% assess it as below the level they consider sufficient (globally 17%).

How would you rate your organization's cyber resilience?



- The top three challenges to achieving cyber resilience reported by organizations in this region are:
 1. Rapidly evolving threat landscape and emerging technologies (61%)
 2. Third-party and supply chain vulnerabilities (49%)
 3. Cybersecurity skills and expertise shortage (42%)
- 95% of respondents report active engagement from their board in cybersecurity matters, which is the strongest percentage across regions.

With regard to the ways in which your board is engaged in cybersecurity, the following statements apply:



Supply chain

- The top three cyber risks related to supply chain security reported by organizations in this region are:
 1. Inheritance risk: Inability to assure integrity of third-party software, hardware and services
 2. Concentration risk: A high degree of dependence on critical third-party suppliers
 3. Visibility: Lack of visibility into own organization's extended supply chain"
- To mitigate these risks, 70% of organizations in this region prioritize assessing their supplier security maturity, while 66% involve their security function in the procurement process.

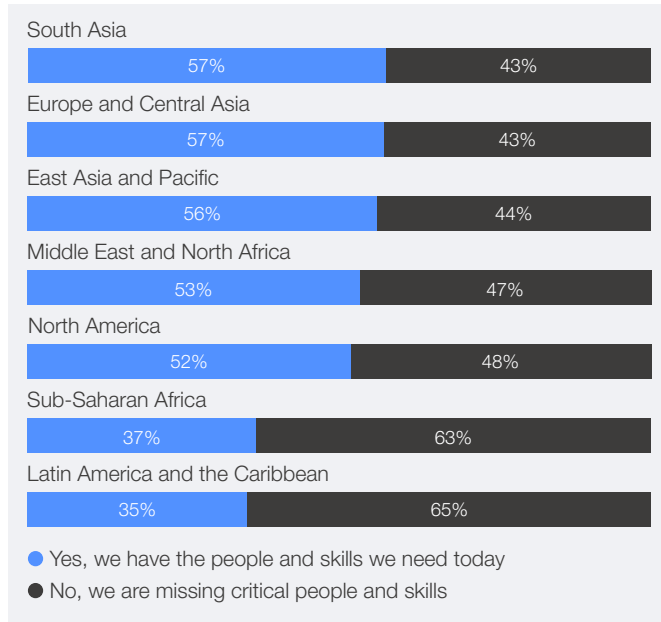
How does your organization address supply chain cyber risk?



Cyber skills

- European and Central Asian organizations report the lowest cybersecurity skills gap among the regions surveyed along with South Asia. Some 43% of businesses report they lack the workforce skills required to meet their current cybersecurity objectives (globally 50%).

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



- However, 42% of organizations in this region identify shortages in cybersecurity skills and expertise as one of the biggest obstacles to becoming cyber-resilient.
- 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](#).