Global Cybersecurity Outlook 2026
Regional Analysis:

East Asia and Pacific

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

Key takeaways on East Asia and Pacific

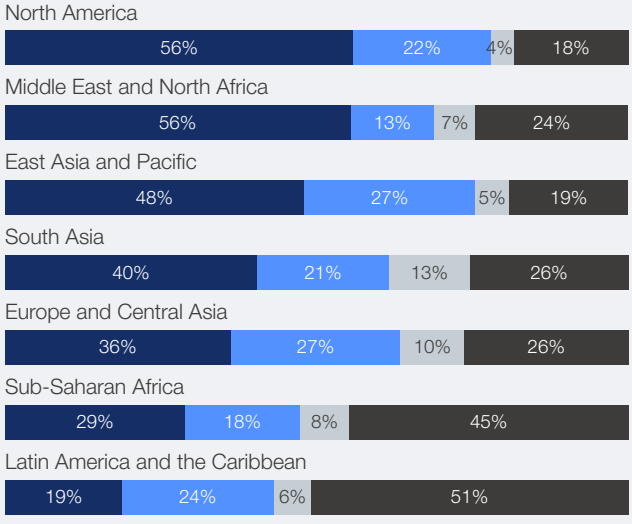
- 95% of organizations in the region believe AI and machine learning will have the greatest impact on cybersecurity in the next 12 months.
- 81% of organizations in this region have implemented AI-enabled tools to fulfil their cybersecurity objectives.
- 47% of organizations in East Asia and Pacific express confidence in their country's ability to respond to a major cyber incident affecting critical infrastructure, above the global average of 37%.
- 79% of organizations in this region reported an increase in cyber fraud and phishing attacks, higher than the global average of 77%.
- 16% of organizations in East Asia and Pacific rate their cyber resilience as insufficient, compared with 17% globally.
- 44% of organizations in East Asia and Pacific report they lack the workforce skills required to meet their current cybersecurity objectives (globally 50%)

AI security

AI risk perception

- According to the GCO 2026 survey, 95% 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 79% report that AI-related risks have increased in the past year (globally 87%).
- Data leaks are considered the most pressing cybersecurity issue linked to generative AI in this region, cited by 42% of respondents (globally 34%).
- This heightened concern is not unique to East Asia and Pacific but the region is taking additional steps to address it. According to the GCO 2026 survey, 75% of organizations in this region report having processes to assess the security of AI tools prior to deployment – the second-highest rate across regions after North America (78%).

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



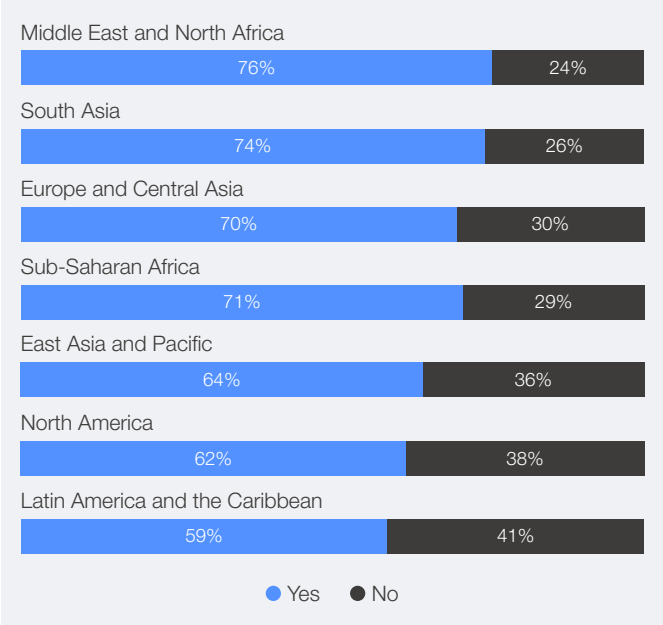
AI for security

- Organizations in East Asia and Pacific are actively adopting AI-enabled tools to strengthen their cybersecurity posture, according to 81% of respondents (globally 77%).
- However, organizations in the region report facing two hurdles in adopting AI for cybersecurity:
  1. Insufficient skills – cited by 57% of organizations as the most significant challenge
  2. Unclear business case – highlighted by 51% as a major barrier to implementation

Geopolitics

– In East Asia and Pacific, only 64% report adapting their cybersecurity strategy in response to geopolitical developments, a proportion slightly lower than the average of the other regions (66%).

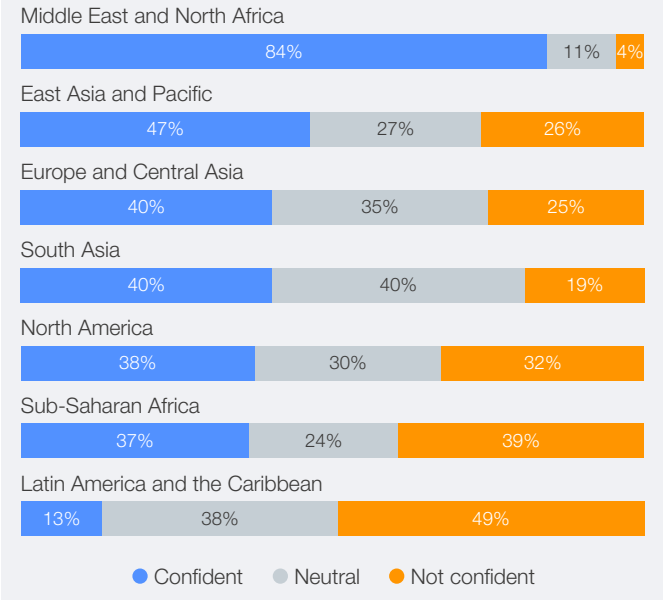
Has your organization's cybersecurity strategy evolved because of geopolitical volatility?



– Nevertheless, geopolitically motivated cyberattacks remain the leading factor shaping cyber-risk mitigation strategies in the region, with 62% of organizations stating that they actively consider it in their approach.

– With regard to critical infrastructure, 47% of organizations express confidence in their country's ability to respond to a major cyber incident affecting critical infrastructure, which is the second-largest percentage after the Middle East and North Africa (84%).

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 the exploitation of software vulnerabilities and ransomware attacks are the top two cyber risk concerns in the region.

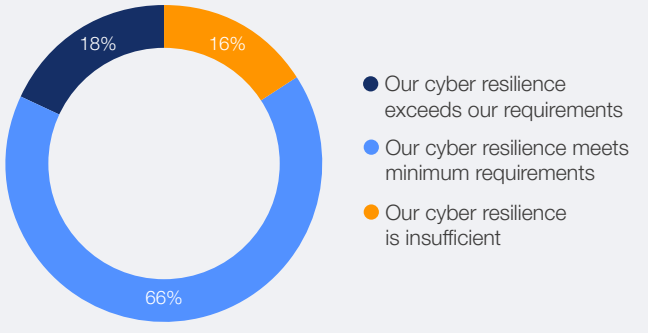
Rank	Which cyber risks concern you most for your organization?
1	Exploitation of software vulnerabilities
2	Ransomware attack
3	AI vulnerabilities

– Additionally, 79% of organizations in the region report an increase in cyber-enabled fraud and phishing attacks, along with AI-related vulnerabilities (79%).

Resilience

– In East Asia and Pacific, 16% of organizations rate their cyber resilience as insufficient, while 18% assess it as exceeding their requirements. Most of the organizations (66%) rate their cyber resilience as meeting minimum requirements, in line with global levels (64%).

How would you rate your organization's cyber resilience?

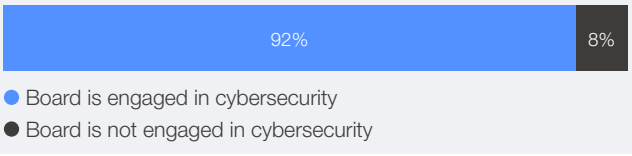


– The top three challenges to achieving cyber resilience in East Asia and Pacific are:

1. Rapidly evolving threat landscape and emerging technologies (62%)
2. Third-party and supply chain vulnerabilities (48%)
3. Cybersecurity skills and expertise shortage (44%)

– Encouragingly, 92% report active engagement from their board in cybersecurity, in line with the global average of 93%.

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



Supply chain

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

1. Inheritance risk: Inability to assure integrity of third-party software, hardware and services
2. Procurement risk: Inability to apply security controls to third-party suppliers
3. Visibility: Lack of visibility into own organization's extended supply chain, tie with

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

– To mitigate these risks, 67% of organizations in the region assess their suppliers' maturity, while 60% of organizations prioritize involving the security function in procurement processes.

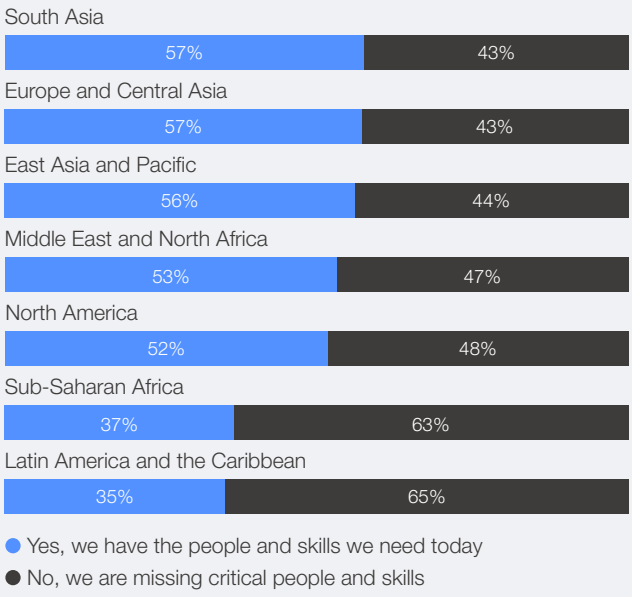
How does your organization address supply chain cyber risk?

Cyber skills

– 44% of businesses in East Asia and Pacific report they lack the workforce skills required to meet their current cybersecurity objectives (globally 50%).

– Threat intelligence analyst is the most critical missing cybersecurity role in the region, as identified by 27% of organizations.

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



**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.