Global Cybersecurity Outlook 2026
Regional Analysis

Latin America and the Caribbean

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 Latin America and the Caribbean, providing a focused view of the region's evolving cybersecurity landscape.

Key takeaways on Latin America and the Caribbean

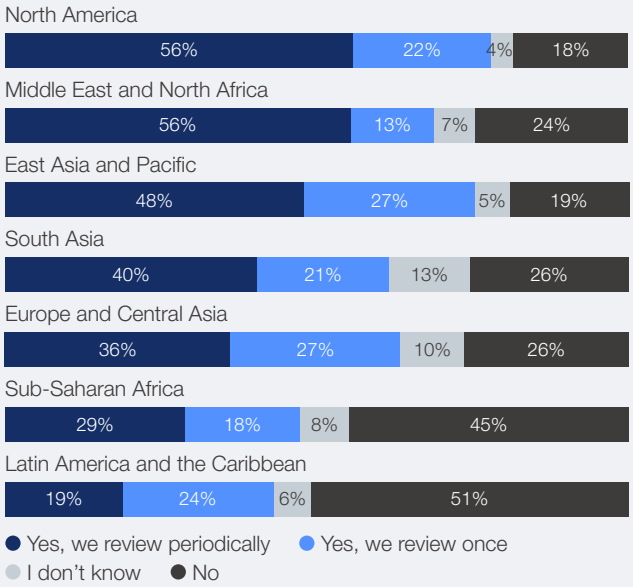
- 85% of respondents from Latin America and the Caribbean report that risks related to AI vulnerabilities have increased in the past year (globally 87%).
- 51% of respondents report not having any processes in place to assess the security of AI tools before deploying them (globally 29%). However, 74% of respondents from this region report having implemented AI for cybersecurity (globally 77%).
- Ransomware is the number one concern, followed by cyber-enabled fraud. Some 77% of respondents report that they or someone in their network have been affected by cyber-enabled fraud (globally 73%).
- 59% of organizations based in Latin America and the Caribbean report their cybersecurity strategies have evolved because of geopolitical volatility (globally 66%).
- 65% of organizations in Latin America and the Caribbean report a lack of critical people and skills to meet 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, and 85% report that AI-related risks have increased.
- This heightened concern is not unique to Latin America and the Caribbean but the region faces additional challenges. According to the survey, compared with other regions more than half of organizations in Latin America and the Caribbean (51%) report not having processes in place to assess the security of AI tools before deployment. Furthermore, data leaks are the most pressing cybersecurity issue linked to generative AI, according to 38% of respondents from the region.

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



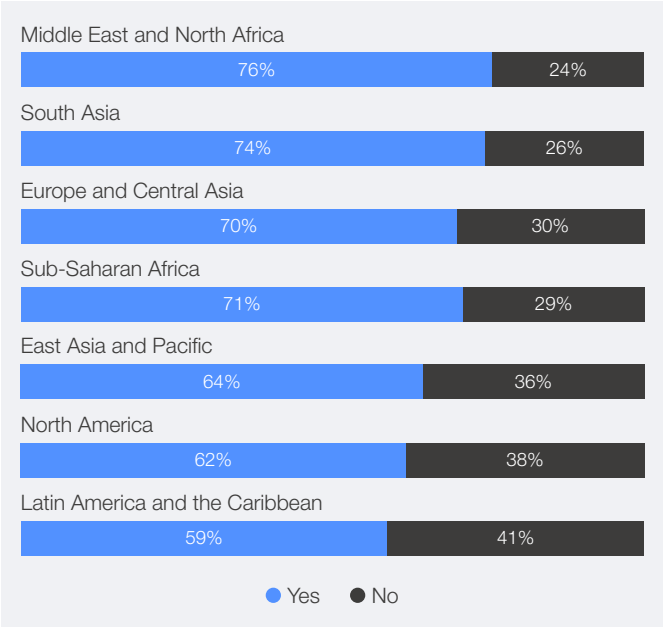
AI for security

- Organizations in Latin America and the Caribbean are actively adopting AI-enabled tools to strengthen their cybersecurity posture. Survey data indicates that 74% have already implemented such solutions, signalling strong momentum towards AI-driven security even if barriers remain.
- Despite this progress, 59% of organizations in this region cite insufficient skills as a key hurdle in embracing AI (globally 54%), while 46% point to uncertainty about risk as a major barrier to embracing AI for cybersecurity (globally 39%).

Geopolitics

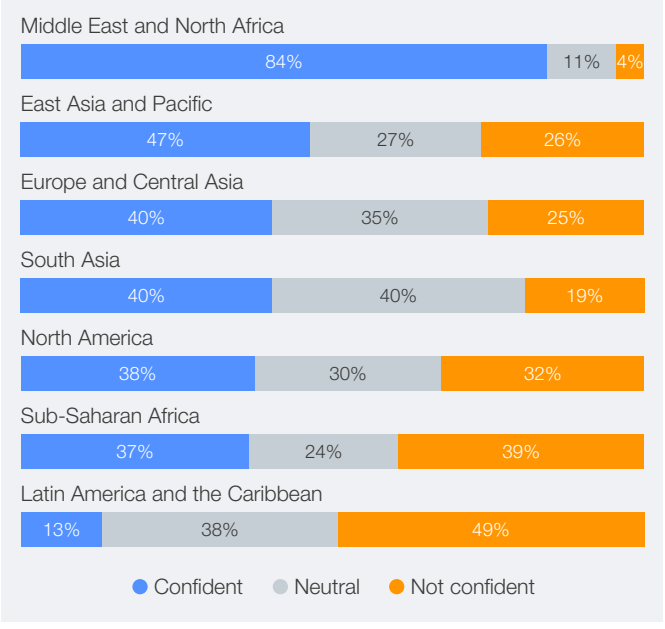
– Only 59% of organizations in Latin America and the Caribbean report adjusting their cybersecurity strategy due to geopolitical volatility, which is lower than the overall average of 66%. Additionally, 44% incorporate geopolitically motivated cyberattacks into risk mitigation plans, compared with a global average of 64%.

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



– Preparedness challenges are accompanied by relatively low confidence in national resilience. Only 13% of organizations express confidence in their country's ability to respond to a major cyber incident affecting critical infrastructure (globally 37%), with nearly half reporting no confidence. Compared to other regions, this represents the widest confidence gap.

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



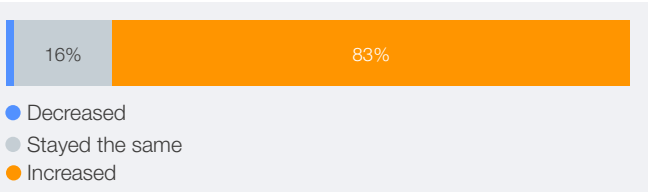
Cybercrime

– The GCO 2026 survey reveals that ransomware attacks and cyber-enabled fraud and phishing are the top two cyber risk concerns in the region, mirroring trends in Europe and Central Asia as well as in South Asia.

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, 83% of organizations report an increase in cyber fraud and phishing attacks, marking the second-highest surge in this category after AI-related vulnerabilities.

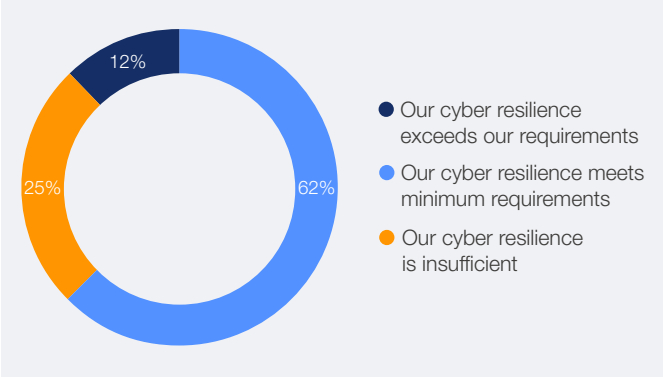
In the past year, do you think cyber-enabled fraud and phishing have increased, decreased, or stayed the same?



Resilience

– In Latin America and the Caribbean, 12% of organizations rate their cyber resilience as exceeding requirements, while around 25% assess it to be insufficient, resulting in the second-lowest resilience level across regions, according to the GCO 2026 survey.

How would you rate your organization's cyber resilience?



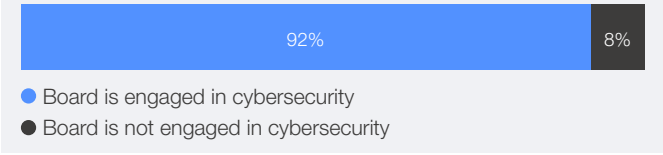
– The top three challenges to achieving cyber resilience reported by organizations in this region are:

1. Rapidly evolving threat landscape and emerging technologies (52%)
2. Shortage of cybersecurity skills and expertise (50%)
3. Third-party and supply chain vulnerabilities (40%)

– Additionally, 35% of organizations highlight insufficient incident response and recovery planning as a main challenge to resilience – the highest rate for this factor among all regions.

– Encouragingly, 92% report active engagement from their board in cybersecurity matters, which is similar to other regions (globally 93%).

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 Latin America and the Caribbean are:

1. Visibility: Lack of visibility in own organization's extended supply chain
2. Concentration risk: A high degree of dependence on critical third-party suppliers
3. Inheritance risk: Inability to assure integrity of third-party software, hardware and services

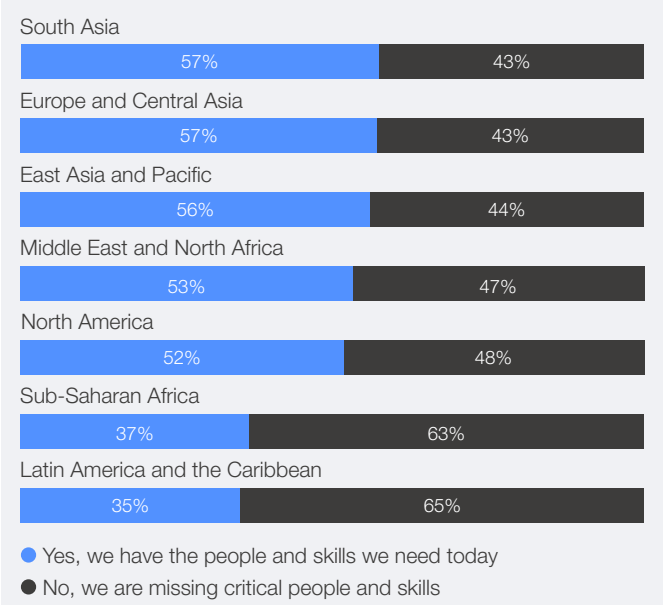
– To mitigate these risks, 58% of organizations in this region prioritize involving the security function in procurement processes, while 52% assess their supplier maturity. This approach is broadly consistent with practices observed in other regions.

How does your organization address supply chain cyber risk?

Cyber skills

– Organizations in Latin America and the Caribbean report the widest cybersecurity skills gap among the regions surveyed. Nearly 65% of businesses report they lack the workforce skills required to meet their current cybersecurity objectives.

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



– Moreover, 50% 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

  Notably, DevSecOps engineers and incident responders represent the highest percentages of missing cybersecurity roles across all regions.

– To address this challenge, 39% of organizations in the region report that they are leveraging AI to alleviate the cyber skills gap.

**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.