Global Cybersecurity Outlook 2026
Regional Analysis

North America

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 North America, providing a focused view of the region's evolving cybersecurity landscape.

Key takeaways on North America

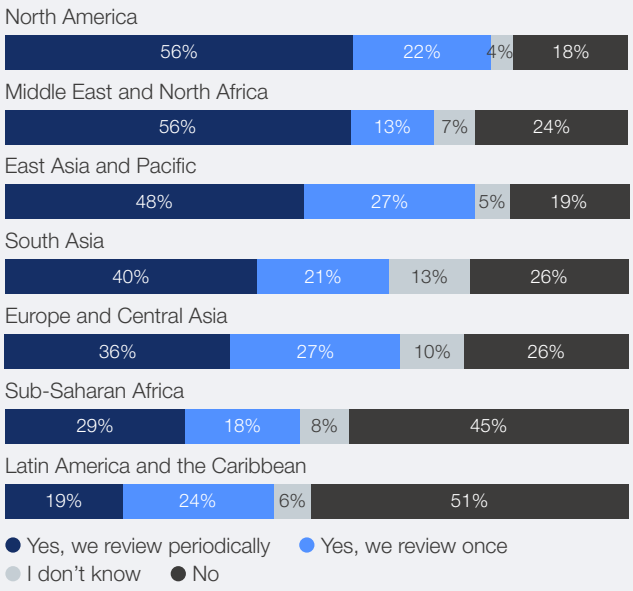
- 95% of respondents from North America reported that risks related to AI vulnerabilities have increased in the past year (globally 87%).
- 78% of organizations reported they have processes in place to assess the security of AI tools before deployment, exceeding the overall average across all regions (64%) and representing the strongest level observed.
- Cyber-enabled fraud is the number one concern in the region. Some 79% of respondents indicate they themselves or someone in their network has been affected by cyber-enabled fraud, compared with an average across all regions of 73%.
- 62% of organizations reported their cybersecurity strategies have evolved because of geopolitical volatility (globally 64%).
- 67% of organizations stated that they actively consider geopolitically motivated cyberattacks in their cyber risk mitigation strategy, compared with an overall average across all regions of 64%.
- 62% of respondents declared their cyber resilience meets minimum requirements, compared with an overall average across all regions of 64%, and 38% 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 38%).

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 92% report that AI-related cyber risks have increased (globally 87%).
- Furthermore, advancement of adversarial capabilities is considered the most pressing cybersecurity issue linked to generative AI in this region, cited by 35% of respondents. Data leaks rank second, highlighted by 30% of respondents.
- This heightened concern is not limited to North America but the region is taking additional measures to address it. According to the GCO 2026 survey, compared with other regions, 78% of organizations in this region report they have processes in place to assess the security of AI tools before deployment (globally 64%) – the highest level reported across regions.

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



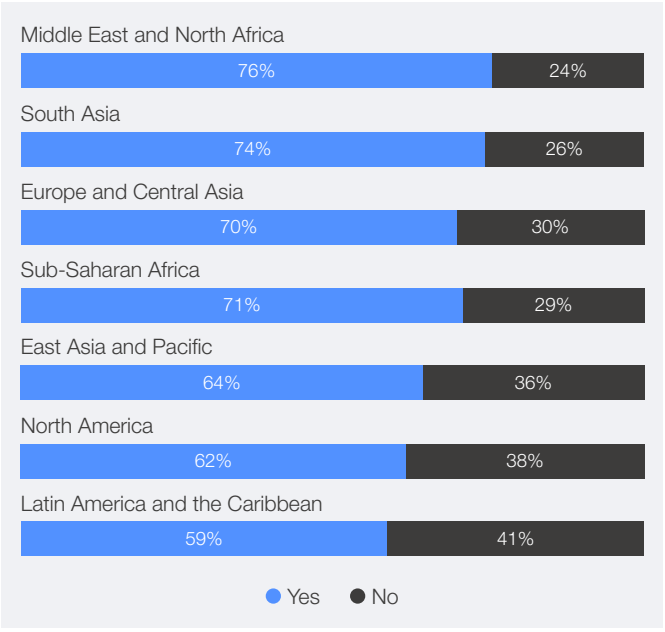
AI for security

- Organizations in North America are actively adopting AI-enabled tools to strengthen their cybersecurity posture, with survey data indicating that 80% have already implemented such solutions. This signals a strong momentum towards AI-driven security even if barriers still remain.
- Despite this progress, organizations in the region report several key hurdles in adopting AI for cybersecurity:
  1. Insufficient skills – cited by 50% of organizations as the most significant challenge
  2. Human validation required for AI-generated security responses – highlighted by 48% as a major barrier to implementation
  3. Uncertainty about risk – noted by 44% of respondents as a critical concern

Geopolitics

In North America, only 62% of organizations report adapting their cybersecurity strategy in response to geopolitical developments, a proportion slightly lower than most of the other regions. Nevertheless, geopolitically motivated cyberattacks remain the leading factor shaping cyber-risk mitigation strategies in the region, with 67% of organizations stating that they actively consider it in their approach.

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



- Preparedness challenges are accompanied by moderate confidence in national resilience. Some 38% of organizations express confidence in their country's ability to respond to a major cyber incident affecting critical infrastructure, while 32% report having no confidence. These figures broadly reflect the trends reported in other regions.

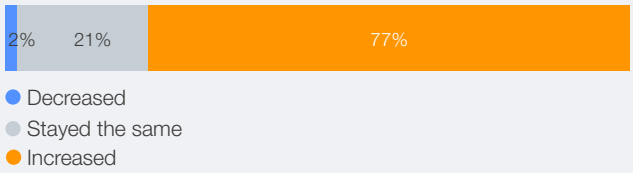
Cybercrime

- The GCO 2026 survey reveals that cyber-enabled fraud, phishing and exploitation of software vulnerabilities are the top two cyber risk concerns in the region.

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

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

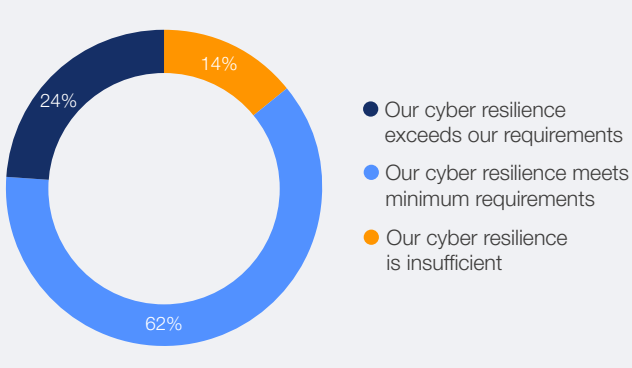
In the past year, do you think cyber-enabled fraud and phishing have increased, decreased, or stayed the same?



Resilience

- In North America, only 14% of organizations rate their cyber resilience as insufficient, while 24% assess it as exceeding their requirements – the second-highest percentage across all regions, according to the GCO 2026 survey.

How would you rate your organization's cyber resilience?

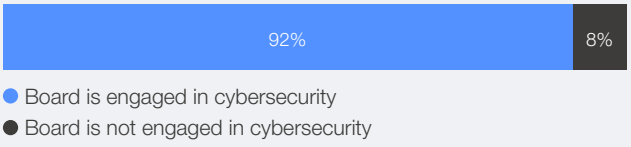


– The top three challenges to achieving cyber resilience reported by organizations in this region are:

1. Rapidly evolving threat landscape and emerging technologies (68%)
2. Third-party and supply chain vulnerabilities (47%)
3. Legacy systems (37%)

– 92% report active engagement from their board in cybersecurity matters, which is in line with the global average (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 this 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. Concentration risk: A high degree of dependence on critical third-party suppliers

– To mitigate these risks, 77% of organizations in this region prioritize involving the security function in procurement processes (overall average across all regions: 65%), while 75% assess their supplier maturity (overall average across all regions, 66%).

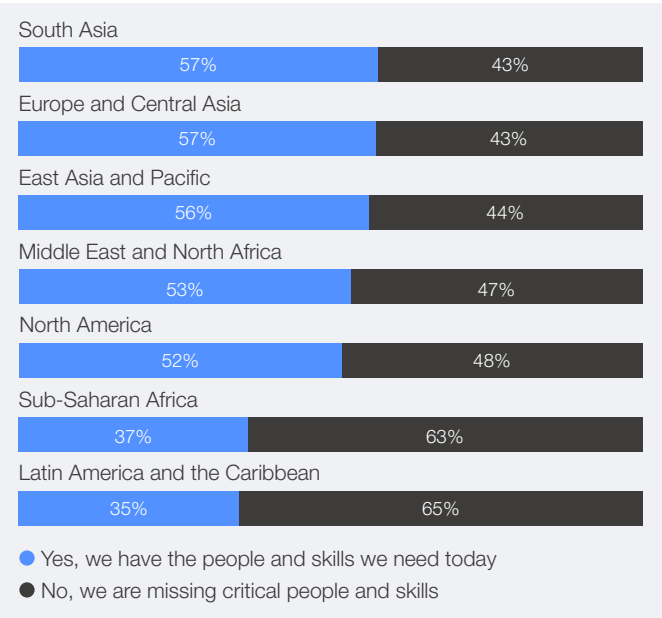
How does your organization address supply chain cyber risk?

Cyber skills

– 48% of organizations in North America report a lack of workforce skills required to meet their current cybersecurity objectives, almost matching the global average of 49%.

– DevSecOps Engineer is the most critical missing cybersecurity role in this region.

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.