QUOINTELLIGENCE

GEOPOLITICS, CYBER RISK AND STRATEGIC COMMUNICATION: A GROWING PRIORITY FOR CISOS

At QuoIntelligence, we strongly believe in the power of communities and the value of open dialogue, which consistently provides us with valuable insights.

In two recent sessions led by our CEO and founder, Marco Riccardi, we took note of the key takeaways that emerged from these conversations.

Here are some of the highlights:

*Geopolitical awareness emerged as a central theme in the evolving role of cybersecurity leadership. The event drew a full house of sharp minds, with approximately **85% of attendees being Global or Regional Chief Information Security Officers (CISOs)**. Participants came from a diverse set of industries, including Automotive, Finance, and others, highlighting the cross-sector relevance of the topic.*

GEOPOLITICAL AWARENESS AS A NEW OPERATIONAL MANDATE

One of the most revealing insights from the session was that nearly **70% of CISOs now monitor geopolitical developments daily**. This reflects how global tensions—such as the Russia-Ukraine war or trade restrictions with China—directly affect cybersecurity, from increasing the frequency of state-sponsored attacks to disrupting supply chains and access to critical technologies.

Geopolitical shifts also drive regulatory change and sanctions that impact vendors, infrastructure choices, and cross-border data flows. For CISOs, this means expanding their role beyond technical defense to include strategic risk interpretation, integrating political foresight into resilience planning. In today's environment, understanding international dynamics is as essential as managing firewalls.

COMPLIANCE AND THE REGULATORY TSUNAMI

The growing complexity of the threat landscape has led many CISOs to rely on dedicated compliance teams. **About 80% of those surveyed indicated that their organizations now have teams tasked with navigating regulatory obligations and adapting to shifting risks**. The scale and pace of change make it increasingly clear that managing cybersecurity is no longer a one-person task, but a collective effort requiring diverse expertise.

This is especially relevant in the face of what many now describe as a "regulatory tsunami" in cybersecurity. As geopolitical tensions trigger policy responses, regulations such as NIS2, DORA, and the Cyber Resilience Act are reshaping the obligations of public and private sector actors alike. Yet most CISOs admit they still respond reactively—adjusting to laws after they're enforced, rather than forecasting the political dynamics that give rise to them. In this context, **anticipating regulation is becoming a strategic advantage**.

THE CHALLENGE
OF TECHNOLOGICAL SOVEREIGNTY

A third area of concern discussed during the session was the widespread hesitation to onboard non-EU technology suppliers, with **more than 80% of participants expressing a clear preference for European vendors**. The rationale is consistent: in times of geopolitical uncertainty, reliance on foreign technologies introduces risk. However, participants also acknowledged that full autonomy remains elusive, as critical components—such as operating systems—still lack viable EU-based alternatives at scale.

This tension reflects a deeper structural issue: the **current limitations of Europe's technological sovereignty**. While policymakers have placed digital autonomy high on the agenda, organizations continue to face real-world constraints. Bridging this gap will require coordinated efforts between public institutions, industry leaders, and innovators.

BOARD COMMUNICATION
THE WEAKEST LINK?

Despite growing geopolitical awareness, many CISOs acknowledged that **communication with the board remains a major challenge**. Translating complex threats into clear, business-relevant language is still a weak point in many cybersecurity strategies.

Yet, effective board communication is essential. It improves risk prioritization, fosters executive alignment, and ensures that organizations can respond coherently to emerging threats. **In a context where geopolitics actively shapes cyber risk, board engagement must evolve into an ongoing, strategic dialogue.**

Cybersecurity leadership is expanding in scope and complexity. As geopolitical pressures, regulatory demands and board-level expectations converge, **CISOs must evolve into strategic enablers of resilience—well beyond the technical domain**.

QUOINTELLIGENCE

curious@quointelligence.eu www.quointelligence.eu