Cyber trends and risk mitigation

Thursday 18 June

Speakers

Justine Phillips
Partner (Chair)
Los Angeles
justine.phillips
@bakermckenzie.com

Carolina Pardo
Partner
Bogota
carolina.pardo
@bakermckenzie.com

Michael Schmidl
Partner
Munich
michael.schmidl
@bakermckenzie.com

Frankie Tam
Partner
Hong Kong
frankie.tam
@bakermckenzie.com

Dino Wilkinson
Partner
Abu Dhabi
dino.wilkinson
@bakermckenzie.com

This session explored how geopolitical tensions and regulatory change are reshaping the global cybersecurity landscape. Threat activity is increasing, particularly against critical infrastructure, and AI is accelerating this trend by enabling faster, more sophisticated attacks. At the same time, organisations are facing stricter regulatory expectations, including tighter reporting deadlines and more prescriptive technical and organisational security requirements.

Asia-Pacific: expanding frameworks and faster reporting timelines

Across APAC, cybersecurity laws are evolving, particularly in areas linked to critical infrastructure and national security. Regulators are expanding obligations, strengthening enforcement, and introducing shorter reporting timelines. In mainland China, for example, incidents may need to be reported within one hour for critical infrastructure and four hours for non-critical infrastructure. This is driving a shift towards operational readiness, with organisations expected to detect, assess, and report incidents within tight timeframes.

European Union: layered regulation and continuous resilience expectations

In the EU, proactive cybersecurity readiness is a core regulatory obligation supported by a layered framework of laws addressing operations, products, and infrastructure. Key regimes such as NIS2, the Cyber Resilience Act, and the Digital Operational Resilience Act (DORA) introduce strict reporting timelines, stronger governance, and supply chain risk management. There is a clear focus on management accountability and embedding security into systems and products, with regulators expecting organisations to continuously demonstrate the effectiveness of their controls.

United Kingdom: expanding scope and ransomware prohibition proposals

The UK's proposed Cyber Security and Resilience Bill will broaden the range of organisations in scope and capture a wider set of incidents, including those with the potential to cause significant disruption. It will also introduce a two-stage reporting model, with an initial notification within 24 hours followed by a fuller report

within 72 hours. Ransomware remains a key focus, with proposals for payment restrictions, prevention measures, and mandatory reporting.

Middle East and North Africa: emerging frameworks shaped by geopolitical risk

Across MENA, most countries have introduced cybercrime laws under a shared regional framework, but broader cybersecurity regulation remains limited outside key sectors and critical infrastructure. Saudi Arabia has developed this further by expanding its national authority from a strategic and advisory body into an active regulator with enforcement powers. The region also shows how geopolitical tensions are directly reshaping cyber risk, with conflict-driven targeting of data centres and digital infrastructure driving multinational organisations to reassess resilience and risk strategies.

Latin America: rising threats and regulatory convergence

Latin America has experienced a significant increase in cyberattacks in the past year, driving stronger regulatory responses. New laws, national strategies, and sector-specific requirements are emerging, alongside stricter reporting timelines and increased focus on governance and board accountability. However, varying levels of cybersecurity maturity across the region and ongoing skills shortages continue to present challenges.

North America: national security-driven controls and preparedness

Regulatory developments in the US reflect a strong national security focus, including controls on foreign access to sensitive data, evolving critical infrastructure reporting regimes, and new audit obligations such as annual cybersecurity certifications in California from April 2028. In Canada, organisations must put appropriate safeguards in place and report breaches that pose a real risk of significant harm as soon as feasible. In Mexico, obligations span multiple frameworks, with growing focus on personal data breaches and data connectivity risks, as organisations face increased exposure from real-time government access to data and mandatory data sharing with public authorities.

Across all regions, there is a clear emphasis on ensuring proactive cyber compliance. Practical steps for clients include undertaking gap assessments, conducting vendor due diligence, and regularly testing incident response plans through training and tabletop exercises.

To catch up on the webinars from our Annual Compliance Conference 2026, click here.