Cybersecurity Forecast 2026: EMEA

Google Cloud Security

This Google Cloud Cybersecurity Forecast 2026 special report aims to help EMEA organizations prepare for the unique threats and challenges they may face in the year ahead.

Cyber Physical and Other Threats

In October 2025, EU Commission President Ursula von der Leyen stated that Europe must use more than just traditional defense in order to counter escalating hybrid warfare. Throughout next year, Europe must be prepared for cyber physical attacks targeting critical infrastructure such as energy grids, transport, and digital infrastructure. Potential cyber physical attacks will likely be combined with information operations to undermine public trust.

We anticipate increased cyber espionage campaigns from state actors, particularly Russia and China, targeting European governments, defense, and research in critical and emerging technology sectors. Additionally, threat actors are expected to continue to target European supply chains, especially managed service providers and software dependencies, to gain access to numerous downstream targets.

DPRK IT Worker Expansion

By 2026, DPRK IT workers will likely have further established and scaled their expansion across Europe, posing financial and espionage risks to European organizations. Law enforcement pressure and awareness has stifled operations in the U.S., forcing these operatives to strategically pivot, focusing on Europe to secure employment and maintain revenue streams for the regime.

Organizations should anticipate a rise in aggressive extortion campaigns, as we've observed workers threaten to release sensitive data or source code. The workers' technical sophistication is also expected to grow, utilizing skills in AI and blockchain.

The adoption of corporate virtualized infrastructure and BYOD environments may challenge traditional security monitoring, making detection more difficult for global companies. This rapid formation of a global ecosystem, supported by facilitators in the UK, represents a growing risk.

Navigating the Regulatory Landscape

Regulatory frameworks on AI and cybersecurity will shift from preparatory phases to active enforcement in 2026, and organizations across EMEA will need to be ready.

In August, the EU AI Act's most stringent requirements, particularly for high-risk AI systems, will come into force. This necessitates an immediate, comprehensive approach to AI governance, forcing companies operating within the EU to implement robust risk management systems, ensure data quality and unbiasedness, and embed human oversight into their technology. The extraterritorial scope and threat of fines up to 7% of global annual turnover will compel businesses to swiftly demonstrate compliance, ensuring AI governance is appropriately reflected in their operations.

Simultaneously, the NIS2 Directive's transposition into national law will continue to shape the cybersecurity landscape. This expansion of scope across 'essential' and 'important' sectors makes cybersecurity an explicit board-level responsibility. Organizations will face new duties for supply chain risk management and mandatory incident reporting. With penalties reaching 2% of global turnover and introducing personal liability for senior management in the EU, and the UK's similar Cybersecurity & Resilience Bill following suit, 2026 will be defined by systemic governance changes driven by these and other regulatory pressures.

Download the full Cybersecurity Forecast 2026 report for a global look at what our Google Cloud security leaders and frontline experts are thinking about next year, from AI to cybercrime to nation-state activity.

Google Cloud