Cybersecurity Forecast 2026: JAPAC

Google Cloud Security

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

Political Espionage Targeting Diplomats, Notably at Conferences

In 2026, a series of high-profile political and security summits across the region are expected to serve as targets for increased cyber espionage activity. These events—The ASEAN Summit in the Philippines, the APEC Economic Leaders' Meeting in China, and the Pacific Islands Forum in Palau—will fuel operations seeking political, industrial, and military intelligence to gain a negotiation advantage, and inform sponsor nations' political positioning and decision-making.

Espionage campaigns will build upon 2025 activity targeting Southeast Asia diplomats, and a 2024 operation leveraging a U.S.-Taiwan defense industry conference-themed lure to target individuals likely associated with the event.

Vehicle-Mounted False Base Station Scams

In 2026, the threat posed by vehicle-mounted false base stations (FBS) will continue, utilizing deceptive tactics that exploit the inherent lack of security in cellular broadcast messages. These mobile stations impersonate legitimate cellular networks to lure nearby devices into connecting.

Once connected, the FBS can deliver phishing SMS messages—often promising discounts or other content—with links directing users to sites controlled by threat actors. This crime is often carried out by suspected China-nexus cybercriminals who hire low-level "mules" via social messaging applications like Telegram.

We expect this trend to persist given the lure of easy money and the challenge of apprehending the perpetrators. Despite successful law enforcement operations and arrests in countries like Thailand and Indonesia in Q1 2025, the operations quickly re-emerged in Q3. This demonstrates the profitability and resilience of the FBS tactic, indicating its continued use globally in the coming year.

Supply Chain Cyber Mandates

In 2026, organizations operating in or with ties to Japan and South Korea will need to implement substantial new, proactive supply chain cybersecurity mandates as both nations are tightening defense following high profile incidents.

Japan is rolling out a Cybersecurity Measures Evaluation System by Fiscal Year 2026. This system will require companies, particularly in the manufacturing sector (like chipmaking), to visualize and verify the security status of their supply chains to meet security effectiveness measures based on the international standard ISO/IEC 15408. The government will also use a new cybersecurity rating system to assess companies' overall security posture.

South Korea is overhauling its cyber defense posture for critical sectors like telecommunications following major breaches. This will translate into stricter government oversight and mandatory investments in robust security systems across their extensive technology supply chain.

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