Top risk leaders feel unprepared to deal with surging rates of AI-driven cyber attacks, finds new Aon study

- In the APAC region, cyber incident frequency rose 29 percent in the past year and 134 percent over the past four years.
- Ninety-eight percent of risk leaders said they do not feel fully prepared to manage AI risks.
- Of the 1,414 global cyber events analysed, 56 developed into reputation risk events. Reputation risk events could reduce shareholder value by 27 percent for businesses.

AUCKLAND, 04 Aug, 2025 - Aon plc (NYSE: AON), a leading global professional services firm, has released the APAC findings of its 2025 Cyber Risk Report, revealing a sharp rise in AI-driven cyber attacks and growing concern over systemic risk and technology supply chain vulnerabilities.

Cyber incidents spiked 29 percent over the past year — and 134 percent over the past four — as organisations face increasingly sophisticated and interconnected threats.

Social engineering, AI-powered deception and deepfake attacks are among the fastest rising threats, driving a 233 percent year-on-year increase in fraud-related cyber insurance claims.

New Zealand's longstanding sense of geographical security is being challenged as threats can now be orchestrated from anywhere.

Over the past 18 months, local entities have faced direct and significant impacts from overseas technology failures, including software supply chain disruptions and vendor outages. The increasing interdependence of systems means that even distant events can cause business interruption, data loss or financial harm.

The report calls out that technology interdependence is a Faustian pact, in that the benefits of innovation and efficiency come at the cost of greater exposure to external shocks.

Last year, 63 percent of suspected nation-state cyber operations globally originated in APAC. Many of these targeted critical infrastructure and key industries, often resulting in high-profile, reputationally damaging events.

Of the 1,414 global cyber events Aon analysed, 56 evolved into high-profile incidents with significant media attention. The companies affected in this way saw average shareholder value drop by 27 percent.

At the same time, there's a widening readiness gap. The report reveals that 98 percent of chief risk officers feel only "somewhat" or "not ready" to manage emerging AI-related risks. While 79 percent of businesses surveyed are already using or planning to use AI tools, just 32 percent have a formal inventory of them.

This rush to integrate AI — without addressing security, legal or risk implications — is expanding the digital attack surface faster than most companies can manage.

Encouragingly, organisations are getting better at recovering when incidents do occur. The percentage of entities paying a ransom dropped to an all-time low of 25 percent in 2024, with the median ransom payment sitting at USD $110,890 in the fourth quarter of 2024. These figures suggest improved disaster recovery and incident response plans, but also point to the value of planning ahead rather than reacting late.

For New Zealand businesses, the changing threat landscape is coinciding with more favourable conditions in the cyber insurance market. After ten consecutive quarters of pricing increases, rates fell by approximately seven percent in the first quarter of 2025, with broader coverage now available. This is prompting more organisations to reconsider their cyber insurance needs — whether entering the market for the first time or expanding existing programmes to match the scale of risk exposure.

“New Zealand businesses are getting more mature in how they approach cyber risk — but the old belief that we’re somehow safer because of our isolation no longer holds,” said Duncan Morrison, cyber practice leader in New Zealand for Aon.

“Disruptions to global software vendors and tech supply chains have already hit local organisations hard. As we adopt more advanced tools like AI and real-time data systems, the interconnectivity that powers progress also increases our exposure,” continued Morrison.

Morrison added that Aon is seeing more New Zealand organisations reassess their cyber insurance needs — not just because pricing is more competitive, but because the risk is now tangible.

“The rise in AI-driven attacks, the growth in fraud claims and the sharp drop in ransom payments all point to two things: the threat is real, and smart preparation works,” concluded Morrison.

Adam Peckman, head of risk consulting and cyber solutions, APAC, and global head of cyber risk consulting at Aon, says global and regional geostrategic tensions remain a key driver of cyber risk for companies in the APAC region.

“Nation-state-backed threat actors are increasingly using cyber campaigns for asymmetrical conflict, economic coercion, or corporate espionage. Businesses need the tools to make better, data-driven cyber decisions,” said Peckman.

Morrison agreed: “The good news is that businesses don't have to face these challenges alone. There are practical steps they can take today: from exploring cyber insurance options to using better data analytics for risk assessment and ensuring AI investments are properly protected. The key is to take action now.”

The APAC insights from the Aon’s 2025 Cyber Risk Report can be found here.

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries

with the clarity and confidence to make better risk and people decisions that protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

Media Contact

Jini Pillai
Jini.pillai@aon.com
+65 8133 8523