AON

How Organisations in Asia Pacific Can Navigate the Path Towards Cyber Resilience

Cyber attack or data breach is the number one risk facing organisations in the Asia Pacific region and is predicted to remain in this position by 2026, according to Aon's latest Global Risk Management Survey.

This reflects the pervasiveness of cyber risks in an increasingly technology-driven regional economy and mirrors a global trend of growing awareness of the expanding cyber threat landscape, as can be seen in the risk's steady rise in our survey's top 10 global rankings over recent years.

High-profile data breaches and ransomware attacks in the Asia Pacific region in successive years and increased focus on data protection by securities and privacy regulators combined with a recently hardening cyber insurance market cycle, are likely to have elevated cyber risk as the top concern facing many C-suite leadership teams.

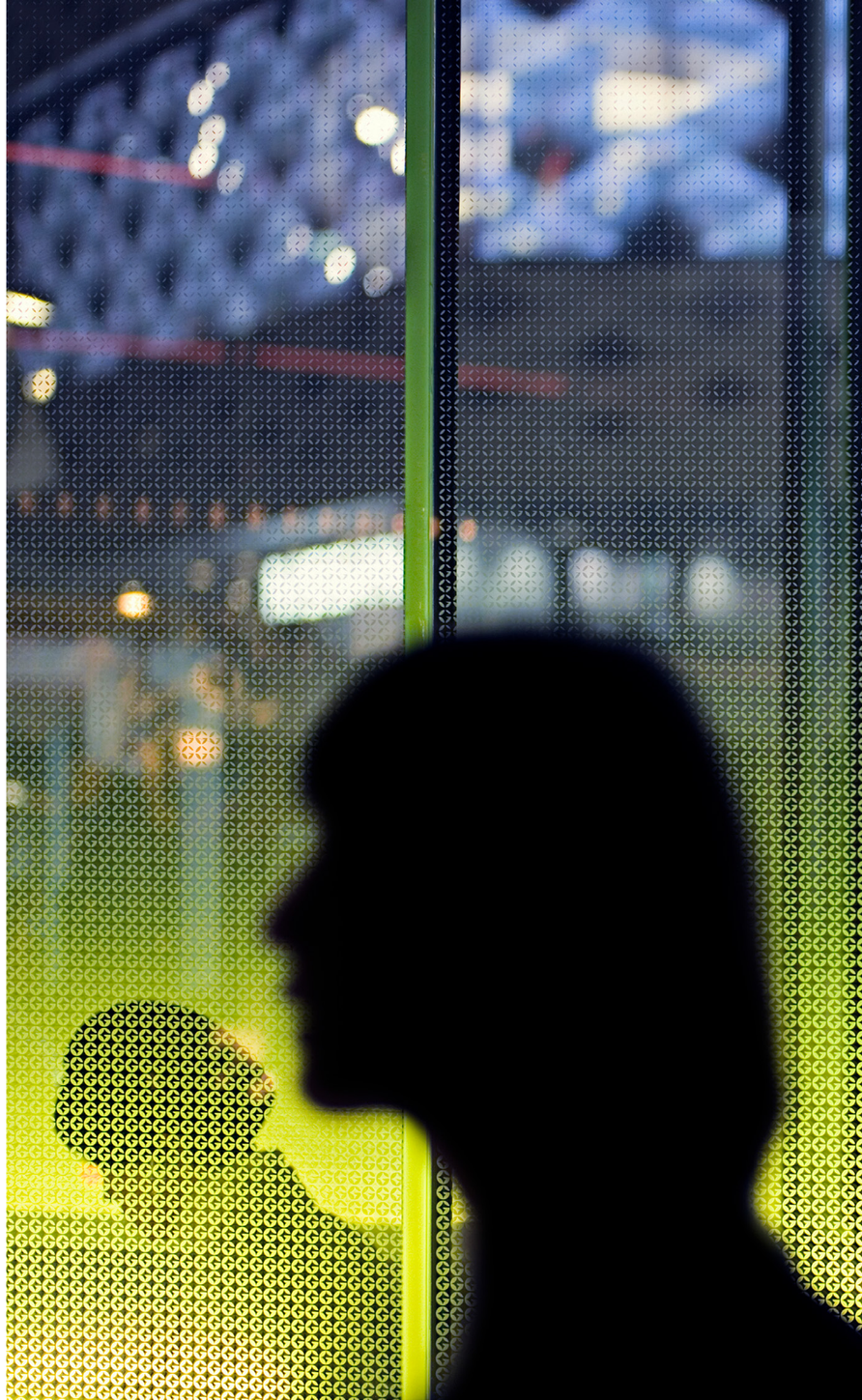
Cyber attack or data breach also maintains its number one ranking in Asia Pacific's top 10 future risks according to our survey, highlighting the strategic importance of managing cyber during a period of uncertainty in the region, characterised by a confluence of drivers shaping the outlook for cyber risk. These include geopolitical tensions that may result in the weaponisation of nation-state cyber capabilities, security challenges associated with the reconfiguring of supply chains across the region, and new cyber risks that will arise with the adoption of emerging technologies such as Artificial Intelligence (AI).

Why is a Cyber Attack or Data Breach a Top Risk for Organisations in Asia Pacific Today?

Cyber threats and ransomware attacks have become more frequent, sophisticated, and severe in the past four years, with impacts ranging from reputational and financial damage to strategically important infrastructure being compromised.

After peaking in 2021, the number of ransomware attacks in the Asia Pacific region declined in 2022 amid a period of competing geopolitical priorities for nation-state sponsored threat actors[1], a bottoming in the digital asset market (used to facilitate ransomware payments)[2], together with companies adopting better cybersecurity and risk mitigation (including more rigorous cyber-insurance underwriting) during that period[3].

Unfortunately, in 2023 this trend reversed. Ransomware attacks finished up 214 percent on a year-over-year basis in Q4 2023, and up 1,281 percent when indexed against ransomware frequency before the pandemic (Q1 2019)[4] signalling a need to remain vigilant in managing this threat through continued cyber risk assessments, testing of controls, and investment in appropriate response capabilities and insurance.



[1] Aon analysis of fund flows via on-chain data from Chainalysis. See also Top 10 Global Risks report on Cyber Attack or Data Breach, 7 November 2023
[2] Emily Nicole and Olga Kharif, A $2 Trillion Free-Fall Rattles Crypto to the Core, Bloomberg, 27 June 2022
[3] Aon analysis of cybersecurity maturity via CyQu data, published in Aon's 2023 Cyber Resilience Report, August 2023. See also APAC: Regulators and Companies Respond as Ransomware and Reputational Risks Intensify, 18 August 2023
[4] Aon analysis of Risk Based Security Data as of 1/1/2024; Claim count development may cause these percentages to change over time.

Aon's 2023 Global Risk Management Survey results also reflect this grim reality with one in five respondents reporting that their organisations had lost income from cyber attacks and data breaches in the prior 12 months. This is higher than the global average[5].

Due to the increasing deployment and dependency of technology[6], responding and recovering from cyber attacks, particularly those that disrupt business critical services, has become increasingly complex. The impact from cyber events extends beyond the immediate impact to IT systems, and can materially harm customers, partners, and shareholders[7]. Through the lens of impact to market capitalisation, the average loss of shareholder value from a cyber event amounted to approximately USD$3bn[8]. Consequently, a range of regulatory bodies – consumer, privacy, securities – in the Asia Pacific region are narrowing their focus on cyber-security requirements, and it is anticipated this will remain the prevailing board agenda item over the next few years.

Growing geopolitical tensions and the use of AI to facilitate cyber crime, are likely to also keep cyber risk high on the C-suite risk registers across Asia Pacific. Cyber attacks are increasingly being utilised by state actors in the region to create strategic leverage with rivals, build competitive advantage for local industry (predominantly via intellectual property theft), or signal military strength through non-kinetic actions[9]. Strategically important industries (construction and infrastructure, natural resources, and transportation and logistics) are all potential targets of these actions.

The role of AI in exacerbating cyber crime is also top of mind for many executives. Generative AI tools are increasingly being used to facilitate social engineering attacks by impersonating members of the C-suite, that result in employees, vendors, or even call centres mistakenly providing sensitive information, login credentials, or fund transfers. As companies navigate the economic opportunities associated with adopting AI they will need to contemplate the necessary security controls and guardrails to manage the potential threats.

Losses and Preparedness

Just under a fifth of respondents suffered a loss due to a cyber attack or data breach, and nine in ten indicated they have plans in place to respond to the risk[10].

20.2%

of respondents indicated cyber risk contributed to a loss for their organisation in the 12 months prior to the survey[11].

91.5%

of respondents stated their organisations had set up a plan to respond to cyber risk[12].

[5] Regional average 20.2% vs Global average 18.3%, Aon, 2023 Global Risk Management Survey, 7 November 2023
[6] Simon Lin, 3 strategies for delivering digital transformation in the Asia-Pacific, World Economic Forum, 30 January 2023
[7] Aon, Overcoming the Reputational Cost of Cyber Attacks: The 10-Day Plan, 25 September 2023
[8] Aon, Overcoming the Reputational Cost of Cyber Attacks: The 10-Day Plan, 25 September 2023
[9] The Council of Foreign Relations attribute 728 cyber events to state-sponsored entities since 2005. 102 of these occurred in 2023 alone. 61% of these involved state actors in the Asia Pacific region. Council on Foreign Relations, Cyber Operations Tracker
[10] Aon, 2023 Global Risk Management Survey, Cyber Attack or Data Breach, 7 November 2023
[11] Aon, 2023 Global Risk Management Survey, 7 November 2023
[12] Aon, 2023 Global Risk Management Survey, 7 November 2023

How Can Organisations Mitigate the Impact of a Cyber Attack or Data Breach?

Navigating the path to cyber resilience is challenging. But forward-looking resilience strategies are essential to help minimise financial, operational and reputational impacts from cyber events.

Although cyber risk is the top enterprise risk for Asia Pacific business leaders today, and over the next three years, the results of our survey identify that more focus and investment are required to improve cyber resilience.

Risk Management Strategies for Cyber Risk in Asia Pacific[13]

23.6%
Assessed risks

14%
Quantified risk

20.8%
Developed continuity plans

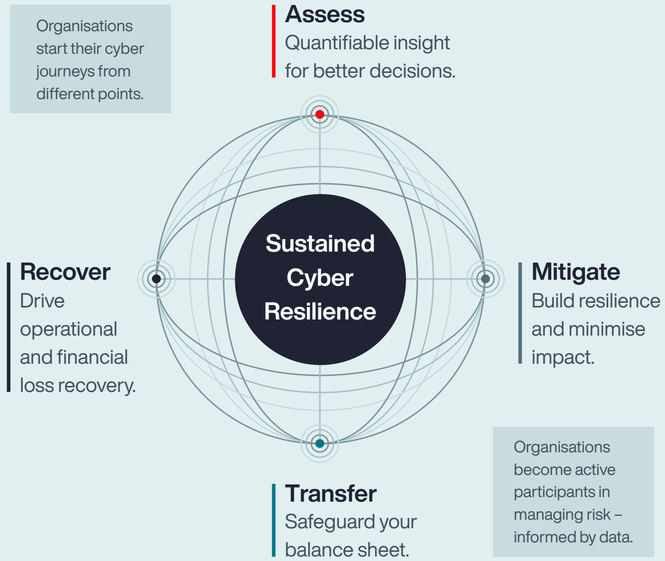
24.1%
Developed risk management plans

16.5%
Evaluated risk financing/ transfer solutions

27%
Current or Planned Captive strategy

To achieve this, companies in Asia Pacific should view cyber resilience as a risk management journey requiring a cross functional approach that combines risk assessment, risk mitigation, response preparation and recovery, and risk transfer mechanisms.

The Cyber Loop



[13] Aon, 2023 Global Risk Management Survey, 7 November 2023

Identify and assess cyber risk

From the results of the survey, only 23.6 percent of companies are assessing cyber risk, and 14 percent are formally quantifying the financial exposure from cyber risk[14]. It is critical that companies approach the construction of their risk mitigation and transfer strategies through the lens of the potential balance sheet exposure from a cyber event. Insights on the potential financial volatility created by cyber risk ensures the total cost of risk is optimised. Furthermore, presenting cyber risk in the context of financial loss and shareholder value erosion helps the C-suite, that may not have technical knowledge, to better understand the investment priorities to protect client, colleague, and shareholder interests.

Assessing and quantifying cyber risk should first involve assessing the adequacy of the control environment against a range of threat actors – most often, using an internationally recognised cybersecurity standard as the basis for that determination of control adequacy – then quantifying a range of credible cyber scenarios that could impact business operations. This should be extended to scenarios that include breaches of data privacy, disruptions to business-critical technology services, and events impacting the upstream or downstream suppliers and vendors.

> “Cyber still does not enjoy the same formal risk quantification approaches as the more traditional risk topics do, like property damage or business interruption. Companies must adopt these approaches to contextualise their investment settings in cybersecurity and cyber insurance. Doing so ensures these investments are appropriate to the balance sheet exposure and demonstrates an appropriately sophisticated approach to shareholders and regulators.”
>
> **Adam Peckman**
> Head of Cyber Solutions,
> Asia Pacific, Aon

The outcomes of this analysis may feed into a range of subsequent decision-making processes in the cyber resilience journey. Including control investment, recovery planning and risk transfer settings.

Mitigate cyber risk

A critical aspect of any cyber-resilience journey is testing and updating risk mitigation strategies, business-continuity arrangements, and disaster-recovery plans based on changes to systems, technologies and business operations.

In the Asia Pacific region, only 20.8 percent of companies have developed business continuity plans to address cyber events, and only 24.1 percent have developed risk management plans.

To help mitigate cyber threats and prepare for more-rigorous insurance underwriting, companies should continuously evaluate evolving threats and provide quantifiable evidence of the effectiveness of current controls to insurers and the marketplace.

This process should include having a thorough understanding of the attack surface of the company and key supply chain dependencies. As AI continues to be adopted, this understanding of the attack surface should extend to identifying any pockets of unknown AI usage, known as ‘shadow AI’.

Given the continued resurgence of ransomware, Asia Pacific companies should focus on security controls that mitigate these disruptive attacks, particularly controls that are a critical part of the insurance underwriting process. As the lack of these controls have been identified as contributing to losses tracked by the insurance market.

Ransomware strategies should include both technology and non-technology recovery plans. Technology plans include the security incident response (IR) and information technology disaster recovery (ITDR)

[14] Aon, 2023 Global Risk Management Survey, 7 November 2023

strategies. The non-technology recovery plans, that are left under-developed, should contemplate how the non-IT business operations (commercial, HR and finance for example) will sustainably work around a cyber event that is impacting critical technology platforms.

In addition to developing risk mitigation strategies for increasingly sophisticated cyber-attacks, risk mitigation plans should also address the human element to cyber risk. Half of the digital forensics and incident response (DFIR) matters handled by Aon in 2022 were related to social engineering and phishing[15]. Accordingly, security awareness training is a critical component in mitigating risks. The importance of complying with cybersecurity measures should be clearly communicated from the top levels of an organisation and reinforced with regular messaging, training and support.

Transfer cyber risk

Once a company has been through a structured process of assessing cyber risks and building appropriate risk mitigation strategies, the cyber resilience journey should consider the role of insurance. Risk transfer is important to deliver financial resilience and hedge shareholders from losses. Transfer options are not limited to traditional insurance placement – captive insurance and alternative capital are also viable approaches to support balance sheet protection. This is where formal cyber risk quantification plays an important role in deliberations on the most appropriate risk financing and transfer strategy. During the recent hardening of the cyber insurance market, Asia Pacific captive utilisation increased by from 24 percent to 27 percent[16]. However, these decisions should only be made with a range of datapoints, including exposure models, market pricing, and internal cost of capital calculations.

Prepare cyber-incident response and recovery

Recovering from a cyber incident can be a complex, and if not handled well, protracted process. Preparing in advance can allow organisations to initiate this process much more quickly and with greater success. Incident response, containment and investigation efforts should be undertaken alongside an assessment of financial and operational impacts, including third-party and insurance claims. With advance planning, these efforts can be measured against and aligned to business objectives while helping to expedite claims processing and work to achieve cash-flow neutrality.

> Managing the first 10 days of a cyber crisis was linked to 66% of total shareholder value loss[17].

Managing cyber issues, a top risk concern on the minds of business leaders in Asia Pacific both today and in the future, is best addressed with a holistic approach that comprises the full cyber risk lifecycle, with the goal of building and maintaining sustained cyber resilience.

[15] Aon, 2023 Global Risk Management Survey, 7 November 2023
[16] Aon, 2023 Global Risk Management Survey, 7 November 2023 and 2021 Global Risk Management Survey
[17] Aon, Overcoming the Reputational Cost of Cyber Attacks: The 10-Day Plan, 25 September 2023

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 and sovereignties with the clarity and confidence to make better risk and people decisions that help 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.

aon.com