AON

A Resilient Response to Social Engineering Risks in Asia Pacific

Key Takeaways

1

AI is supercharging social engineering attacks on organisations in Asia Pacific, increasing incident frequency and making scams more effective and harder to spot.

2

Vishing and deepfake campaigns designed to maximise financial gain are targeting people and supply chains.

3

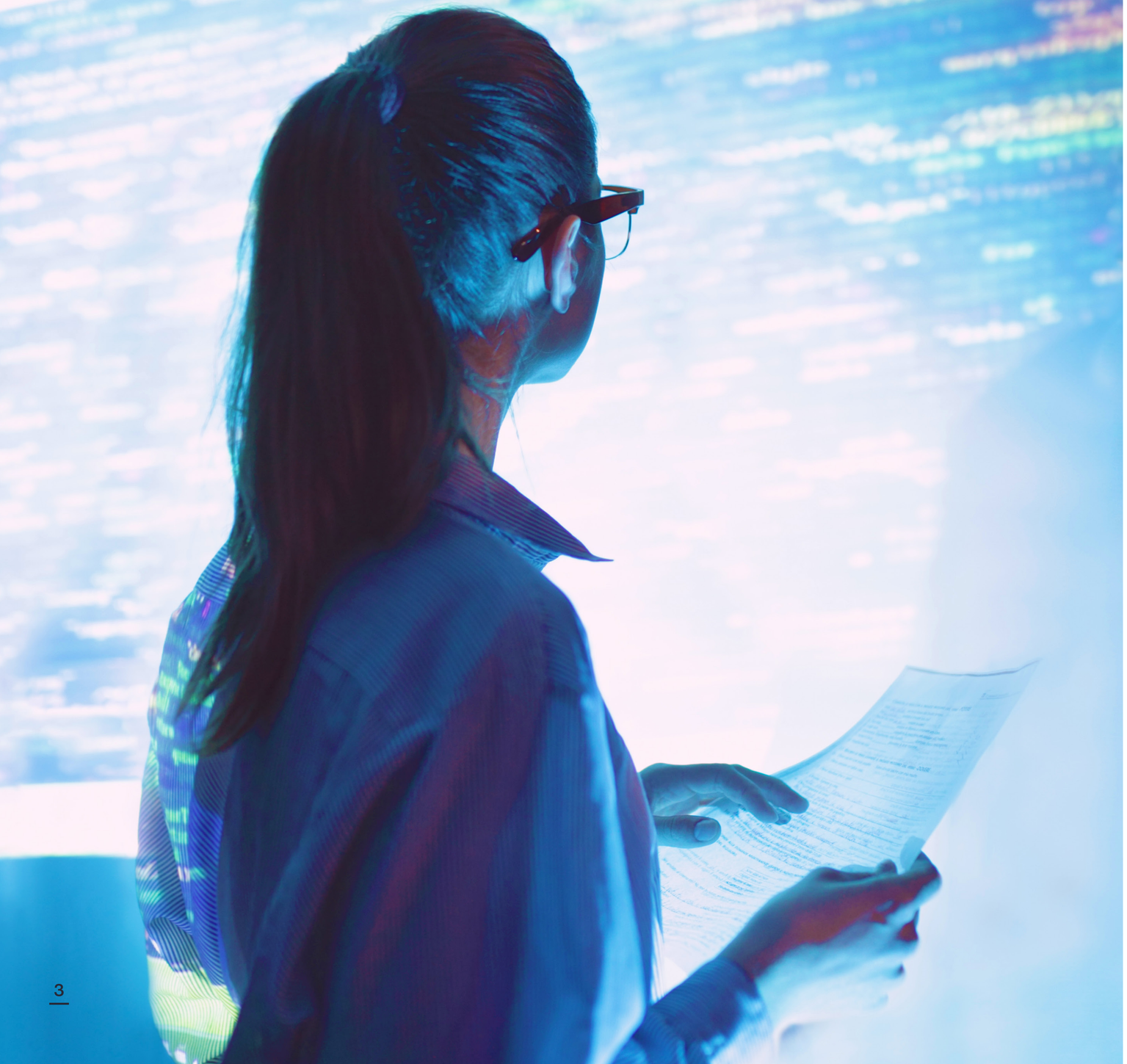
A combination of training for awareness, disciplined process, enhanced detection and carefully structured insurance (cyber plus crime) can help protect against losses.

Across Asia Pacific (APAC), cyber risk is on the rise. Aon's 2025 Cyber Risk Report reveals a 29 percent year-on-year increase in cyber incident frequency for the region, contributing to a 22 percent increase in cyber insurance claims in 2024. AI is playing a major part in this upward trend with a rise in AI-driven deepfake activity coinciding with a 53 percent increase in incidents utilising social engineering techniques and a 233 percent increase in social-engineering fraud claims.

AI is now front and centre on both sides of the cyber risk equation: attack and defence. It offers the potential to improve detection and response, yet it also increases the scale and effectiveness of social-engineering activity conducted through voice and video.

> "Social engineering is not really a new concept. But these new AI tools are supercharging this type of threat activity."

Duncan Morrison
Cyber Practice Leader
New Zealand
Aon



The Role of AI in Cyber Attacks

The objectives of cyber-attacks using these techniques are familiar. One pathway seeks unauthorised access to systems or data, often through impersonation and service-desk interaction to reset passwords or obtain support. Another goal is financial fraud, where instructions to carry out a transfer are presented by content that impersonates a senior decision-maker or trusted partner or supplier. In either case, the use of synthetic voice or manipulated video on collaboration and communication platforms can make routine verification more challenging if controls and processes are not robust.

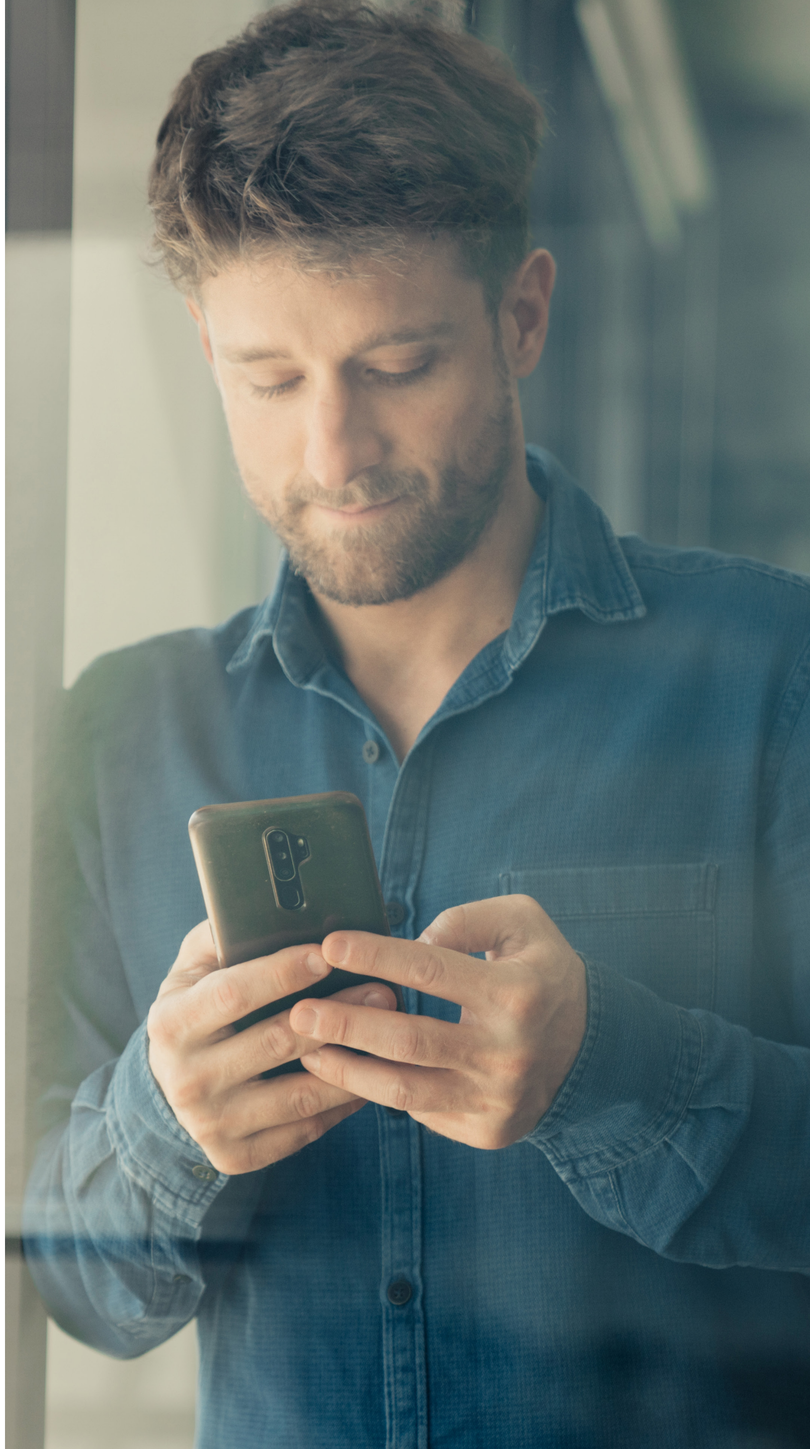
> “Vishing is particularly effective because it bypasses traditional technical controls. Threat actors can manipulate people over the phone without having to deploy malware.”
>
> **Thomas Tracey**
> Client Executive,
> Cyber Solutions Group
> Aon

How Vishing and Deepfakes Unfold

Video and voice impersonations can be combined in live collaboration environments to imitate legitimate stakeholders from an organisation. This enables cyber-attacks to be even more effective in convincing employees to follow routine requests for access or payment. A deepfake call, for example, could be followed by a second contact that appears to come from a legal authority, complete with documentation, to support a requested transfer.

> “Through a vishing event, a threat actor could obtain credentials and target either data exfiltration or disruption towards a ransomware incident.”
>
> **Thomas Tracey**
> Client Executive,
> Cyber Solutions Group
> Aon

Financial services firms remain one of the prime targets for vishing attacks, as attackers seek to exploit firms with immediate access to assets and frequent high-value transactions. Healthcare organisations, which hold vast amounts of sensitive data, are also frequently targeted, alongside technology and SaaS providers that present attractive opportunities for cyber criminals. Threat actors can seek access to help desks or password-reset workflows at managed service providers to access the data of their many corporate and retail customers. This supply-chain exposure is a vital consideration. When a provider is socially engineered, the ‘secondary risk’ quickly becomes the data and funds of the many organisations depending on that provider.



Consequences for the Bottom-line and Beyond

Financial loss is the most direct and immediate impact when fraudulent transfer requests are successful. The broader consequences are similar to those experienced across a range of cyber incidents. When credentials are captured, data ransom and financial demands will generally follow. In other cases, wider system disruption can be used to increase leverage. Reputational impact will likely depend on the quality and speed of an organisation's response, and how the incident is explained to stakeholders.

Responding with Resilience

People

Awareness training should keep pace with current techniques rather than generic phishing examples. Finance teams, controllers and approvers are a priority audience, given their role in verifying requests and initiating payments. Training should highlight behaviours associated with voice and video impersonation and provide clear steps for escalation when requests are inconsistent with established procedures.

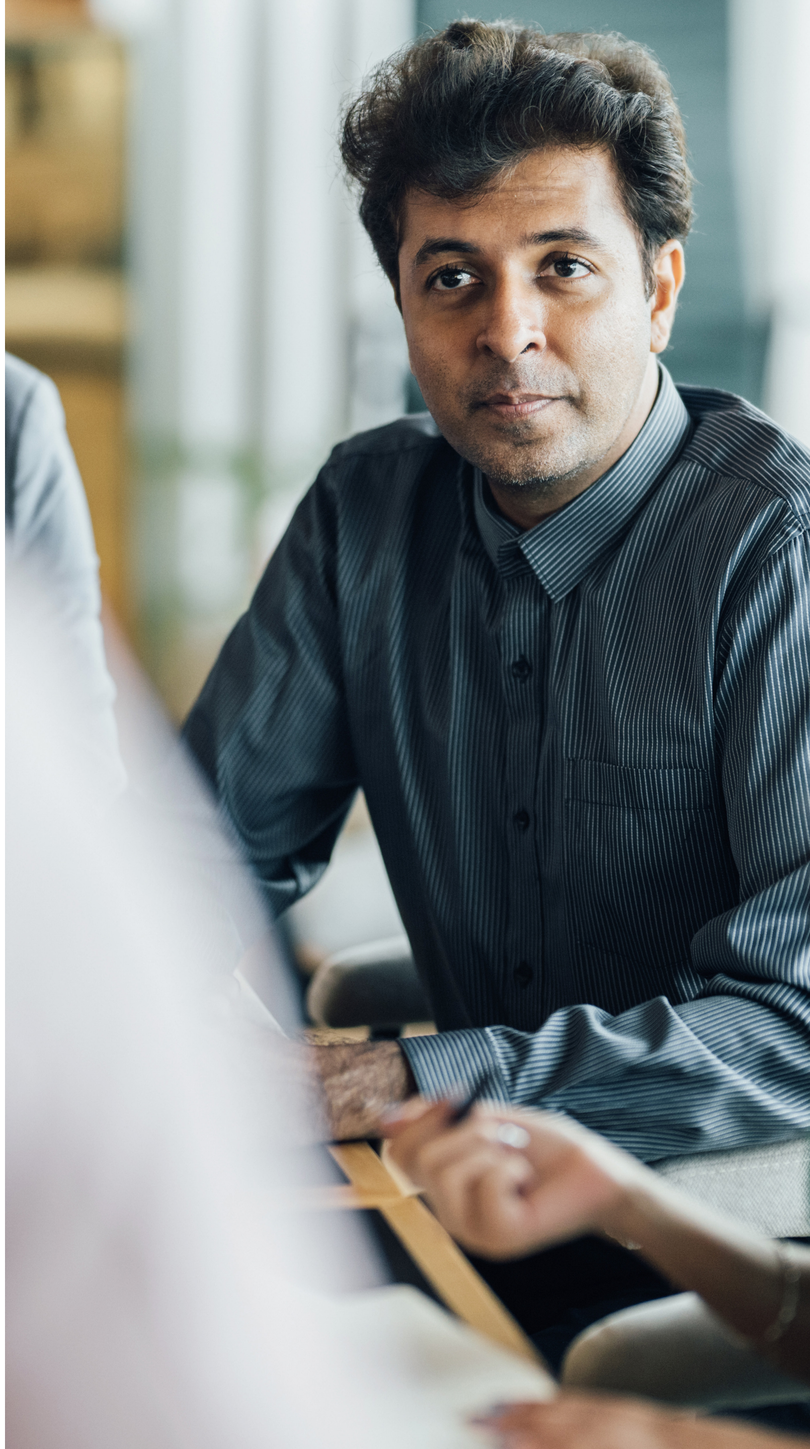
Process

Process discipline remains the most reliable defence against convincing but irregular requests. Standard operating procedures should require independent verification for changes to payment instructions and access privileges, using a separate communication channel where appropriate. Dual control for exceptional transactions reduces the probability of a successful attack, especially when timelines are compressed.

Organisations should also define the criteria for pausing activity while additional checks are completed and take steps to ensure these are well understood across finance, technology and procurement stakeholders.

Platforms

Controls for system endpoints and identities remain essential, supported by automated monitoring that can identify unusual access patterns or communication anomalies. AI-enabled analytics can shorten time to detection by tracking behaviour across systems and collaboration tools. Detection strategies should consider how voice and video content may be used to obtain access or validate a false identity and track interactions that change authentication status or authorisation scope.

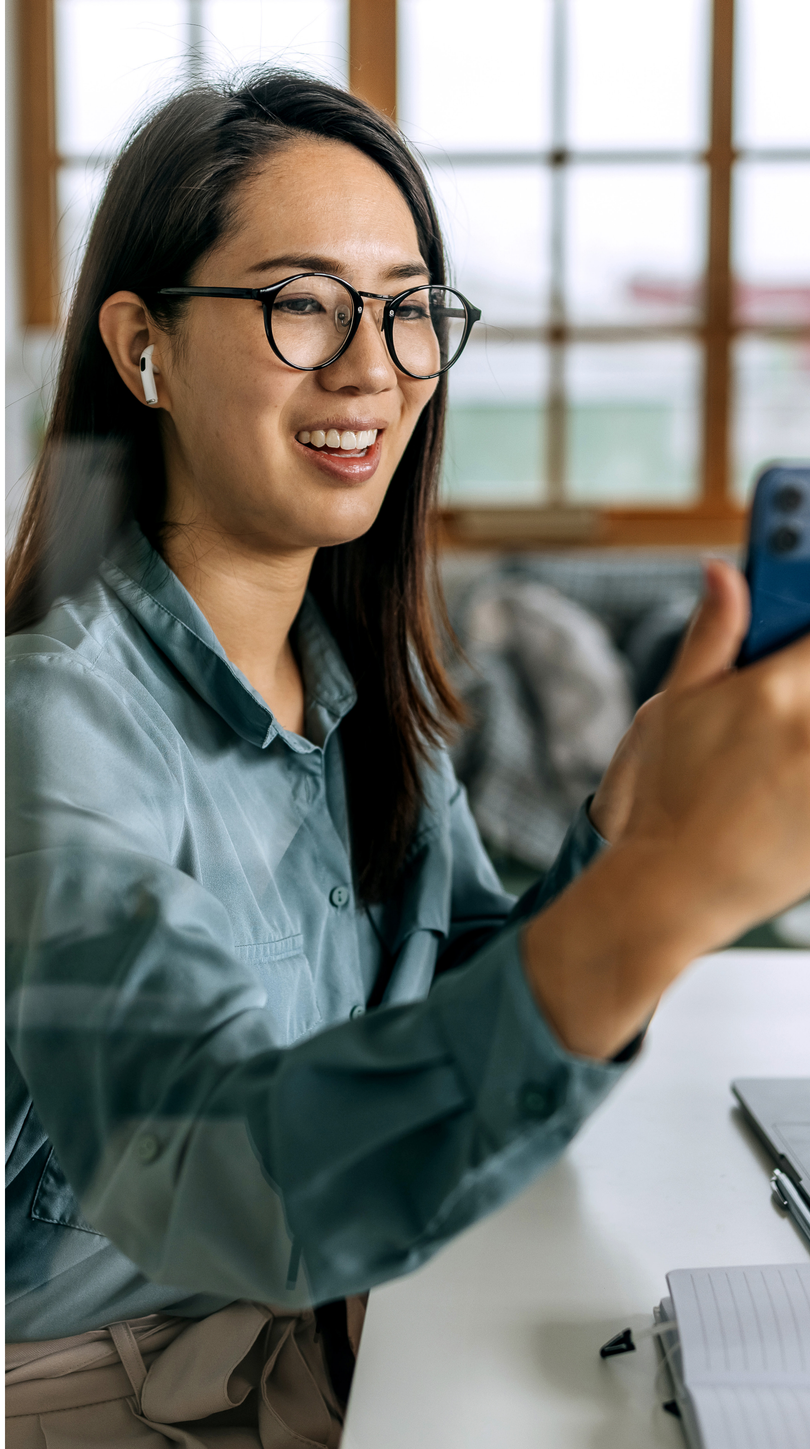


Using Insurance Intelligently

For organisations considering their insurance coverage in light of this change in the cyber risk landscape, the APAC market continues to offer competitive coverage with ample capacity available. Many APAC organisations compare well with global peers on cyber protection measures, recording a 16 percent year-on-year improvement in cyber risk scores, which supports the case for access to cover and competitive rates.[1] However, overall take-up across the region is still low, sitting at about 6 percent of the addressable market, which suggests scope for APAC organisations to use risk transfer more effectively.[2]

To renew or expand coverage, insurers will continue to look for evidence that access and security controls are effective in detecting and responding to exceptions and anomalies. They expect to see documented approvals, dual control for exceptions and second-channel verification for changes to payment instructions or access. They also look for clear identity and access controls and defined ‘pause’ criteria for unusual or urgent requests. Targeted training and periodic testing for approvers and service desks complete the picture, showing that the insured’s processes work under pressure — not just on paper.

Organisations should review how social-engineering fraud loss is addressed within their insurance cover and consider the interaction between cyber and crime policies for incidents involving vishing or voice-led deception. Risk leaders should determine how social-engineering loss is addressed in their current policies and exclusions, and review wording for events that may start with deception but lead to broader operational or data impacts.



[1, 2] Aon, Global 2025 Cyber Risk Report, Asia-Pacific’s Commitment to Cyber Security Pays Off, June 2025

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 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

Contact Us

Duncan Morrison
Cyber Solutions Practice Leader, New Zealand
duncan.morrison@aon.com

Thomas Tracey
Client Executive, Cyber Solutions Group, Australia
thomas.tracey6@aon.com