Continuum

CYBER INSURANCE AND THE EMERGING RISK GAP IN APAC

RISK INSIGHT SERIES

AUGUST 2026

Contents

AI Disclosure: This article was created with the assistance of AI tools for research and drafting. It was reviewed, edited, and fact-checked by our human editorial team before publication.

Introduction

Cyber policy wordings in market today were written for a threat environment that no longer exists in full. When most current cyber wordings were drafted, the dominant loss was a data breach: unauthorised access to a database, followed by regulatory notification obligations and remediation costs. That loss profile still exists. But it is no longer the loss profile that drives the largest claims.

Three shifts have moved the ground under cyber insurance. Ransomware has turned a security failure into an operational shutdown, with business interruption now the dominant cost driver. AI-generated attacks have introduced a new category of loss that sits awkwardly between cyber, crime, and social engineering fraud, exemplified by the USD 25 million deepfake fraud against engineering firm Arup in Hong Kong in early 2024.[1] Supply chain and third-party compromise has become the most common attack path, with 30 percent of all breaches in 2025 involving a third party, a 100 percent year-on-year increase.[5]

The environment in APAC has raised the stakes further. Regulators across MAS, HKMA, and JFSA have tightened technology risk management expectations. Manufacturing across the region accounts for 40 percent of all APAC cyberattacks, and the region's role in global software and logistics concentration means supplier disruptions in APAC now travel globally.[11]

What has not kept pace is the insurance response. Cyber policies renewed on similar terms to the prior year frequently carry the same limits, the same sub-limits, and the same wordings that were priced against a different loss environment. When a modern attack arrives, the cover often responds partially or not at all.

This report maps the emerging risk gap across four categories: what a modern cyber policy actually delivers, how business interruption has become the dominant cost, how AI-generated attacks have blurred the coverage lines, and where the three most common gaps sit in current APAC wordings. It closes with a view on what a defensible cyber programme looks like when the wording is aligned with the attack the firm is actually facing.

Background

How the Cyber Threat Landscape Has Shifted

The cyber threat environment in 2026 looks nothing like the one that shaped most cyber policy wordings in circulation. Two shifts matter most for the insurance response, and a third is now emerging as a distinct category.

From Data Breach to Operational Shutdown

The first shift is that ransomware has moved the dominant cyber loss from data breach to operational shutdown. Average ransomware downtime across industries reached approximately 24 days in 2025.[7] IBM's 2025 Cost of a Data Breach Report puts the average total cost of a ransomware incident at USD 5.08 million once downtime, legal exposure, remediation, and business interruption are included.[3] Sophos reports mean recovery costs of USD 1.5 million globally, with healthcare seeing means of USD 2.57 million.[4]

The critical finding for insurance sizing is that the cost of downtime as a result of a ransomware attack can frequently amount to fifty times more than the ransom demand.[7] A cyber policy sized to respond to a data breach and its associated regulatory exposure is often materially under-sized against a modern ransomware event, which drives cost through business interruption rather than through data-related liability.

From System Breach to Deception at Scale

The second shift is that AI-generated attacks have moved a share of the loss profile away from security failure and toward deception. The Arup case is the reference point. In early 2024, a Hong Kong-based finance employee at Arup, a UK-headquartered engineering firm, made 15 wire transfers totalling approximately USD 25 million to five bank accounts in Hong Kong after attending a video conference in which the group CFO and other colleagues appeared to be present.[1] The CFO was not present. Every participant in the call, apart from the finance employee, was an AI-generated deepfake.[8]

The attack pattern the Arup case exemplifies has continued to develop through 2025 and 2026. Deepfake video and audio impersonation of executives has moved from novelty to routine attack vector. Personalised phishing is generated at machine speed. AI reconnaissance tools scan for infrastructure vulnerabilities faster than any human red team.[2] The result is a class of loss that traditional cyber wordings, drafted around security event triggers, do not always contemplate.

From Direct Attack to Supply Chain Compromise

The third shift is that supply chain and third-party compromise has become the most common attack path. Thirty percent of all breaches in 2025 involved a third party, up from 15 percent the prior year.[5] Each vendor breach affects an average of 5.28 downstream companies, and disclosure windows have extended to 117 days on average.[5] For APAC firms, the exposure is compounded by regional concentration in manufacturing, software, and logistics.[11]

The rest of this report works through what these shifts mean for the insurance response.

What a Modern Cyber Policy Actually Buys You

The Emergency Services Sitting Behind the Indemnity

Most firms buy cyber cover thinking of it as protection against a data breach. The most valuable part of a modern cyber policy is not the indemnity for the eventual loss. It is the incident response the insurer mobilises within hours of the first call. For firms operating at scale in APAC, understanding what actually sits behind a cyber policy is the starting point for evaluating whether the cover is adequate.[14]

Incident Response Coordinators

Modern cyber wordings include access to a panel of incident response coordinators, on retainer with the insurer rather than appointed after the loss. When a breach or ransomware event is discovered, the first call to the insurer triggers deployment of the coordinator, typically within hours. The coordinator manages the vendor sequence: forensics, legal counsel, ransomware negotiation, crisis communications, and business continuity support.

The value of pre-appointed coordinators is speed. In a ransomware event, every hour without containment increases the eventual cost. Coordinators who already know the insurer's process, the panel of vendors, and the notification timelines move faster than counsel appointed on the day of the loss.

Digital Forensics

Digital forensics teams identify the entry point, the scope of the compromise, and whether data has left the environment. This is the diagnostic work that determines both the technical remediation and the legal notification obligations.

For APAC firms operating under MAS, HKMA, or JFSA supervision, the forensic timeline matters directly for regulatory notification.[15][16] A firm that can produce a defensible forensic report within days is in a materially different position from one that takes weeks to establish what happened. Cyber cover with strong forensic support built into the policy delivers that speed as a matter of course.

Ransomware Negotiation and Containment

Where the attack is ransomware, the panel typically includes specialists who handle negotiation and payment logistics where permitted. This is technical work with legal and reputational implications. Payment logistics involve sanctions screening on the ransomware group, cryptocurrency settlement mechanics, and the assessment of whether decryption keys received will actually restore the environment.[13]

For firms in Singapore and Hong Kong, sanctions screening of the ransomware group is not optional. Payment to a designated party can trigger separate enforcement exposure. The insurer's panel manages this screening as part of the response, which shifts a critical compliance step onto specialist counsel rather than the firm's own team.

Legal Counsel and Regulator Notification

External legal counsel advises on regulator notification timelines, customer disclosure obligations, and the sequencing of external communications. The specifics vary by jurisdiction. MAS expects notification of material technology incidents within one hour of discovery in some categories. Hong Kong has parallel timelines under the HKMA Cybersecurity Fortification Initiative 2.0.[16] Getting notification timing right is often the difference between a manageable regulatory response and an enforcement action for late disclosure.

Business Interruption Cover

Modern cyber wordings include business interruption cover for the days or weeks the systems are down. This funds lost profit during the outage, subject to a waiting period. The value of the BI cover depends heavily on how the wording defines the trigger, the waiting period, and the calculation of lost profit. Sub-limits on BI often cap the cover well below what a real outage would cost.[3]

Retainer vs Reactive Response

The distinction between a pre-appointed vendor panel and counsel engaged after the loss matters more than most buyers appreciate. Retained coordinators can be on a call within an hour of the initial notification. Counsel engaged after the loss typically requires days to onboard, review the underlying policy, and coordinate with the insurer. In a ransomware event, that gap costs money and reputational recovery.

The value calculation is simple. A cyber policy without a strong pre-appointed panel is essentially just an indemnity vehicle. A policy with a strong panel is an emergency service that pays out. For firms deciding between two placements at similar price points, the quality and depth of the vendor panel is often the more consequential differentiator.

Six Vendor Categories Inside a Modern Cyber Policy

A defensible cyber programme includes access to all six.

1. Incident response coordinator — mobilised within hours of the first call
2. Digital forensics — establishes entry point, scope, and data exfiltration
3. Ransomware negotiator — handles engagement and payment logistics where permitted
4. External legal counsel — regulator notification and customer disclosure
5. Crisis communications — public and stakeholder messaging
6. Business continuity support — operational recovery during and after the incident

> "The most valuable part of a modern cyber policy is not the indemnity. It is the incident response the insurer mobilises within hours."

Sizing the Cover to the Outage, Not the Breach

The Business Interruption Question Every Board Should Be Asking

The dominant cyber loss today is not the data breach. It is the business interruption that follows a ransomware event. Most cyber towers were built for the wrong scenario.[3]

Where Cyber Cover Has Historically Been Sized

Cyber cover has historically been sized to data breach exposure. That exposure has three relatively quantifiable components: regulatory penalties, notification costs, and third-party liability from affected data subjects. Actuarial models for these components have matured over the past decade, and insurers have priced cyber cover accordingly.

Business interruption is a different exercise. It requires modelling what the firm's operations would look like if core systems were unavailable for extended periods. Most firms have not done that modelling with rigour, and most boards do not have a defensible answer to the question of what a multi-week outage would cost.

What the Numbers Actually Show

The IBM Cost of a Data Breach Report 2025 puts the average total cost of a ransomware incident at USD 5.08 million.[3] Sophos data shows mean recovery costs of USD 1.5 million globally.[4] Average downtime across industries reached 24 days in 2025.[7]

The critical finding for insurance sizing is that the cost of downtime can amount to fifty times the ransom demand.[7] A firm evaluating whether to pay a ransom is often looking at the wrong number. The downtime cost is the larger exposure, and it accumulates whether the ransom is paid or not.

Contingent Business Interruption

Contingent business interruption cover responds when a supplier or vendor goes down. This is a distinct exposure from the firm's own outage, and it is often sub-limited well below the main aggregate.[5] For firms operating in APAC's concentrated software and logistics markets, contingent BI is where the largest supply chain losses land.

The sub-limit gap on contingent BI is one of the most consistent findings in mid-market cyber programme reviews. A firm with USD 10 million in main cyber aggregate may find its contingent BI capped at USD 1 million or USD 2 million, which does not respond to a supplier outage that shuts down the firm's own operations for weeks.

Reputational Harm and Customer Churn

Reputational harm and customer churn from a public cyber event show up in the following two to four quarters, not just the incident window. These are hardest to quantify in advance and hardest to insure. Cyber cover typically does not respond to reputational damage in a direct sense, but the associated revenue loss can be captured through well-drafted BI cover if the wording defines the recovery period broadly enough.

The Right Tower Reflects Operational Continuity

The right cyber tower reflects operational continuity, not just compliance exposure. For most APAC firms of scale, that means larger BI limits, broader contingent BI sub-limits, longer recovery periods in the BI definition, and explicit modelling of the outage scenario before the cover is placed.

How to Size the BI Cover

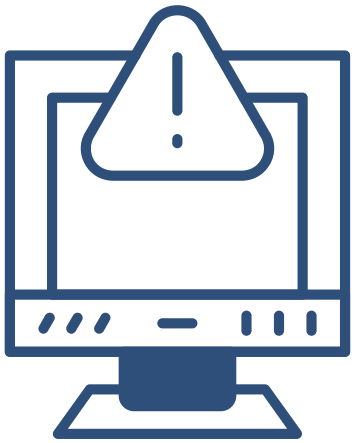
Sizing BI cover properly requires three inputs. First, the firm's daily revenue across every operating channel, quantified at the level of granularity the finance team already reports. Second, the fixed costs that continue to run during an outage: payroll, contracted vendor payments, real estate, licensed software. Third, the realistic recovery timeline for the firm's most critical systems, tested against a scenario in which the primary and backup systems are both compromised.

Multiplying daily revenue by realistic downtime, then adding fixed cost accumulation and remediation, produces the number the BI cover should respond to. Most firms have not run that calculation with rigour. Insurers are increasingly asking to see it before quoting.

Common Sizing Mistakes

Three sizing mistakes recur across mid-market cyber placements. The first is anchoring to peer benchmarks rather than the firm's own operational footprint. What a peer of similar revenue buys is a starting point at best, and often a misleading one where the peer's technology stack, customer concentration, or regulatory exposure differs materially. The second is accepting the default contingent BI sub-limit rather than negotiating it against the firm's real vendor concentration. The third is treating the recovery period in the BI definition as a technical detail rather than a load-bearing negotiation point, when the length of the covered recovery window frequently determines whether the cover responds to a real outage or only to the first phase of it.

Each of these mistakes is easy to make and hard to reverse mid-policy. The disciplined approach is to test the placement against a specific scenario at renewal rather than at claim.



The Deepfake Era and the New Attack Surface

What the Arup Case Changed, and Where the Cover Lands

AI has changed the cyber attack surface. The Arup case in Hong Kong is the reference point, and the pattern it exemplifies is now the shape of the attack facing large firms across APAC.

What Happened at Arup

In January 2024, a Hong Kong-based finance employee at Arup, a UK-headquartered engineering firm, made 15 wire transfers totalling approximately USD 25 million to five separate Hong Kong bank accounts.[1] The instructions came from a video conference in which the CFO and several colleagues appeared to be present. Every participant apart from the finance employee was an AI-generated deepfake, using video and audio synthesised from publicly available material.[1][2] The fraud was discovered only when the employee followed up with Arup's actual headquarters. As of early 2025, none of the funds had been recovered.[2]

Why the Arup Pattern Matters for APAC

Three features make the pattern particularly relevant to the APAC insurance market. The target was a legitimate finance employee acting in good faith on instructions from an apparently authorised executive. The loss was a voluntary transfer, not the result of unauthorised access. And the funds moved through Hong Kong banks in a single day, limiting recovery.[9] Similar deepfake-driven fraud attempts have been reported across APAC through 2025 and 2026.

The Coverage Grey Area

Cyber policies traditionally respond to losses arising from a security failure. The Arup loss was not a security failure. There was no unauthorised access, no data exfiltration, and no compromised systems. It was a voluntary transfer by an authorised user, triggered by deception.[1][2]

That scenario sits more naturally within Crime and Social Engineering Fraud cover than within Cyber. But Crime wordings often contain voluntary parting language that excludes losses arising from the insured's willing transfer, even where that willingness was based on deception.[10] SEF endorsements are typically sub-limited well below the main aggregate.

Where Wordings Are Catching Up

Some insurers have begun to reference AI-generated content and deepfake fraud explicitly in policy wordings. Most wordings in APAC market today are silent on the specific attack pattern. Silence at renewal is not neutral. It leaves the coverage question to be resolved at claim, which is the least favourable moment for the insured. A specific review of Cyber, Crime, and Social Engineering Fraud cover against the deepfake attack pattern is now a baseline discipline.

The Three Emerging Risk Gaps in APAC Cyber Wordings

Where the Cover Consistently Falls Short

Three gaps consistently show up in mid-market and fintech cyber placements across APAC. Each represents an area where the threat has moved but the wording has not. Each is fixable through specific negotiation at renewal, and each is expensive to leave in place until the first claim.

Gap One: AI-Specific Exposures

AI is rarely named explicitly in cyber wordings currently in market. Cover for model manipulation, prompt injection, or AI-generated fraud is typically inferred from the general security event trigger rather than affirmed. Where a claim arises from an AI-specific attack vector, coverage depends on how the insurer characterises the underlying event.

For firms deploying AI in their own operations, the exposure is compounded. Model poisoning, prompt injection against internal systems, and unauthorised access to training data all create loss scenarios cyber wordings were not drafted for. Requesting affirmative AI cover, or at minimum explicit clarification, is the disciplined response at renewal.

Gap Two: Supply Chain and Third-Party Risk

Supply chain and third-party risk sits under contingent business interruption, which is often sub-limited far below the main aggregate.[5] Thirty percent of all breaches in 2025 involved a third party.[5] Each vendor breach affects an average of 5.28 downstream companies, and disclosure windows have extended to 117 days on average.[17]

For APAC firms with concentrated dependency on regional software, logistics, or shared infrastructure, contingent BI is often the largest uninsured exposure.[11] A supplier ransomware event can shut down operations without any breach of the firm's own systems, and the sub-limit may not respond to the outage.

Gap Three: Social Engineering and Voluntary Parting

Social engineering is placed inconsistently across Cyber and Crime wordings, with voluntary parting exclusions catching claims that would otherwise appear to be covered.[10] A firm carrying Cyber cover with a social engineering sub-limit of USD 250,000 and Crime cover with voluntary parting language has, in practice, capped recovery at USD 250,000. The Arup case would exhaust that sub-limit approximately 100 times over.

Aligning triggers and sub-limits across Cyber, Crime, and any standalone Social Engineering Fraud cover is the disciplined response.

The Cumulative Effect

Each of these three gaps is a specific coverage issue that can be addressed at renewal. Cumulatively, they describe a market where the standard cyber wording was drafted for threats that no longer dominate. Insurers are beginning to update wordings, but the update is uneven and requires specific negotiation for each firm's exposure profile.

Building a Defensible Cyber Programme

What Coordination Across Cyber, Crime, and PI Actually Requires

A defensible cyber programme aligns wording across cyber, crime, and professional indemnity to close the emerging risk gaps. This is not a single-line placement discussion. It is a coordination exercise across multiple lines that respond to overlapping attack patterns.

The Coordination Question

The three lines that most commonly respond to a modern cyber event are Cyber, Crime, and PI. Cyber responds to security events. Crime responds to theft of money or securities. PI responds to professional service failures. In a typical ransomware or deepfake fraud event, more than one of the three may be triggered by the same underlying incident, and the question of which policy responds first, at what sub-limit, and with what notification obligations, determines the actual recovery position.

The disciplined approach is to align triggers across the three lines, coordinate notification windows so a single event does not trigger different actions in different policies, and stress-test sub-limits against realistic attack scenarios. Where the three lines are misaligned, coverage disputes at claim become almost inevitable, and defence cost erosion during the dispute can exceed the underlying loss.

The Scenario-Based Review

The best test of a cyber programme is not the schedule at placement. It is a scenario-based review that walks realistic attack patterns through the cover. Ransomware with 21 days of business interruption. A deepfake-driven wire fraud following the Arup pattern. A supply chain compromise flowing through a critical software vendor. Model manipulation of an internal AI system. Each scenario tests different combinations of trigger, sub-limit, and coordination.

Most APAC cyber programmes have not been reviewed against these scenarios explicitly. The renewal cycle is often treated as an administrative exercise, with prior-year terms rolled forward. That approach carries the greatest risk of unmodelled exposure at exactly the moment the threats are shifting most rapidly.

The Continuum View

The right answer for APAC firms operating at scale is a coordinated cyber programme built around the actual attack patterns, not the ones the wordings were drafted for. That means modelling the outage scenario with the board before sizing the BI cover. It means reviewing the Cyber, Crime, and Social Engineering Fraud triple against a deepfake attack pattern. It means treating contingent BI sub-limits as a specific negotiation point rather than accepting the default. And it means coordinating the wording across all three lines so a single event has a coherent response.[14] Continuum's practice is built around exactly that coordination question for firms operating across APAC's cyber, fintech, and digital asset markets.

Summary

The threat has moved. Most APAC cyber wordings have not.

Cyber policy wordings in market today were drafted for a threat environment dominated by data breaches. That environment still exists. But it no longer drives the largest claims. Ransomware has moved the dominant loss to business interruption, with average incident costs of USD 5.08 million and downtime averaging 24 days.[37] AI-generated attacks have introduced a class of loss that sits between Cyber, Crime, and Social Engineering Fraud, exemplified by the USD 25 million Arup case in Hong Kong.[1] Supply chain compromise has become the most common attack path, involved in 30 percent of breaches in 2025.[5]

What has not kept pace is the insurance response. Cyber cover has historically been sized to data breach exposure, which is quantifiable, rather than to business interruption exposure, which is harder to model but larger in scale. Contingent BI is routinely sub-limited far below the main aggregate. Social engineering fraud sub-limits are typically a small fraction of the actual transaction authority thresholds firms operate with. AI-specific exposures are rarely named explicitly in wordings. Coordination across Cyber, Crime, and PI is inconsistent, creating coverage disputes at exactly the moment defence costs are accumulating.

The three most consistent gaps in APAC cyber programmes are AI-specific exposures, supply chain and third-party risk, and social engineering fraud with voluntary parting exposure. Each is fixable through specific negotiation at renewal. Each is expensive to leave in place until the first claim.

For firms, the immediate action is to run a scenario-based review of the current cyber programme against realistic 2026 attack patterns: ransomware with three weeks of outage, a deepfake-driven wire fraud, a supply chain compromise through a critical vendor, and AI-specific attacks against internal systems. Sub-limits should be stress-tested against the exposures those scenarios actually produce. Triggers should be aligned across Cyber, Crime, and PI. Contingent BI should be treated as a specific negotiation point rather than a default sub-limit.

For insurers, the underwriting opportunity is real. APAC firms are increasingly aware that their cyber cover is sized for the wrong loss. Insurers that update wordings to name AI exposures explicitly, raise contingent BI sub-limits meaningfully, and coordinate with adjacent lines will write differentiated business. Those that renew on prior-year terms without engaging with the shift in attack patterns will find themselves declining claims at the moments the market is watching how they respond.

The attacker changed. The policy needs to change too.

References

1. CNN, "Arup Revealed as Victim of $25 Million Deepfake Scam Involving Hong Kong Employee," May 2024. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk

2. World Economic Forum, "Cybercrime: Lessons Learned from a $25M Deepfake Attack," February 2025. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

3. IBM Security, "Cost of a Data Breach Report 2025," 2025. https://www.ibm.com/reports/data-breach

4. Sophos, "The State of Ransomware 2025," 2025. https://www.sophos.com/en-us/whitepaper/state-of-ransomware

5. SecurityScorecard, "2025 Global Third-Party Breach Report," March 2025. https://securityscorecard.com/wp-content/uploads/2025/03/SSC-Third-Party-Breach-Report_031225_03.pdf

6. Verizon, "2025 Data Breach Investigations Report," 2025. https://www.verizon.com/business/resources/reports/dbir/

7. Deepstrike, "2026 Global Ransomware Statistics: Key Trends and Costs," 2025. https://deepstrike.io/blog/ransomware-statistics-2025

8. Fortune, "A Deepfake 'CFO' Tricked British Design Firm Arup in $25 Million Fraud," May 2024. https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/

9. CFO Dive, "Scammers Siphon $25M from Engineering Firm Arup via AI Deepfake CFO," 2024. https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/

10. Ward and Smith, "Social Engineering Fraud and Your Crime Policy: Why Your Insurer May Deny the Claim," 2025. https://www.wardandsmith.com/article/social-engineering-fraud-and-your-crime-policy-why-your-insurer-may-deny-the-claim-and-what-you-can-do-about-it

11. Cyble, "Supply Chain Attacks Surge in April to May 2025," 2025. https://cyble.com/blog/supply-chain-attacks-surge-in-april-may-2025/

12. Adaptive Security, "Arup Deepfake Scam: How $25M Was Stolen via Video Call," 2024. https://www.adaptivesecurity.com/blog/arup-deepfake-scam-attack

13. Financial Action Task Force, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs," 2025. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

14. Continuum, "Cyber Insurance," 2026. https://www.continuuminsure.com/coverage/cyber-insurance/

15. Monetary Authority of Singapore, "MAS Notice on Technology Risk Management," 2025. https://www.mas.gov.sg/regulation/notices/notice-on-technology-risk-management

16. Hong Kong Monetary Authority, "Cybersecurity Fortification Initiative 2.0," 2025. https://www.hkma.gov.hk/eng/key-functions/banking/cybersecurity-fortification-initiative-2-0/

17. Black Kite, "2026 Third-Party Breach Report," 2026. https://blackkite.com/reports/third-party-breach-report-2026

18. Recorded Future, "Third-Party Risk Statistics," 2025. https://www.recordedfuture.com/blog/third-party-risk-statistics

Continuum

Risk. Insurance. Technology.

hello@continuuminsure.com

www.continuuminsure.com