UIB CyberCube

Unlocking Asia's Cyber Insurance Opportunity: The Broker's Role in Growth

AUTHORS

Dimaggio Rigby, Head of Cyber and Fin Pro Lines, UIB

Yvette Essen, Head of Communications & Market Engagement, CyberCube

Jon Choi, Director of Insurance Risk Consulting, CyberCube

Nate Brink, Head of Broker Partnerships, CyberCube

INTRODUCTION

Asia represents one of the most significant growth frontiers for cyber insurance globally. A soft rate environment in the United States, United Kingdom, and parts of Western Europe, has encouraged underwriters to look further afield to higher-growth areas in the middle market and large corporate space.

Across Asia, however, penetration remains structurally low. In many markets, fewer than 5% of small businesses currently purchase standalone cyber insurance. Even in developed Asian economies like Japan, South Korea, Hong Kong, and Singapore, larger entities with multi-billion-dollar revenues often purchase only modest cyber limits relative to their exposures. This signals both underinsurance and significant room for structured market expansion.

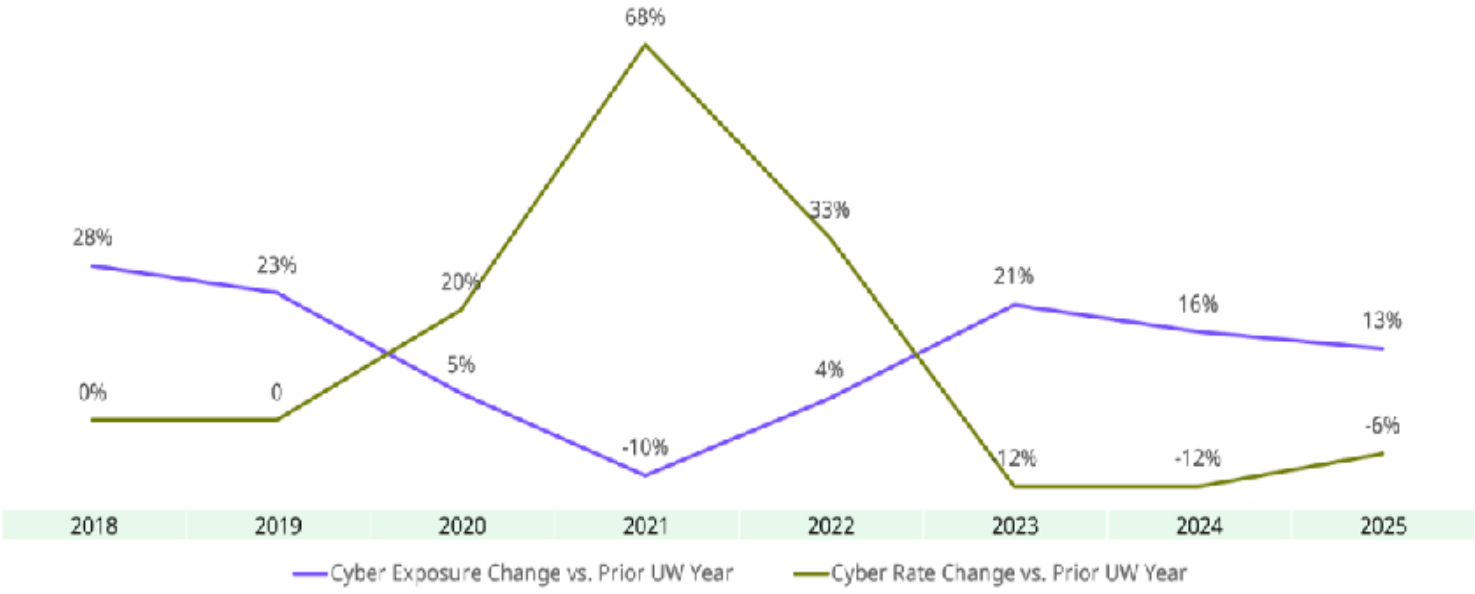
Leveraging its specialist cyber broking capabilities, United Insurance Brokers Limited (UIB) works with clients across Asia to assess cyber exposure, benchmark coverage levels, and structure insurance programmes aligned with evolving digital risk through its recently announced partnership with CyberCube. As the global leader in cyber risk analytics for the insurance industry, CyberCube has a growing client base in the Asia Pacific (APAC) region.

The central thesis of this joint report is that, in a softening cyber market defined by abundant capacity and pressure on rates, sustainable growth will not come simply from a favourable pricing cycle. It will emerge from developing markets such as Asia, driven, in part, by brokers who recognize opportunities in the Far East.

MARKET CONTEXT: LOW PENETRATION, RISING RISK

In a soft market, with cyber (re)insurers navigating a world of rising, increasingly complex threats, the underpenetration of the APAC market presents an opportunity. Growing competition has pushed cyber globally into its third consecutive year of rate reductions, as insurance supply continues to outpace demand (see **Exhibit 1**). This dynamic is offsetting recent exposure growth due to negative rate changes, and driving further concessions on premiums, coverage and security controls.

Exhibit 1: Global Cyber Rate Reductions Eroding Organic Exposure Growth (2018 - 2025)



Recent high-profile cyber incidents involving major Asian companies, including large-scale ransomware events and operational shutdowns, show that cyber risk in the APAC region is no longer theoretical. Attacks in the past year have included the Bank of China (Singapore branch) suffering a ransomware attack in April 2025, when customer data was exposed via a vendor (Toppan Next Tech). In September 2025, a cyber attack by ransomware group Qilin shut down production across Japanese beermaker Asahi for as much as a week, with October sales down 10% to 40% on the corresponding period the year prior. And, in December 2025, a cyber incident at South Korean e-commerce giant Coupang exposed data from nearly 34 million customers.

Such incidents are starting to shift perceptions and deliver a wake-up call for boards and decision-makers, prompting a reassessment of cyber resilience and financial protection strategies. UIB and CyberCube view post-event discussions as a valuable opportunity to educate clients and industries about their cyber exposures.

Evolving regulatory landscapes and increasing contractual requirements, particularly for companies working with governments or large enterprises, are also expected to drive greater demand for cyber insurance in the region.

However, even in more developed Asian markets, including South Korea, Japan, Hong Kong, and Singapore, large organizations with multi-billion dollar revenues often only purchase levels of cyber insurance coverage in single-digit millions of dollars.

"In many Asian markets, cyber risk awareness has increased significantly over the past few years, but insurance purchasing behaviour has not always kept pace," **says Dimaggio Rigby, Head of Cyber, Media & Tech RisksCyber Specialist at UIB**. *"We frequently see organisations with substantial digital dependency carrying cyber limits that would not fully reflect the financial impact of a significant operational disruption."*

RANSOMWARE ACCELERATION AND AI-ENABLED THREATS DRIVES INTEREST

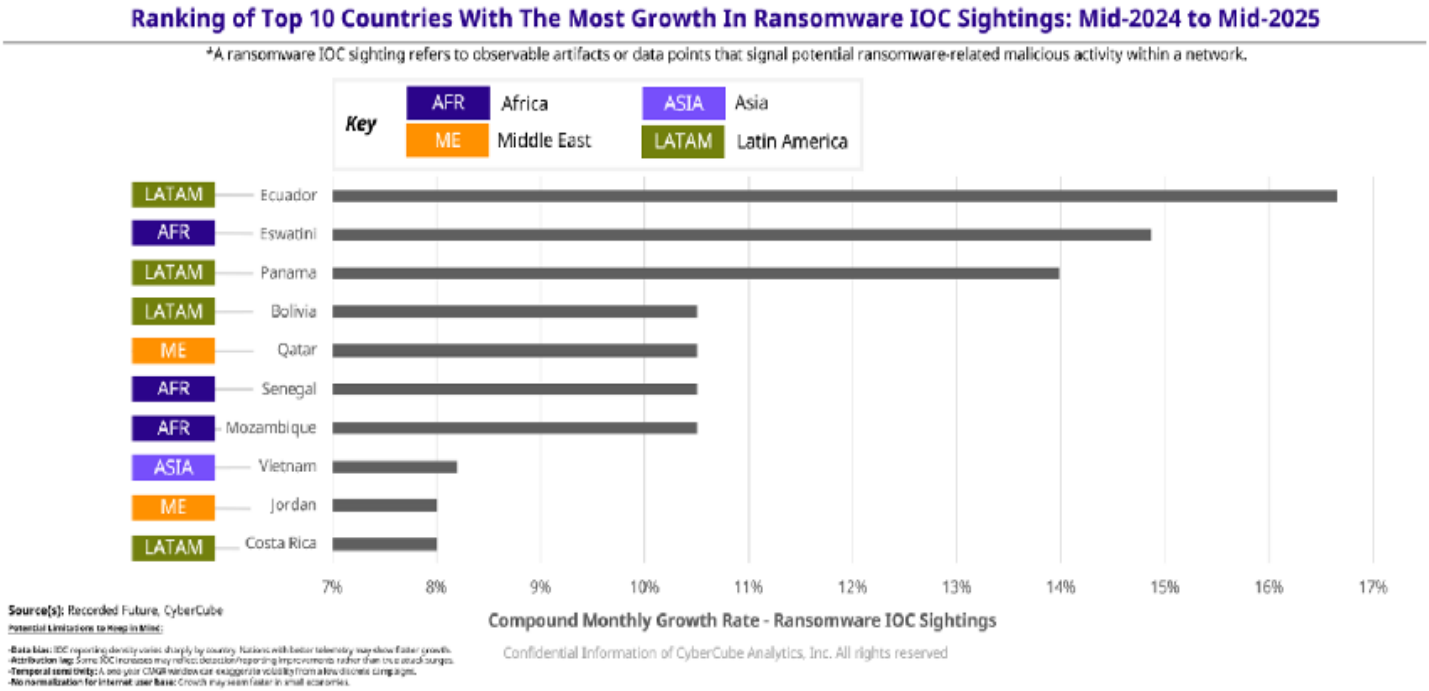
CyberCube and UIB have seen strong demand from Asia in the past year, with the region poised to emerge in 2026 as one of the fastest-growing markets outside the US. This has partly been fuelled by growing awareness of an increase in cybersecurity risks driven by a rise in ransomware demands across the region.

Rapid digital expansion, combined with unmatched cyber defences, creates concentrated exposures across the region. Weak IT Security postures leave organisations vulnerable to the kind of increasingly sophisticated attacks that are being observed in greater numbers.

Ransomware campaigns, phishing attacks, and business email compromise remain the most common forms of attack affecting individual businesses. Historically, linguistic and cultural differences provided a degree of insulation for many Asian markets, limiting the effectiveness of foreign threat actors. However, the rapid adoption of AI tools and large language models has significantly diminished this protective moat. These technologies enable attackers to generate highly convincing, context-aware, and grammatically accurate phishing and social engineering content at scale, lowering barriers to entry and increasing the effectiveness of cross-border attacks.

CyberCube analyzed recent ransomware trends in emerging economies across Latin America, Africa, the Middle East, and Asia. This study found a trend underscore ransomware's shift beyond traditional hotspots toward regions characterised by rapid digitalization, uneven defences, and growing strategic importance. Vietnam, which ranks in the top 10 countries in this study, is one of the countries within Asia where ransomware is spreading fastest, based on compound monthly growth rates of ransomware indicators of compromise (IOCs) from mid-2024 to mid-2025 (**Exhibit 2**).

Exhibit 2



Vietnam's economy has been experiencing a period of widespread and rapid digitalization, with strategic government initiatives targeting the digital economy and high-tech manufacturing to contribute 30% of its overall GDP by 2030. This growth in its high-tech economy is reflected in supply-chain vectors and manufacturing integration,and corresponds with attackers gaining footholds via third-party service providers in industrial supply chains, enabling cascading ransomware penetrations.

From a broking perspective, specialists at UIB note that ransomware scenarios remain one of the most frequent cyber risk concerns raised in client discussions across Asia. While awareness is increasing, many organisations still underestimate the potential scale of business interruption losses, which often represent the largest financial impact following a cyber incident.

UIB notes several recurring themes in cyber discussions with Asian clients:

- Increasing board-level awareness following high-profile cyber incidents
- Greater focus on business interruption exposure linked to digital dependency
- Growing contractual cyber insurance requirements within supply chains
- Demand for clearer benchmarking when determining appropriate policy limits

Alongside attacks and ransomware demands affecting individual companies, systemic cyber risk is becoming an increasing concern.

Businesses globally are consolidating their operations around a small number of major clouds, content management, and service providers. This concentration creates aggregation risk. While these providers maintain high uptime, even a brief outage can cause widespread disruption and global headlines. The trend toward digital consolidation suggests that systemic cyber events may become more prominent in the coming years, particularly in highly interconnected Asian markets.

UIB notes that the cyber market is responding by increasingly including IT supply chain failure coverage and various policy language amendments to ensure that insureds have indemnity against their third-party supplier exposure, on a security breach and business interruption basis.

EVIDENCE OF MARKET GROWTH

CyberCube's Broking Manager, which is powered by a growing database of real cyber policies and claims experience globally, reveals that intermediaries are actively monitoring opportunities in the APAC region. CyberCube's analytics platform enables intermediaries to communicate cyber risk to clients effectively and illustrates the financial exposure and benchmarking details needed to substantiate cyber insurance recommendations.

CyberCube's analysis of Broking Manager APAC company searches reveals a consistent year-over-year increase in 2024 and 2025 (see **Exhibit 3**). This trend points to growing demand for cyber insurance across both the large corporate and Small-to-Medium Business (SMB) sectors. The expansion within the SMB segment suggests a favorable movement toward more widely available and standardized regional policy

Exhibit 3: The APAC SMB Cyber Insurance Market (2024-2025) Market Adoption by Company Size

Segment	Revenue Tier	Adoption Growth (YoY)	Market Sentiment
Small and Micro Companies	Up to $250M	**+116%**	Mandatory Requirement/Shift toward Standardized Insurance Policies
Medium & Large Companies	$250M+	**+152%**	Mature Cyber Insurance Buyer/ Higher-Limit Requests

Opportunities for growth are increasingly concentrated in specific Asian markets and sectors. CyberCube analysis highlights India as a breakout market in the region, driven primarily by SMBs adopting coverage. While Financial Services remains the leading sector for cyber insurance demand, there has been a 400% jump in small manufacturing companies requesting cyber insurance (specifically in India). Hong Kong and Singapore are seeing secondary growth signals, albeit starting from a smaller base.

REGULATORY AND CONTRACTUAL MOMENTUM

Regulatory developments are expected to play an important role in accelerating cyber insurance adoption across Asia. While some markets may not impose explicit mandates requiring cyber insurance, evolving regulations and contractual obligations are likely to increase liability expectations. Businesses seeking to contract with governments or multi-national organizations may be required to demonstrate cyber insurance cover.

UIB believes this dynamic introduces drivers of structural demand that go beyond voluntary purchase decisions and reinforce the need for brokers to help clients quantify and justify appropriate limits. Expansion is expected to be driven by Asian enterprises that often lack a clear understanding of their true financial exposure to cyber threats. Many of these organisations also operate without internal cybersecurity leadership, lack dedicated specialised IT security teams, and have yet to implement structured approaches to risk financing.

Cyber insurance functions as a relatively affordable financial backstop against operational disruption, ransomware attacks, and business interruption costs and expenses. Carriers are increasingly partnering with technology providers and cybersecurity firms to offer more integrated solutions that combine risk transfer with preventative services before a cyber incident and response services after an incident.

This “full-stack” approach is particularly relevant for companies that cannot afford extensive in-house cybersecurity capabilities or need assistance in prioritising key services.

THE ROLE OF BROKERS IN FOSTERING GROWTH

Brokers play a critical role in helping organisations translate cyber risk into structured financial protection. UIB has prioritised analytics, education, specialisation and digital distribution. It has seen a shift in cyber risk discussions - from a focus on technical IT issues to a broader emphasis on financial impact and operational resilience planning.

To scale this segment profitably, brokers need to:

- Move from transactional premium discussions to financial impact modeling
- Embed benchmarking tools in client conversations
- Reduce administrative burden through digital integration
- Upskill generalist producers
- Develop sector specialization in high-exposure verticals

For brokers across Asia, sustaining client relationships and capturing new business requires shifting from a transactional focus on premiums to a more consultative approach centred on risk financing. Success depends on evolving into trusted advisors combining technology, specialisation, and data-driven insight.

Enhancing the advisory role begins with embedding analytics and benchmarking into the placement process. By providing clients with clear comparisons of their risk posture against regional and sector peers, UIB has brokers can transformed a routine transaction into a more strategic conversation.

Crucially, gaining credibility with senior decision-makers requires reframing cyber risk in financial terms. Brokers need to move away from technical language and articulate the balance sheet impact of cyber events.

"Leveraging advanced analytics, brokers can model loss scenarios to demonstrate how specific coverage limits mitigate a defined proportion of financial exposure," **said Nate Brink, Head of Broker Partnerships, CyberCube.** *"This approach not only strengthens the case for appropriate insurance limits but also supports investment in cybersecurity controls by evidencing how improved risk posture can lead to more favourable underwriting outcomes."*

ASIA'S DEFINING ROLE IN 2026

Asia represents one of the most compelling growth frontiers for cyber insurance, yet it remains structurally underpenetrated. Significant opportunity lies in expanding coverage among small and medium-sized enterprises, where uptake remains limited, as well as in addressing persistent underinsurance among larger organizations.

At the same time, the threat landscape is intensifying, with ransomware and AI-enabled attacks increasing in both frequency and sophistication, while systemic risks continue to accumulate across interconnected digital ecosystems. Regulatory expectations and contractual requirements are also evolving, increasing the need for more robust cyber risk transfer solutions.

In a soft market, growth will be driven less by rate increases and more by the industry's ability to attract bring new buyers into the market. Brokers who can effectively combine advanced analytics, client education, seamless digital workflows, and deep sector expertise will be best positioned to unlock this opportunity. As these dynamics converge, Asia is set to play a defining role in the next phase of global cyber insurance

ABOUT CYBERCUBE

CyberCube is the leading provider of software-as-a-service cyber risk analytics to quantify cyber risk in financial terms. CyberCube leverages data, analytics, artificial intelligence, and human resources to serve insurance institutions globally. The CyberCube platform was established in 2015 within Symantec and has operated as a standalone company since 2018. With offices in San Francisco, New York, Chicago, London, and Tallinn, Estonia, the team is committed to helping organizations and society build resilience to cyber risk. For more information, please visit www.cybcube.com or email info@cybcube.com.

ABOUT UIB

United Insurance Brokers (UIB) is a global insurance and reinsurance Lloyd's broker providing specialist solutions across a broad range of industries and geographies. With an expanding international presence—particularly across LATAM and Asia—UIB combines deep local knowledge with global expertise to deliver tailored placement strategies and advanced risk solutions. For more information, please visit www.uib.co.uk or contact enquiries@uib.co.uk.