Gallagher Re

Protecting the Digital Revolution

The state of the Asian cyber insurance market in 2024

Cyber insurance is a fast-growing market right across this dynamic region. If you are looking to underwrite in this area, here's what you need to know.

Key Points

- The Asia-Pacific (APAC) region has experienced rapid digital transformation of its economy and society in recent years, particularly since the COVID-19 pandemic. This has driven a corresponding increase in cyber risks.

- As a result, demand for cyber insurance cover is growing fast. The market in APAC has been expanding at an impressive rate, at almost 50% a year, to account for 7% of the global cyber insurance market as of 1st January 2024. There is plenty of scope for this to grow further, with market penetration rates still low compared to some other regions (in the US, cyber insurance premiums were worth 0.0353% of GDP in 2022, against an average 0.0025% across APAC — at least 14 times lower).

- The greenfield opportunity is particularly large for markets we identify as 'up-and-comers', like Thailand, Malaysia, Vietnam, Indonesia, and the Philippines; but equally, the emerging giants of China and India still have plenty of room for penetration rates to improve.

- One important driver for future growth is regulatory. Markets such as Singapore, China, and others across the region are implementing stringent data protection laws. Ensuring adequate cyber insurance coverage is often a requirement for compliance with these regulations.

- Cyber coverage for small and medium enterprises (SMEs), and even personal-lines coverage for individuals, represent significant untapped markets across APAC.

- As in other regions, the cyber insurance market in APAC has challenges to overcome. These include a lack of standardization in policy wording and coverage; the underwriting and risk-assessment challenges of keeping up with a fast-moving cyber threat landscape; and the relative lack of historical claims data in a new and evolving field.

- Reinsurance solutions can help insurers address these challenges. Reinsurance helps mitigate the financial impact of large-scale cyber incidents, allowing insurers to underwrite larger risks and provide more comprehensive coverage.

Introduction

The Asia-Pacific (APAC) region has experienced rapid digital transformation of its economy and society in recent years, particularly since the COVID-19 pandemic. This has driven a corresponding increase in cyber risks, which require robust insurance solutions.

This article explores the current market conditions, key drivers, challenges, reinsurance options, and prospects for the cyber insurance sector in the APAC region. If you're looking to underwrite cyber insurance, here is what you need to know.

Cyber Insurance: The Basics

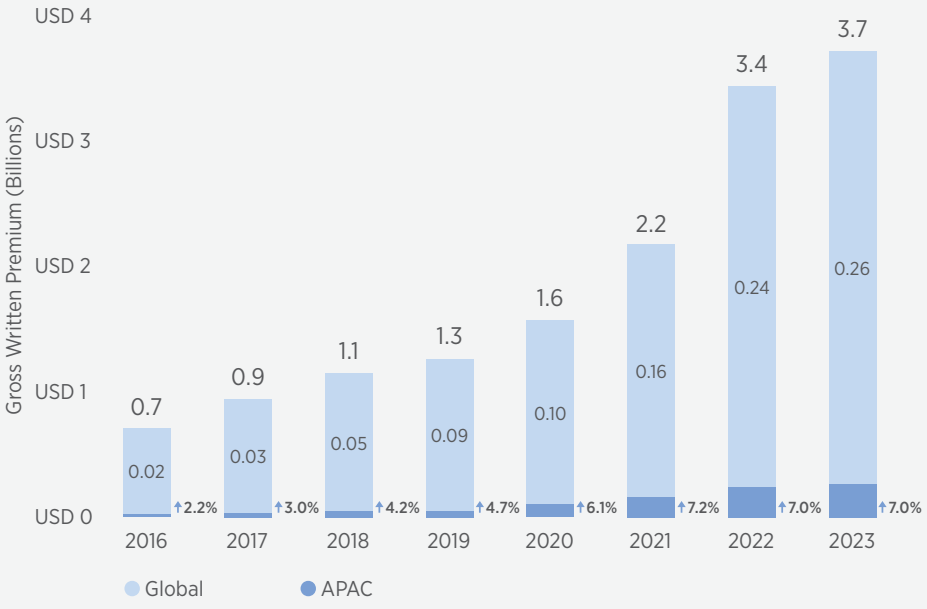
Cyber insurance is designed to protect businesses (as well as individuals) against the financial consequences of cyber incidents, such as data breaches, business interruptions, and cyber extortion. As businesses increasingly rely on digital operations, as well as individuals on digital adoptions, the importance of cyber insurance has grown, making it a crucial component of risk management strategies in the digital age.

Market Overview

The cyber insurance market in APAC has been growing at an impressive rate, at almost 50% a year, to 7% of the global market share (as per Lloyd's Statistics at 1st January 2024). This has been driven both by increasing awareness of cyber threats and regulatory changes. The market is characterized by a diverse range of players, including global insurers like AIG, Beazley, Chubb and Zurich; domestic carriers; and InsurTech startups. The demand for cyber insurance products is fueled by the rising frequency and sophistication of cyber-attacks, coupled with stringent data protection regulations enacted by several APAC countries.

LLOYD'S STATISTICS

Lloyd's Cyber Premiums represent approximatley 20%–25% of global



7% Lloyd's APAC domiciled Cyber business was **7% of the Global portfolio in 2023**; up from 2% in 2016.

2x APAC portfolio is **growing at twice the rate of the Global portfolio**.

APAC portfolio outperforming the Global portfolio in terms of profitability.

7-yr CAGR

27%

50%

Regional Insights

The APAC region's cyber insurance market is witnessing varied growth trajectories across different countries.

By the end of 2023, the number of privacy laws passed by governments in the region had expanded by nearly 25% compared to 2021. In the past year alone, several key jurisdictions – China, Thailand, and Indonesia – have either adopted or are in the process of implementing comprehensive privacy laws for the first time. Looking ahead, 2024 is set to bring two more major players into the fold: India and Vietnam. Meanwhile, countries with established privacy frameworks, such as Australia, Japan, South Korea, New Zealand, and Singapore, are continuously refining their laws to better align with European standards.

Notably, more jurisdictions are expanding the scope of their privacy laws to include extraterritorial provisions, mandatory breach notifications, and the appointment of data privacy officers. While concerns about stricter data localization rules persist, these requirements are largely limited to countries like China, and Vietnam. Encouragingly, India's latest legislative proposal omits such localization mandates, signaling a positive development.

We categorize these countries into four tiers based on their market maturity and regulatory environment.

APAC - TIERS IN READY POSITION

Positive penetration rates means APAC is poised to break through and thrive in the cyber insurance market.

	Country	Economic Indicators (2023 ~ 2022)				Non-Life					
		Population (mn)	GWP (USD mn)	Total Insurance Penetration	Nominal GDP (USD mn)	Non-Life Share of Wallet (SOW)	Penetration	Non-Life GWP (USD mn)	Cyber Premiums 2023 (USD mn)	Proportion Share of Non-Life GWP	Cyber Pen Rate 2023 (against GDP)
	Mature Asia										
Tier 1 Leaders	Australia	(mn)	59,235	3.8%	1,572,965	70.9%	2.7%	42,001	476	1.1328%	0.0302%
	Japan	125.1	339,321	8.0%	4,246,646	22.4%	1.8%	76,015	196	0.2581%	0.0046%
Tier 3 Fast Followers	Singapore	5.6	24,773	5.2%	480,226	15.0%	0.8%	3,727	39	1.0425%	0.0081%
	Hong Kong	7.3	71,197	19.7%	361,989	11.6%	2.3%	8,275	17	0.2062%	0.0047%
	New Zealand	5.1	8,095	3.4%	241,511	80.0%	2.7%	6,478	24	0.3667%	0.0098%
	South Korea	51.6	200,252	11.8%	1,703,596	47.5%	5.6%	95,145	3	0.0036%	0.0002%
	Taiwan	23.3	83,427	11.3%	741,261	8.7%	1.0%	7,221	2	0.0259%	0.0003%
	Emerging Asia										
Tier 2 Emerging Giants	China	1,411.8	675,296	3.9%	17,217,773	31.7%	1.2%	213,797	11	0.0051%	0.0001%
	India	1,417.2	110,407	3.9%	3,288,322	24.2%	0.9%	30,930	23	0.0739%	0.0007%
Tier 4 Up and Comers	Malaysia	33.0	20,214	5.0%	406,137	27.6%	1.4%	5,572	6	0.1025%	0.0014%
	Thailand	71.7	20,629	4.1%	501,576	38.4%	1.6%	7,919	5	0.0672%	0.0011%
	Indonesia	275.5	17,081	1.4%	1,248,810	36.6%	0.5%	6,246	7	0.1151%	0.0006%
	Vietnam	98.2	10,412	2.6%	402,851	27.5%	0.7%	2,863	1	0.0311%	0.0002%
	Philippines	115.6	7,466	1.9%	395,575	25.7%	0.5%	1,919	3	0.1638%	0.0008%
	APAC	**3,667.0**	**1,647,805**	**5.0%**	**32,809,239**	**30.8%**	**1.5%**	**508,108**	**813**	**0.1600%**	**0.0025%**
	US	**333.0**	**2,953,708**	**11.6%**	**25,463,000**	**77.5%**	**9.0%**	**2,287,801**	**9,000**	**0.3934%**	**0.0353%**

Source: Gallagher Re estimates

TIER 1

Leaders: Australia and Japan

- **Australia:** The cyber insurance market in Australia is expanding rapidly, driven by high-profile cyber-attacks and a proactive regulatory approach. The 2018 introduction of the government's Notifiable Data Breaches (NDB) scheme[1] has heightened the importance of cyber insurance for Australian businesses, and the market has a particularly high penetration rate.
- **Japan:** Japan's mature insurance market and strong regulatory framework make it a key player in the APAC cyber insurance sector. Japanese businesses are highly aware of cyber risks, and there is a growing trend toward purchasing comprehensive cyber insurance policies.

TIER 2

Emerging Giants: China and India

- **China:** As the largest economy in APAC, China's cyber insurance market is poised for significant growth. The Chinese government's focus on cybersecurity, coupled with the increasing number of cyber incidents, is driving demand for cyber insurance products.
- **India:** India's cyber insurance market is emerging, with increasing cyber threats and regulatory developments. The rapid digital transformation and heightened awareness of cyber risks are key drivers in this market.

TIER 3

Fast Followers: Hong Kong, Taiwan, South Korea, New Zealand, and Singapore

- In markets like **Taiwan, South Korea** and **New Zealand**, a generally advanced digital infrastructure is combined with growing awareness of cybersecurity threats among business and the general public. In most cases, this is further aided by government support and regulatory cybersecurity initiatives. All of these trends are likely to be supportive for cyber insurance.
- In addition, **Singapore**[2] and **Hong Kong** are also regional hubs for financial services and insurance, with regulators that are particularly active in promoting cybersecurity resilience in financial services as a result. Both markets are notable for penetration rates similar to Tier 1, albeit the overall size of these markets is much smaller.

TIER 4

Up and Comers: Thailand, Malaysia, Vietnam, Indonesia, and the Philippines

- **Thailand:** The cyber insurance market in Thailand is developing, with ongoing regulatory efforts to address cybersecurity concerns. The Thai National Cyber Security Committee (NCSC) has issued two notifications that require critical information infrastructure operators (CIIOs) to implement baseline cybersecurity protection measures in their data and information systems.[3]
- **Malaysia:** Malaysia's emerging awareness of cyber risks and government initiatives are driving the growth of its cyber insurance market. Malaysia is now placing a greater focus on combating cyber threats via regulations such as the Cybersecurity Bill and Cyber Risk Guidelines.[4]
- **Vietnam:** Rapid digitalization in Vietnam has increased exposure to cyber risks, creating a growing market for cyber insurance. In 2023, Vietnam introduced its first data protection law, the Personal Data Protection (PDPD) law. This law primarily focuses on safeguarding personal data and imposes obligations to maintain information security controls to prevent unauthorized access to personal data.[5]
- **Indonesia:** Indonesia, a country where digital insurance solutions have fast-growing appeal with the industry, presents a growing market with significant potential.[6] Significant strides have been made in the country's cybersecurity landscape, with policymakers prioritizing the enactment of cybersecurity laws in recent years. A testament to this commitment is the introduction of the inaugural Personal Data Protection (PDP) law in September 2022.
- **The Philippines:** The rising frequency of cyber threats in the Philippines underscores the need for a robust regulatory framework and increased adoption of cyber insurance. In 2024, the Philippines approved the National Cybersecurity Plan, which aims to effectively address the existing gap in cyber-security within the country. This comprehensive plan focuses on:
    1. Protecting critical infrastructure (CI),
    2. Improving government network security,
    3. Educating the workforce on cybersecurity,
    4. Reviewing existing cyber related laws and regulations such as the CPA.

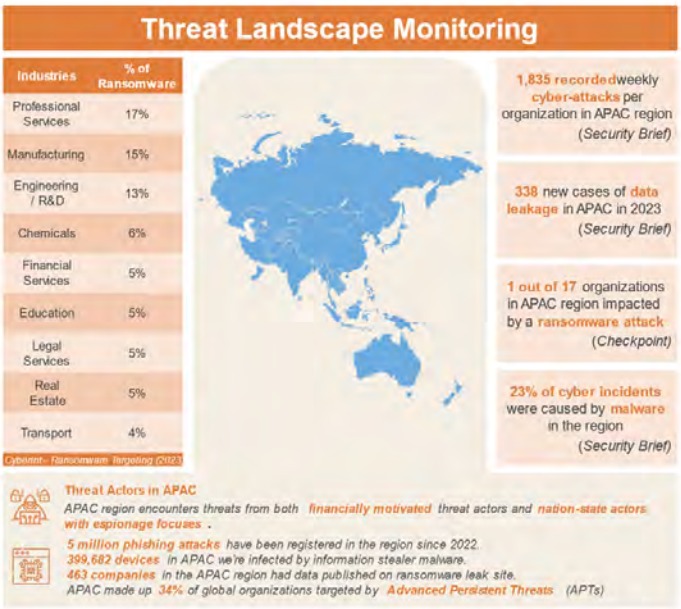
Key Drivers of Growth Across the APAC Region

Digital transformation: The APAC region has digitalized quickly, accelerated by the COVID-19 pandemic. For example, 94% of the region's population were covered by 4G mobile broadband in 2021 – up dramatically from around 60% in 2015. As a result, data traffic is also rising rapidly: between 2021 and 2025 monthly data usage in the region is set to grow from 12 to 37 gigabytes per subscriber on average, largely driven by the extensive adoption of 5G technology.[7] With greater connectivity, though, comes increased exposure to cyber risks. Industries such as finance, healthcare, manufacture and retail are particularly vulnerable.

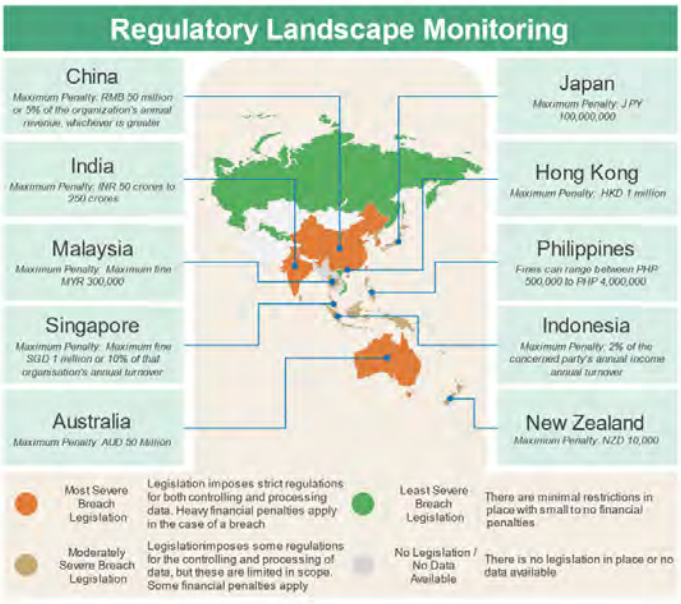
Increased cyber threats: The APAC region has become a prime target for cyber-attacks, with countries like Australia, China, India, Indonesia, Japan, and South Korea experiencing significant breaches. These incidents highlight the vulnerability of businesses and the critical need for comprehensive cyber insurance coverage:

According to one cybersecurity firm, the top threats in 2023 were[8]:

1. Phishing
2. Infostealers
3. MFA bypass techniques
4. Ransomware
5. Software supply chain attacks
6. Hacktivism-motivated attacks
7. Generative AI risks



Regulatory environment: Governments across the APAC region are implementing stringent data protection laws. For instance, Singapore's Personal Data Protection Act (PDPA) and China's Cybersecurity Law mandate businesses to adopt robust cybersecurity measures and ensure data privacy. Compliance with these regulations often includes having adequate cyber insurance coverage.



Increased awareness and education: Partly as a result of government and regulatory information campaigns, businesses and individuals are becoming more informed about the potential financial impacts of cyber incidents and the importance of having insurance to mitigate these risks.

Market Opportunities

We think there are several particular market opportunities here for cyber insurers, targeting currently under-served segments of the population with new and innovative products.

1. **Private and SME Market:** Personal cyber and SMEs represent a significant untapped market for cyber insurance in APAC, with a need for tailored products that cater to the specific needs and budgets of these customers.
2. **Innovative Products:** There is a growing demand for innovative cyber insurance products that go beyond traditional coverage. Policies that include proactive cyber risk management services, such as cybersecurity assessments and incident response planning, are gaining popularity.
3. **Partnerships and Collaborations:** Collaborations between insurers, cybersecurity firms, and government agencies can enhance the development and adoption of cyber insurance. These partnerships can provide comprehensive solutions that combine insurance coverage with cybersecurity expertise.
4. **InsurTech Advancements:** The rise of InsurTech companies in APAC presents opportunities for innovation in product offerings, distribution channels, and customer engagement. InsurTech solutions can streamline the underwriting process, improve risk assessment, and enhance the customer experience.

Market Challenges

As one of the newer parts of the insurance industry, covering a particularly fast-evolving risk environment, cyber insurance faces particular challenges. Some of these are outlined below:

1. **Lack of standardization:** The cyber insurance market in APAC lacks standardization in terms of policy wording and coverage. This inconsistency makes it challenging for businesses and individuals to compare and choose the right policies.
2. **Underwriting complexity:** Underwriting cyber insurance is complex due to the dynamic nature of cyber risks. Insurers must continuously update their risk assessment models to keep pace with evolving threats, which can be resource intensive.
3. **Limited historical data:** The relatively nascent nature of the cyber insurance market means there is limited historical data on cyber incidents and claims. This lack of data hampers the ability to accurately price policies and predict future losses.
4. **Low penetration rates:** As noted above, despite growing awareness, the penetration rate of cyber insurance in APAC remains relatively low compared to regions like North America and Europe. Many individuals, small and medium-sized enterprises (SMEs), large domestic corporations and government entities are yet to recognise the necessity of cyber insurance.

Reinsurance Options

Reinsurance is crucial in the cyber insurance market as it helps insurers mitigate the financial impact of large-scale cyber incidents, allowing insurers to underwrite larger risks and provide more comprehensive coverage. The current reinsurance market for cyber risks is developing, with leading players actively developing cyber risk solutions to support primary insurers.

Collaboration between insurers and reinsurers is essential to address evolving cyber threats. Gallagher Re is actively involved in many such initiatives. We structured and placed one of the market's first-ever cyber catastrophe bonds for the insurer Beazley in January 2023 and were involved in structuring and placing first retro cyber Industry Loss Warranty for Swiss Re in January 2024.

What about cyber catastrophes?

To date, the world has never experienced a truly catastrophic cyber event, i.e. a loss comparable to some of the largest natural catastrophe events that can pose a risk to insurers' financial stability. Insurance losses from the CrowdStrike outage event of July 2024 have been estimated by various sources as high as USD1.5 billion or as low as USD270 million.

It was arguably the most significant event to impact the cyber insurance market since NotPetya in 2017, a malware attack that caused estimated insurance losses of USD3 billion (of which USD300 million to affirmative Cyber insurance market). Neither event came close to being existential for the cyber market. See our recent paper, *The Risk of a Cyber Catastrophe: Solving for Insurers' Fear of the Unknown*,[9] to find out more.

Nevertheless, the potential for a truly catastrophic cyber event raises questions about the sustainability and pricing of reinsurance in the cyber market. Gallagher Re is undertaking ongoing work to understand the dynamics of some of the "near-miss" large cyber events of recent years, exploring what factors could lead to more substantial or catastrophic losses. See our recent paper, *A History of Near Misses: Utilizing Counterfactual Analysis to Understand Cyber Risk*,[10] to find out more.

Why Gallagher Re?

Gallagher Re's Cyber team is well-positioned to navigate the complexities of APAC's rapidly evolving cyber insurance landscape. We provide comprehensive support on complex cyber transactions and strategic advisory services, leveraging global expertise with a strong local presence. Our capabilities span actuarial and underwriting expertise, product development, accumulation management, regulatory compliance, threat landscape analysis, and advanced cyber risk analytics to assess tail risks and systemic exposures. By partnering with key reinsurers, we deliver innovative reinsurance solutions, enabling clients to grow sustainably while optimizing their programs to meet the region's diverse market needs.

Conclusion: The Outlook for Cyber Insurance in Asia-Pacific

The cyber insurance market in APAC is evolving rapidly, with many variations across the region, as detailed above. Nevertheless, several common themes are likely to hold sway.

Firstly, we are likely to see an increase in the relatively low market penetration rates across the region in the medium term, particularly among Retail and SMEs. To help meet this increased demand for coverage, and make it financially sustainable, insurers will enhance the cyber risk management services they offer to insured clients. This will help businesses and individuals better manage their cyber risks and potentially reduce the frequency and severity of claims.

The rapid advancement of data science and analytical techniques, particularly those making use of artificial intelligence, will help insurers improve their risk assessment, pricing accuracy and claims management functions. For those interested to know more on these topics, an excellent overview is provided by Gallagher Re's 2024 Series of InsurTech Sector Reports,[11] which are focused on AI in insurance.

Finally, as governments in APAC continue to strengthen their cybersecurity regulations, the demand for cyber insurance will rise. Insurers will need to stay abreast of regulatory changes and adapt their products accordingly.

Author:

Sie Liang Lau, FIA
Head of APAC Cyber, Gallagher Re
sieliang_lau@GallagherRe.com

Contributors:

Jennifer Braney
Head of International Cyber, Gallagher Re
jennifer_braney@GallagherRe.com

Ed Pocock
Head of Cyber Security, Gallagher Re
ed_pocock@GallagherRe.com

Dayan Patel
Cyber Security Consultant, Gallagher Re
dayan_patel@GallagherRe.com

Eliana Sessa
Executive Director, EMEA Italy-Med, Gallagher Re
eliana_sessa@GallagherRe.com

Simran Kalsi
Consultancy Assistant — Cyber, Gallagher Re
simran_kalsi@GallagherRe.com

Mark Cobley
Senior Editor, Gallagher Re
mark_cobley@GallagherRe.com

Sources

[1] About the Notifiable Data Breaches scheme, Office of the Australian Information Commissioner, accessed 05 September 2024. See also Notifiable Data Breaches scheme, Association of Market and Social Research Organisations, accessed 09 September 2024

[2] Landmark Amendments to Singapore's Cybersecurity Bill, Crowell, 1 April 2024

[3] Cybersecurity law update – New Thai rules mandating baseline cybersecurity requirements for critical systems, Herbert Smith Freehills, 11 March 2024

[4] Act 854, NACSA, NACSA, 26 August 2024

[5] Data Protection Laws of the World: Vietnam, DLA Piper, accessed 9 September 2024

[6] Indonesia enters era of digital insurance distribution, Insurance Asia, July 2024

[7] Asia-Pacific Digital Transformation Report: Shaping our Digital Future (Figure 2-1, p19), Economic and Social Commission for Asia and the Pacific, 30 August 2022.

[8] Top Asian/APAC Cybersecurity Threats of 2023, CyberInt.com, 27 November 2023

[9] The Risk of a Cyber Catastrophe: Solving for insurers' fear of the unknown, Gallagher Re, October 2023

[10] A History of Near Misses: Utilizing counterfactual analysis to understand cyber risk, Gallagher Re, 15 April 2024

[11] Gallagher Re News & Insights: InsurTech, Gallagher Re, accessed September 2024

Learn more about our client-focused, collaborative approach.

Connect with us today at **GallagherRe.com**.

It's the *way* we do it.

Gallagher Re