PUBLISHED AUGUST 2025

An Overview of the Global Cyber (Re)Insurance Market

CYBER RISK TOOLKIT

American Academy of Actuaries
Cyber Risk Task Force, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Cyber Risk Task Force, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the task force.

The American Academy of Actuaries is a 20,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. For 60 years, the Academy has assisted public policy makers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

An Overview of the Global Cyber (Re)Insurance Market

Published August 2025

Introduction & Scope

Since the introduction of the first cyber insurance policies in the late 1990s, the global cyber insurance market has grown and evolved into one of the fastest-growing property and casualty (P&C) lines. The global cyber insurance market is rapidly evolving and varies by geography. It is broadly considered to be established, but not yet mature. While policy wording and coverages are standardized in some regions, they are less so in others. The United States (U.S.) and the United Kingdom (U.K.) markets have been actively shaping the future of the industry for more than two decades, while newer markets in the rest of the world vary in degree of maturity.

The purpose of this paper is to provide a high-level overview of the global cyber insurance market, highlighting differences and similarities between regions and commenting on relevant history that shaped each region's experience to date.

No part of this paper is meant as an original forward-looking projection or a guarantee of future performance in any market. Where cited, projections from third-party sources are included for contextual understanding. Any discrepancies in the quality or relevance of the information in this paper between regions are due to the availability of public information and not reflective of the relative importance or market size of those regions.

Size of the Market

Figure 1.

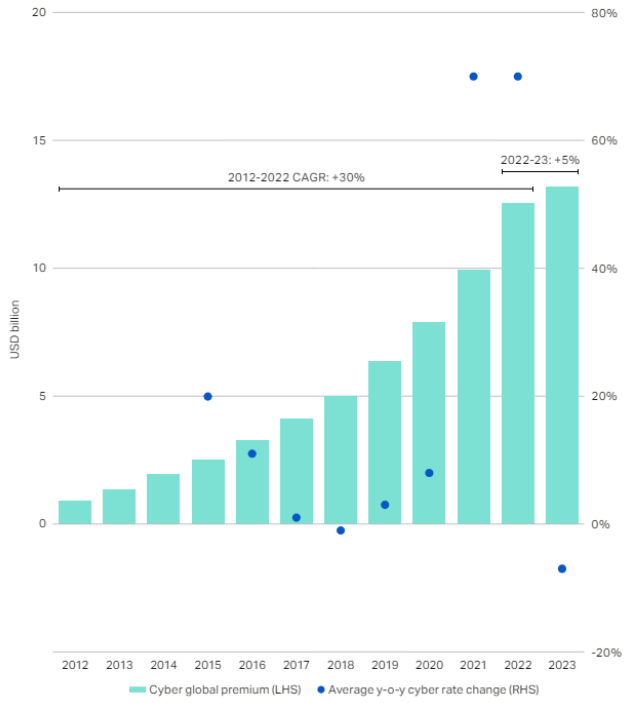


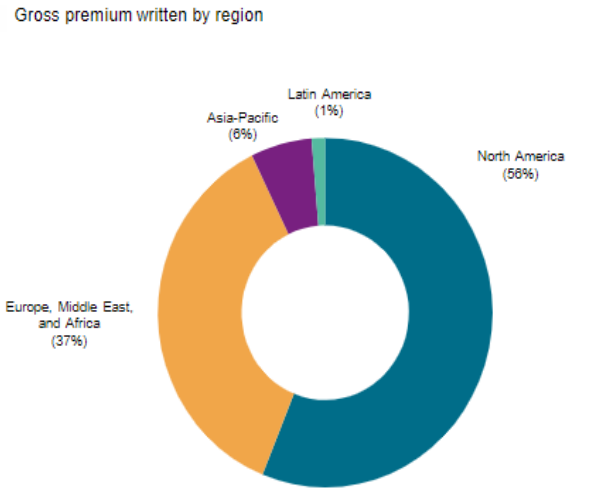
Figure 1. (Howden Re) Globally, cyber insurance gross written premium volumes increased at an annualized rate of 30% from 2012 to 2023, far outpacing the general P&C market, which is estimated to have grown at an annualized rate in the mid-single digits over the same time. Historical growth of cyber insurance was driven by digitalization, high profile attacks, and regulatory responses including data breach notification laws. Exposure and premium rates have both contributed to the growth: rate increases were in the high double digits from the second half of 2020 through 2022 before steeply declining to single digit negatives in 2023-2024. At the same time, insurers updated policy language to clarify coverage, and took action to increase self insured retentions (SIRs).[1, 2]

After nearly a decade of high growth, the global cyber insurance market is estimated at a size of approximately $15B USD in 2024, with some projections indicating growth to almost $30B by 2027[1] and upwards of $40B by 2030.[2]

1 "Global Cyber insurance market trends 2024"; Medium; April 12, 2024.
2 Cyber Insurance: risk, resilience and relevance; Howden Group; June 2024.

Geographies

Figure 2. The largest share of cyber insurance premium still stems from North America.



Data is based on our cyber insurance survey for global multiline insurers and global reinsurance groups. Source: S&P Global Ratings.

Figure 2. North America has historically been, and still is, responsible for the largest share of global cyber insurance premium. In 2023, it is estimated that North American cyber premiums were 56% of the global total, followed by EMEA (Europe, Middle East, and Africa) with 37%, APAC (Asia-Pacific) with 6%, and LATAM (Latin America) with 1%.[3] Nearly half of the growth through 2030 is expected to originate from the U.S., while the remainder is expected to be driven by continental Europe, the U.K. and APAC including Oceania, in that order.[2] More detailed commentary by geography appears at the end of this paper.

Reinsurance, Retrocession & Alternative Risk Transfer

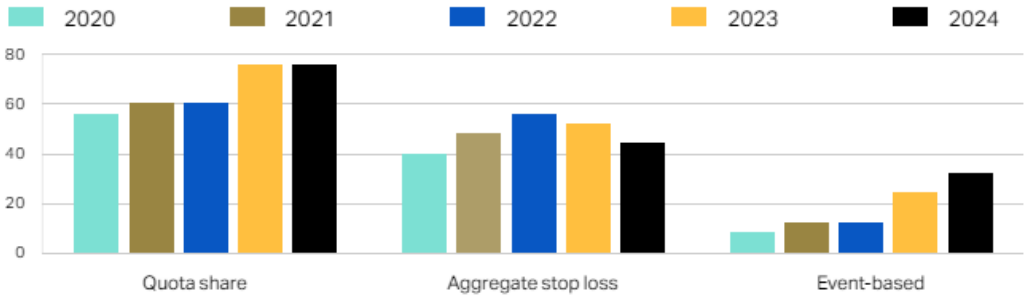
Reinsurance and retrocession capacity are expected to be key supporting players in the continued growth of the global cyber insurance market.[3] Though the reinsurance market is vital to continued growth, overall cessions to reinsurers are decreasing as primary carriers become more comfortable with their cyber exposure. The reduction in cessions is not unusual and could change after a significant loss event. In 2022, some 50%-65% of primary cyber insurance premiums were ceded[3] but more recent estimates indicate that markets are on average ceding only 35% of their primary cyber premium.[4] Cessions vary materially by geography, with less mature regions such as LATAM and APAC ceding more than established regions like the U.S. The decreasing trend in overall cession means that the cyber reinsurance market is projected to grow at a slower rate than the primary market.[3]

3 "Global Cyber Insurance: Reinsurance Remains Key to Growth"; S&P Global Ratings; Aug. 29, 2023.
4 Reframing cyber risk: Navigating threats and embracing opportunities; Howden Re; May 2024.

In 2022, quota share treaties made up about 87% of all reinsurance, while excess of loss, stop loss, and other non-proportional treaties made up most of the remaining 13%.[3] For 1/1/2024 renewals, quota shares were still the most popular form of cyber reinsurance cover, though cedants began to explore more excess of loss treaties and event-based cover, where previously stop loss cover was the preferred non-proportional strategy.[3, 5] Most cyber quota share treaties have loss ratio caps in the range of 300%-350% with a select few exceeding 400%.[5]

Figure 3. The figure below from Howden Re illustrates the shift in non-proportional treaty purchases from 2020 to 2024 and the increase in overall quota share purchase.[4]

Figure 3. Percentage of insurers purchasing cyber treaty structures (2020-2024)



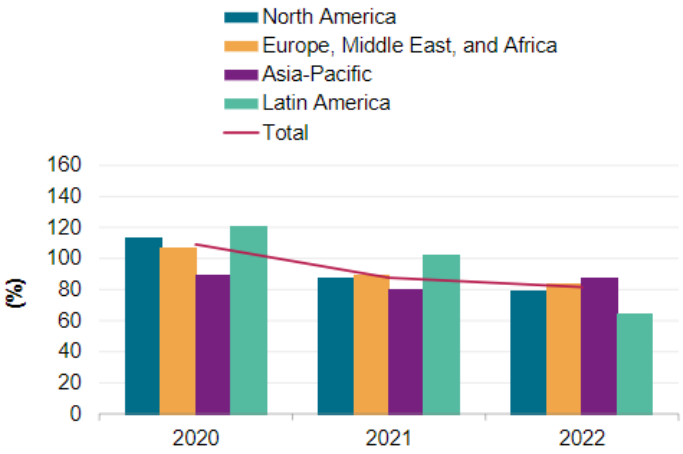
Retrocession will also be important to future market growth. The capacity to date has been relatively limited due to capacity providers' concerns about overall accumulation and due to information-sharing concerns; retrocession capacity is often provided by competitors in the reinsurance space.[6]

The first alternative risk transfer for cyber emerged in 2023 with the issuance of cat bonds to Beazley, Chubb, AXIS Capital, and Swiss Re.[7] In 2024, Swiss Re purchased the market's first cyber retrocession industry loss warranty (ILW), which provides $50M USD catastrophic U.S. cyber event protection against widespread malicious malware or ransomware, prolonged catastrophic cloud outage, and systemic data breach.[8]

5 "Panel: Cyber reinsurers more bullish because of market's scale and maturity"; Cyber Risk Insurer; Feb. 29, 2024.
6 "Cyber reinsurance, retro & ILS all critical to market expansion: S&P"; Artemis; Jan. 16, 2024.
7 Catastrophe Bond & Insurance-Linked Securities Deal Directory; Artemis.
8 "Swiss Re Purchases Cyber Market's First Retrocession ILW"; Reinsurance News; Jan. 16, 2024.

Performance

Figure 4. Gross combined ratio, Primary insurance segment

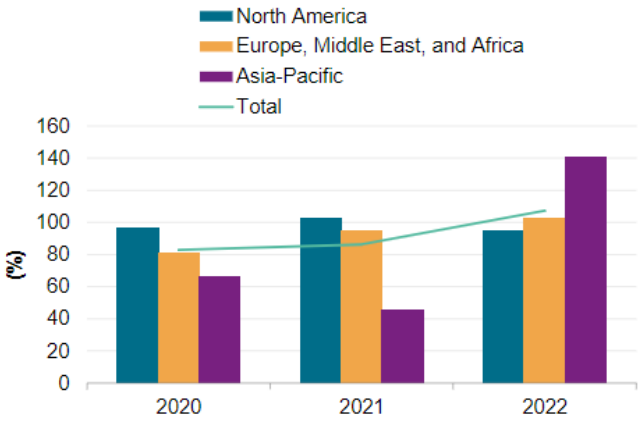


Data is based on our cyber insurance survey for global multiline insurers and global reinsurance groups. Source: S&P Global Ratings.

Figure 4. Primary cyber insurance gross combined ratios decreased from 2020 to 2022 while reinsurance combined ratios increased on average.

North America and EMEA results are broadly aligned for all three years, while there is more variance in the Asia-Pacific and Latin America results. This is not unexpected because of the relatively small size of the Asia-Pacific and Latin American markets.[3]

Figure 5. Gross combined ratio, Reinsurance segment



Data is based on our cyber insurance survey for global multiline insurers and global reinsurance groups. Source: S&P Global Ratings.

Figure 5. Contrary to the primary market experience, reinsurance combined ratios were on the rise from 2020 to 2022. The year 2022 was a difficult one for global cyber reinsurers, with a total gross combined ratio of 107% and net combined ratio of 101%. These results were worse than primary insurance combined ratios, which were well under 100% for 2022.[3]

Recent estimates indicate that primary insurers are ceding more of their cyber exposure than premium by transferring more cyber-CAT potential to reinsurers, through non-proportional reinsurance structures, such as aggregate stop loss, per-risk or per-event excess of loss treaties.[4]

Products & Coverages

Cyber products and coverages are beginning to standardize but still differ by geography. Major coverage differences are related to ransomware payment and business interruption exclusions. For instance, in Canada, it is more likely that ransomware payments are excluded on a cyber insurance policy than in the U.S. or the U.K. Germany cyber insurance policies are more likely to exclude business interruption coverage.[9] The Japanese cyber insurance market is estimated to be the largest in the APAC region, but unlike coverage in North America and Europe, business interruption is not often covered.[10] In Japan, small damages for distress caused by unauthorized disclosure of personal information are often covered and referred to as "apology money".[11] Payment of ransoms is not currently prohibited by the Japanese government, but cyber policies in Japan do not typically cover ransom payments.[12] These differences in coverage may be due to regional laws, maturity of the local market, local cyber-attack experiences, buyer price sensitivity, and perceived exposure variances.

Adoption Rates, SMEs

Cyber insurance adoption rates vary by geography, industry, and business size. Within these classes, mix of standalone cyber policies versus cyber purchased as an add-on or endorsement to a professional liability, Errors and Omissions (E&O) or Business Owners (BOP) policy varies. The U.S. has one of the highest adoption rates and the U.K. has a higher standalone cyber adoption rate than central European countries.[13] It is expected that adoption rates will increase in central Europe in the near future.[14] Amongst industry, across the world, education, governmental entities, financial services, and energy sectors have the highest adoption rates.[13]

SMEs (less than $250M USD in revenues) have consistently lower cyber insurance adoption rates globally than their larger corporate counterparts. In 2023, it is estimated that only one in four SME businesses worldwide had some form of cyber insurance, compared to 75%+ of larger businesses, though SME business accounts for a material share of the world economy/GDP.[2] While SME adoption rates for cyber insurance do appear to be ticking up in recent years, many brokers and industry leaders have called for actions to more rapidly increase adoption in this segment such as increasing awareness and simplifying the buying process.[2]

9 The Global State of Cyber Insurance; Arctic Wolf; March 2024.
10 "Reinsurance in Japan: Ensuring continuity in an evolving risk environment"; Swiss Re; Aug. 23, 2024.
11 Security CyberProtector Service; GMO Payment Gateway.
12 Cybersecurity Laws and Regulations in Japan 2025; ICLG.
13 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption; Sophos; May 2023.
14 "A Brief History of Cyberinsurance"; Slate; Aug. 30, 2022.

Regional Commentary

North America—U.S.

The first cyber insurance product in the U.S. emerged in 1996/1997 when AIG launched its Internet Security Liability (ISL) product. The ISL standard plan covered legal costs and settlement fees if customer credit cards were stolen from insured companies' servers and the credit card company failed to protect them. Throughout the late 1990s and early 2000s, other carriers followed suit and began offering what was referred to as "Security & Privacy" coverage as an add-on to other commercial liability products. These add-ons generally had low sublimits and narrow coverage, often only first party coverage.[14]

States began adopting data breach notification laws in the early 2000s, beginning with California. Today, all states have an active data breach notification regulation.[15, 16] As breach notification legislation was being developed and enacted across the country from the early 2000s to mid-2010s, cyber insurance carriers adapted to expand coverage and Insurance Services Office (ISO) amended the Commercial General Liability (CGL) form to exclude computer data from their definition of tangible property.[17] New coverages included IT forensics, public relations, credit monitoring, customer notification costs, third-party regulatory defense, and fines and penalties.[16]

Breach notification laws and tightening of other commercial policy language to exclude breach response costs for a security incident led to increased demand for and take-up of standalone commercial cyber coverage. By 2014, the US cyber insurance market was estimated to be over $1B in gross written premium.[18] The 2015 estimates of the global cyber insurance market indicate that the United States comprised about 90% of the global cyber insurance premium at the time.[19] High-profile breaches of the mid-2010s in the U.S. included retailers such as Target and P.F. Chang's, health care providers with Blue Cross, and the 2017 Equifax data breach; these breaches made headlines and fed the increasing demand for cyber insurance in the U.S. The mid-to-late 2010s was also a pivotal moment for ransomware as attacks became more targeted.[20] From 2018 to 2020, the average ransom payment grew from about $6,000 to nearly $250,000 as victim size increased and cyber criminals demanded higher ransoms. The U.S. is currently the country most affected by ransomware attacks on organizations.[21] While U.S. public policymakers have discussed banning the payment of ransoms, no such legislation is in place currently; the White

15 Data Breach Notification Laws by State; IT Governance.
16 "The History of Cyber Insurance"; ProWriters.
17 "An Abbreviated History of Cyber Insurance—The First 25 Years"; Koru Risk Management.
18 "Historical Development of Cyber (Re)insurance"; Guy Carpenter.
19 Global Cyber Market Overview: Uncovering the Hidden Opportunities; Aon; June 2017.
20 *Behind the rise of ransomware*; Atlantic Council; Aug. 2; 2022.
21 The Latest 2025 Ransomware Statistics; AAG; June 2025.

House "strongly discourages paying of ransoms, to stop the flow of funds to these criminals and disincentivize their attacks."[22] Driven largely by the increase in frequency and severity of ransomware attacks, the U.S. saw very high levels of premium rate increases on cyber insurance from the end of 2020 through 2022, in some cases upwards of 100%.[21]

North America—Canada

Canada is a fast-growing market for cyber insurance. 2023 premium estimates for the Canadian cyber market approach $500M Canadian Dollars (CAD) (approximately 6.4% of the global cyber premium income[23]), up from under $25M CAD in 2015.[24] Canada experienced increases in ransomware frequency and severity that mirrored the United States' experience,[25] which contributed to poor loss experience in 2019– 2021, driving rate increases, and tightening underwriting standards like those in the U.S. The Canadian breach notification laws that are in place today were not passed until 2018.[26] This delay compared to the U.S. may help explain the lag in popularity of cyber insurance in Canada.

Lloyd's has dominated the Canadian market share since 2015 when it had a 45% share. It continues to do so with 77% of the market share in 2022 Q4[25], though 18 new carriers entered the Canadian cyber insurance market between 2015 and 2022. As of 2022, it was estimated that 74% of Canadian organizations had cyber insurance, and 36% of those with cyber insurance had a standalone cyber policy.[24] A recent Canadian Underwriter survey revealed that clients were most likely to turn down cyber coverage due to price, with 40% of broker respondents giving "price too high" as the main reason for clients declining coverage.[27]

EMEA—the U.K. & Continental Europe

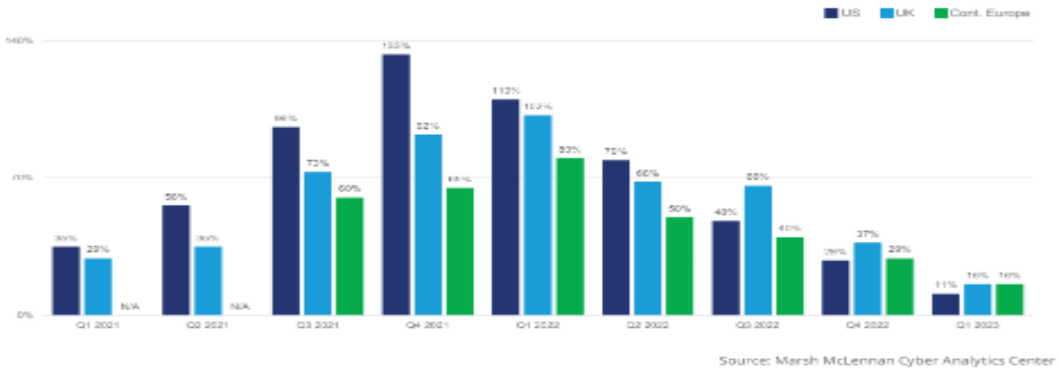
The first cyber policy issued through Lloyd's was written in 1999 and provided both first- and third-party coverage. It is estimated that 25 to 30 cyber markets existed in London as of 2013-2014.[28] Today, Lloyd's remains a world-leading provider of cyber insurance. The Lloyd's Market Association (LMA) led the global market in adding war exclusionary language to cyber insurance policies in 2023 with LMA mandate Y5381.[29]

22 "Ransomware payment debate resurfaces amid Change Healthcare Incident"; Nextgov; March 18, 2024.
23 Through the Looking Glass: Interrogating the key numbers behind today's cyber market; Guy Carpenter; 2023.
24 The Canadian Cyber Insurance Market 2024; Insurance Bureau of Canada; 2024.
25 "The growing challenges & trends in the cyber liability insurance market"; Westland Insurance; Oct. 19, 2023.
26 "Mandatory privacy breach reporting requirements coming into force in Canada November 1"; Norton Rose Fulbright; April 2018.
27 "Pricing still affects brokers' ability to sell cyber"; Canadian Underwriter; April 10, 2024.
28 "Historical Development of Cyber (Re)insurance"; Guy Carpenter.
29 Through the Looking Glass: Interrogating the key numbers behind today's cyber market; Guy Carpenter; 2023.

Growth rates for cyber in the U.K. and European markets has escalated in recent years, outpacing the growth rate in the U.S. and leading (re)insurers to target growth in the region.

Figure 6. Rate changes in the U.K. and continental Europe have lagged those in the U.S., illustrated in the graphic below from a 2023 Marsh report which shows quarterly rate changes by region.[30]

Figure 6.



Source: Marsh McLennan Cyber Analytics Center

Germany and France are estimated to have 6.1% and 2.1% respectively of the global cyber premium income as of 2023, making them the two largest contributors in continental Europe.[30] Research conducted on the German cyber insurance market indicates that policy language is not standardized and coverage differs from the U.S. market, namely physical damage is not as commonly excluded in Germany as in the U.S., and ransomware payments are more commonly excluded in Germany compared to the U.S. Further, there is increased focus on business interruption coverage in Germany, which the researchers attribute to the industrial nature of the German economy.[31] Similarly, there are government restrictions on ransomware payments in France. Until April 2023, French law did not allow for the payment of ransoms; the current law requires a complaint filing to be made within 72 hours of the ransom demand for insurance compensation for the ransom demand to be allowable.[32]

30 Ibid.
31 Bridging the cyber protection gap: An investigation into the efficacy of the German cyber insurance market; Risk Management and Insurance Review; March 8, 2024.
32 "French Law Authorizes Insurability of 'Cyberransoms' Paid by Victims, Subject to Prompt Filing of Complaint"; Jones Day; Feb. 24, 2023.

Middle East and Africa

The Middle East and Africa are estimated to have a cyber insurance market size of approximately $283M USD in 2024, accounting for less than 2% of the global market.[33]

Cyber rates decreased by an average of 6% in the first quarter of 2024, generally driven by low claims activity and new capacity entering the market. This was especially true in the Middle East, where new market entrants increased competition. In South Africa, ransomware restrictions have begun to be lifted for specific risks, though local capacity remains limited.[34]

While security maturity in the region has generally been less advanced than other regions, geopolitical tensions and a rise in cyber incidents across the Middle East and Africa drove an uptick in security maturity in 2022. Insurers and regulators also helped drive improvements.[35]

APAC—Summary

A high rate of digitalization between 2000 and the early 2020s left the region more vulnerable to cyber-attacks.[36] The APAC region is expected to achieve the highest compound annual cyber insurance growth rate of any region from 2023 to 2028 as increased regulatory scrutiny and recent attacks drive demand for cyber insurance coverage. [37]

Cyber risk broke into the top five risks for business leaders in APAC for the first time in 2021 and topped the list of most critical future risk topics over the next five years. Three main drivers of cyber risk in the APAC region are geopolitical tensions, digital supply chain vulnerabilities, and exfiltration of intellectual property from strategic suppliers according to research conducted by Aon. [38]

APAC—Australia

Cyber insurance first emerged in Australia circa 2013. At that time, only a handful of policies were written but by 2018, the market is thought to have been on the order of $60M Australian Dollars (AUS).[39] As of 2022, the Australian cyber insurance market was approximately $200M USD in size.[40] An estimated 20% of Australian SMEs and 35% to 70% of larger Australian business have standalone cyber insurance.[41] Like other regions,

33 Middle East Cyber Insurance Market Report 2025; Cognitive Market Research; May 2025.
34 IMEA Insurance Market Rates Q1 2024; Marsh; March 2024.
35 "EMEA: Building Resilience to Navigate Rising Cyber Risk"; Aon; Aug. 21, 2023.
36 A primer on cyber insurance and the use of models; PeakRe; April 19, 2023.
37 "Cyber insurance market set to surge"; Insurance Business; Aug. 19, 2023.
38 "APAC: Regulators and Companies Respond as Ransomware and Reputation Risks Intensify"; Aon; Aug. 18, 2023.
39 "Cyber Insurance Market Insights—Q3 2018"; Aon Insights Australia; 2018.
40 "New research finds gaps in Australian cyber insurance"; Australian Institute of Company Directors; Oct. 31, 2022.
41 "Cyber risk"; Insurance Council of Australia.

the Australian cyber market is becoming more competitive as loss ratios and profitability improve along with new capital and increased capacity enter the market. Rate increases in the first half of 2023 reduced to +10%-15%, down from +30%-40% in 2022.[42]

The Australian Reinsurance Pool Corporation manages Australia's terrorism and cyclone pool, which currently excludes cyber terrorism. It is anticipated by some industry observers that Australia will wait to see what the U.S. Treasury proposes regarding a federal backstop for catastrophic cyber events. Like the U.S., the Australian government does not condone ransom payments but does not ban victims from paying ransom demands.[43]

APAC—Japan

The Japanese cyber insurance market is estimated to be the largest in the APAC region with 2022 written premium estimates around $200M USD. Adoption is thought to be low compared to North America and Europe. Standalone cyber coverages also differ as business interruption is not commonly provided, and ransom payments are not usually covered.[44]

APAC—China

The Chinese cyber insurance market was estimated to be $30M USD in 2022. A recent increase in interest for standalone cyber insurance is thought to be driven by upticks in ransomware and extortion as well as regulators encouraging the purchase of cyber insurance through industry associations.[44]

APAC—India

As of 2022, it was estimated that the market consisted of approximately 1,000 standalone cyber policies and $30M USD in written premium. Take-up rates are on the rise following high-profile breaches but skewed toward large corporate risks while most SMEs do not have coverage. IT companies, banks, and manufacturers are the top buyers of cyber insurance in India.[44]

APAC—Other

The Southeast Asian market is still nascent, and the premium volume is believed to be very small as of 2022. Cyber coverage is mostly offered as an add-on to commercial package policies, though some companies with U.S. business operations have purchased standalone cyber coverage.[44]

42 Mid-Year Insurance Market Update 2023: Australia; Marsh; 2023.
43 "Cyber insurance trends to look out for in 2024 and beyond"; Landers and Rodgers; March 2024.
44 "A primer on cyber insurance and the use of models"; PeakRe; April 19, 2023.

LATAM

LATAM is one of the fastest growing cyber insurance markets globally.[2] There has been an increased focus on the region recently, with NetDiligence dedicating an entire day of its February 2024 Cyber Summit to Latin America.[45] Cyber attacks are known to be a growing problem in the region. General investment in cybersecurity and awareness is on the rise, as is cyber insurance uptake.[46] However, this market is still in its infancy compared to other global regions, and there is room for education and further market growth.

LATAM has historically had inconsistent progress in addressing cyber risk. Data show that LATAM companies lag their U.S. peers in some critical areas, such as third-party management, business resilience, and application security.[1] Data protection efforts in LATAM vary by country. Some countries such as Argentina and Brazil have active data protection legislation and regulation in place. Others, like Chile, have no data protection regulator and only some regulated markets, e.g. financial institutions, are required to notify authorities of a data breach.[47]

Conclusion

The global cyber insurance market is one of the fastest-growing P&C lines today. Though North America and Europe comprise most of the market today, other regions like APAC and LATAM are growing rapidly. As cyber insurance carriers expand into new regions, there may be increased standardization of cyber policy wording worldwide. Reinsurance and retrocession will play a key role in allowing carriers to continue expanding their reach in new geographies.

45 "Cyber Risk Summit Miami 2024 – Agenda"; NetDiligence; 2024.
46 "Securing Tomorrow: Why Latin America should top Global Cyber Insurers' Lists"; Lexology; Dec. 6, 2023.
47 "Latin America: Three Crucial At-Risk Control Areas"; Aon; Aug. 16, 2023.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**