Cyber

2025 Cyber Insurance Market Conditions Outlook:

Cyber Market Stabilization as Cyber Risks Evolve

By: John Farley, Managing Director, Cyber

Gallagher

Insurance | Risk Management | Consulting

Introduction

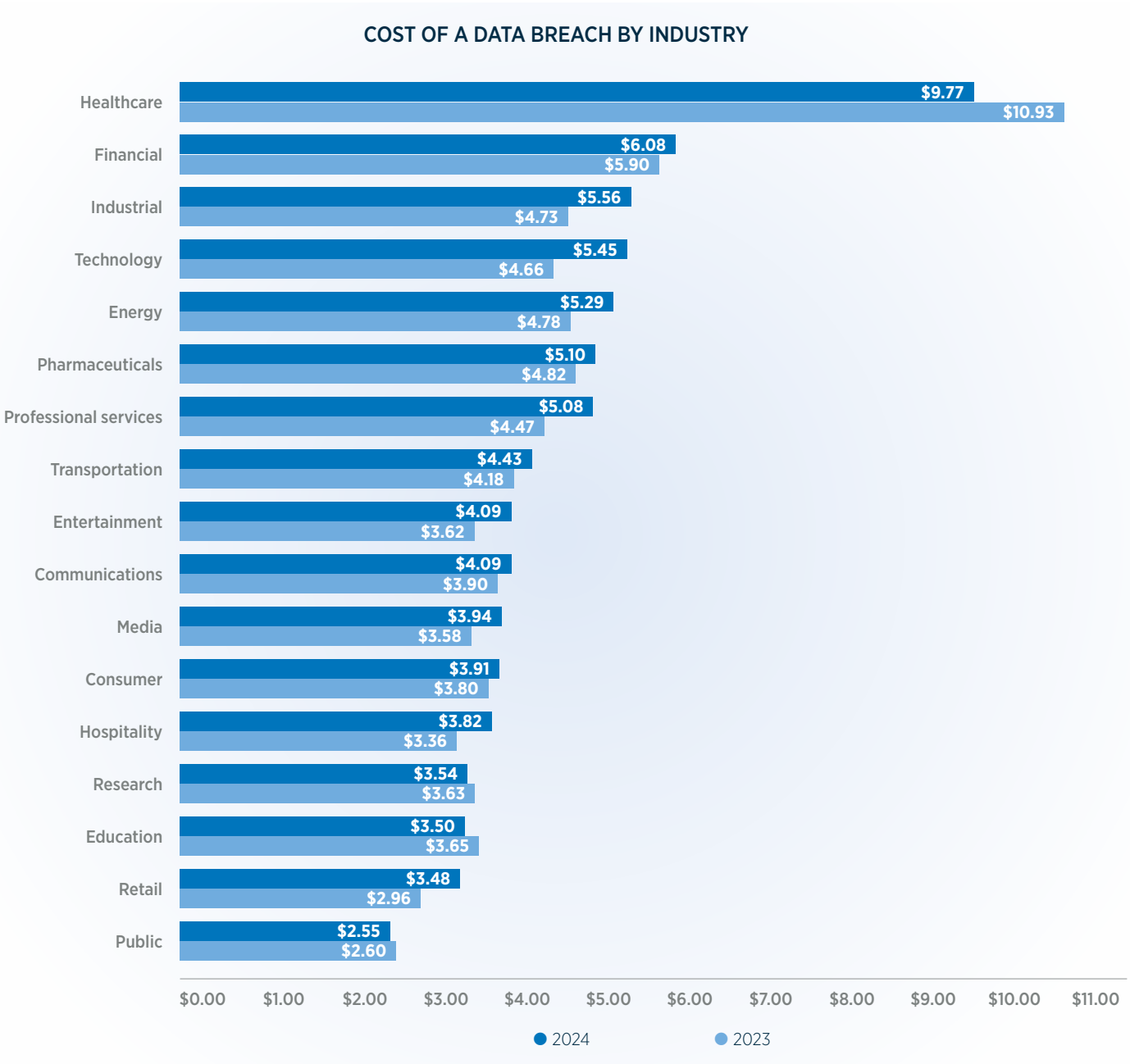
As we look ahead to 2025, the hallmarks of a stabilized cyber insurance market continue as the softening conditions that took hold in 2024 will likely carry over into next year. Intense competition among cyber insurance carriers has provided a buyer-friendly environment with ample capacity, higher limits, enhanced cyber risk management services, and some flexibility in insurance applications. Rates remain near flat and in some cases are falling slightly further.

However, 2024 did bring challenges. Organizations faced continuing cyber losses from ransomware and social engineering attacks that have persisted over the past several years. It also became clear that the growing supply chain attack vector is becoming a favored strategy of threat actors and will be a significant cause for concern moving forward. While the cascading losses from these attacks have not negatively impacted the market in a meaningful way, we do hear a rising chorus of concerns from the underwriting community. Moreover, losses stemming from wrongful data collection claims also started to mature last year, as these long-tail claims led to a second and notable issue for cyber insurance carriers. Finally, the underwriting community has a watchful eye focused on the potential for future losses related to generative artificial intelligence, both from increased threat actor capabilities and from a regulatory compliance perspective.

So, while we have reached a period of relative calm, the market is juxtaposed with gathering storm clouds around a variety of current and emerging cyber claims concerns. This will certainly test the wherewithal of the cyber insurance market in the coming year.

CYBER CLAIMS TRENDS AND THE CURRENT THREAT LANDSCAPE

Today's cyber claims trends reflect the ever-evolving and persistent nature of a wide variety of cyber threats. These were highlighted in several reports published over the past year. In July 2024 the IBM-Ponemon Cost of a Data Breach study revealed that the average cost of a data breach reached an all-time high of $4.88 million. This represents a 10% increase from the prior year and the highest increase since the pandemic.[1]



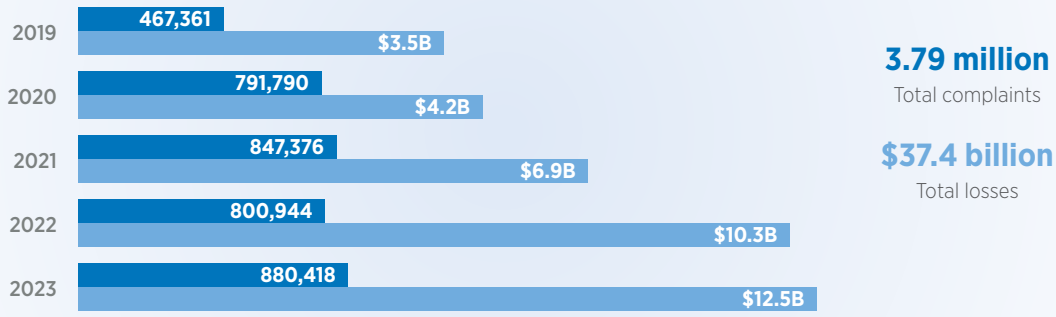
The ransomware ecosystem continues to evolve with the new variants and rebranded criminal groups. They continue to target a wide variety of industry sectors with common tactics involving data exfiltration and threats to expose sensitive information if extortion payments are not made. However, the 2024 ransomware statistics do reveal a glimmer of good news for those that are attacked, including:

- Initial ransom demands have been declining since the beginning of 2023.[2]
- Average ransomware payment decreased from $568,705 in 2023 to $381,980 in 2024.[3]
- The trend of fewer organizations paying ransoms also continued, with one study showing ransom only being paid in 34% of ransomware attacks.[4]

The FBI's Internet Crime Report,[5] published in March of 2024, revealed several emerging cybercrime trends, including but not limited to:

- **Investment scams** were the leading type of attack in 2023. Investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase. Schemes promising investment returns related to cryptocurrency lead the way in this category.
- **Ransomware** increased in 2023 after a brief decrease in 2022. Reported losses rose 74%, from $34.3 million to $59.6 million. Cybercriminals are now using multiple ransomware variants against the same victim. They continue to use threats to expose or to destroy data to add pressure on victims during negotiations.
- **Business email compromise** continued to be a favored tactic of threat actors. In 2023, the FBI received 21,489 BEC complaints with losses amounting to over $2.9 billion.

COMPLAINTS AND LOSSES OVER THE LAST FIVE YEARS



3.79 million
Total complaints

$37.4 billion
Total losses

Several high-profile supply chain attacks occurred last year, with the most impactful affecting those in the healthcare, automotive, and transportation sectors. Threat actors continue to focus attacks on key supply chain providers and will likely impact additional industry sectors. In addition, a recent network outage of a key cybersecurity provider led to significant disruption, highlighting the fact that cyber losses can emanate from a system outage and are not always the result of a targeted attack.

Non-breach privacy claims have become a top concern as these losses started to mature in 2024. Claims based on wrongful data collection, particularly those related to website tracking technology and biometric data, are coming to bear. Allegations are based on a variety of state laws, many of which allow for private rights of action.

Another factor that could exacerbate cyber claims frequency and severity involves heightened regulatory risk. Publicly traded companies are now officially mandated to report "material" cyber incidents to the Securities and Exchange Commission within 4 business days and are required to provide annual reports to detail efforts made around cyber risk management. While our focus is on the regulators at the state and federal level in the United States, we fully expect regulatory risk to continue to extend to international territories and be influenced by other global privacy regimes in 2025.

THE US FEDERAL GOVERNMENT RESPONSE

In March of 2024, the Cybersecurity and Infrastructure Security Agency (CISA) announced their proposed rules for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).[6] The CIRCIA legislation is part of the federal government's continuing focus on enhancing the cybersecurity of critical infrastructure sectors and improving incident reporting to relevant government agencies. Failure to comply with CIRCIA reporting requirements may result in penalties, including fines and potential legal consequences. While the proposed rules aren't expected to be finalized until at least mid-2025, it is important for affected organizations to be familiar with the key aspects of the CIRCIA reporting requirements.

CYBER INSURANCE PRODUCTS RESPOND TO CHANGING THREAT LANDSCAPES

Despite the 2024 cyber loss trends evolving to reflect risks in the supply chain and regulatory landscape around data collection and privacy liability claims, softening conditions remain. Abundant capacity and fierce competition will keep rates relatively low, at least for the short-term. However, there is little sign that the frequency of these losses will slow. Moreover, the potential risks posed by the rapid adoption of generative artificial intelligence will likely be serious considerations for cyber underwriters this year. As a result, the cyber insurance providers now find themselves in a position to provide cutting-edge products that stand apart from the competition while protecting their balance sheets, maintaining market share and profitability. To do this, we are seeing signs that products are evolving. There are several developments in policy wordings that bear watching:

- **Supply chain, war, and systemic risk:** The underwriting community has focused on managing the potential for cascading losses that have manifest, in part, via several supply chain attacks in 2024 and the looming threats of conflict between countries that have significant cyber threat capabilities. On the other hand, the fears around geopolitical conflict have yet to materialize in meaningful losses. Regardless, we note significant cyber insurance policy wordings around these potential exposures. Underwriters are maintaining the widened application of war exclusions, imposing sub-limits for systemic events, and in some cases mandating that their insureds have written contracts with their supply chain vendors to trigger coverage in a supply chain attack scenario. In essence, we see a focus on the extent to which carriers want to provide coverage for those impacted by the cascading effects of an attack on another party, and policy wording varies from carrier to carrier. Finally, non-malicious losses due to system failure have become more of a concern. In a system outage scenario we recommend insureds pay attention to wording around time element coverage wording, including "waiting period," "qualifying period," and "period of interruption." These terms, and the way they are specifically defined, can significantly impact recovery for costs related to business interruption and extra expenses.

- **Regulatory coverage:** The extent to which cyber insurance policies cover regulatory risk has generally become more restrictive, and we see that trend continuing. Underwriting concerns around increasing claims costs generated by a wide-ranging number of regulatory bodies have led to coverage constriction around costs for regulatory investigations, settlements, fines, and penalties. However, we did note that many insurance carriers are affirmatively covering incurred costs to notify regulators of material incidents per the new SEC reporting requirements.
- **"Non-breach" claims and wrongful data collection:** As state, federal, and international privacy law has expanded in scope and complexity, so too has the exclusionary wording in cyber policies. We are paying particular attention to exclusions to website tracking claims and those that exclude claims stemming from specific privacy laws. Terms such as "unauthorized" vs "wrongful" or "unlawful" or "in violation of law" may be the difference between a loss being covered or not. Therefore, we are advising our clients to exercise caution when reviewing this policy language, which may be murky or even appear to be contradictory.
- **Artificial Intelligence-based loss coverage:** The rapid mass adoption of generative artificial intelligence tools will continue throughout 2025, and underwriters are beginning to take note. There is preliminary evidence of claims activity around losses manifesting from the use of AI platforms. In fact, as of this writing, there are over 200 actively litigated cases related to artificial intelligence and machine learning.[7] These include, but are not limited to, data bias, liability for intellectual property and trademark infringement, privacy liability, and regulatory risk. We see the potential exposure of multiple lines of coverage beyond cyber insurance, which may include employment practices liability, product liability, errors and omissions, medical malpractice, and others. While we have not seen absolute clarity on where AI-driven perils may be covered or excluded, we do see evidence of the cyber markets beginning to evolve to reflect these new exposures. At least one cyber carrier is offering a stand-alone AI policy, and others are starting to issue endorsements. Coverage for AI providers, including costs to retrain learning models due to "data poisoning," is one such example. In 2025, we fully expect many more markets to offer AI-loss coverage in some form for both AI platform providers and those that use them.

REINSURANCE: A MAIN PLAYER TO DRIVING GROWTH IN 2025

Reinsurance continues to play a key role in the overall growth and sustainability of the cyber insurance market, providing new capacity with growing support from the capital markets. We are seeing a variety of ways this is being accomplished in the cyber reinsurance market, including:

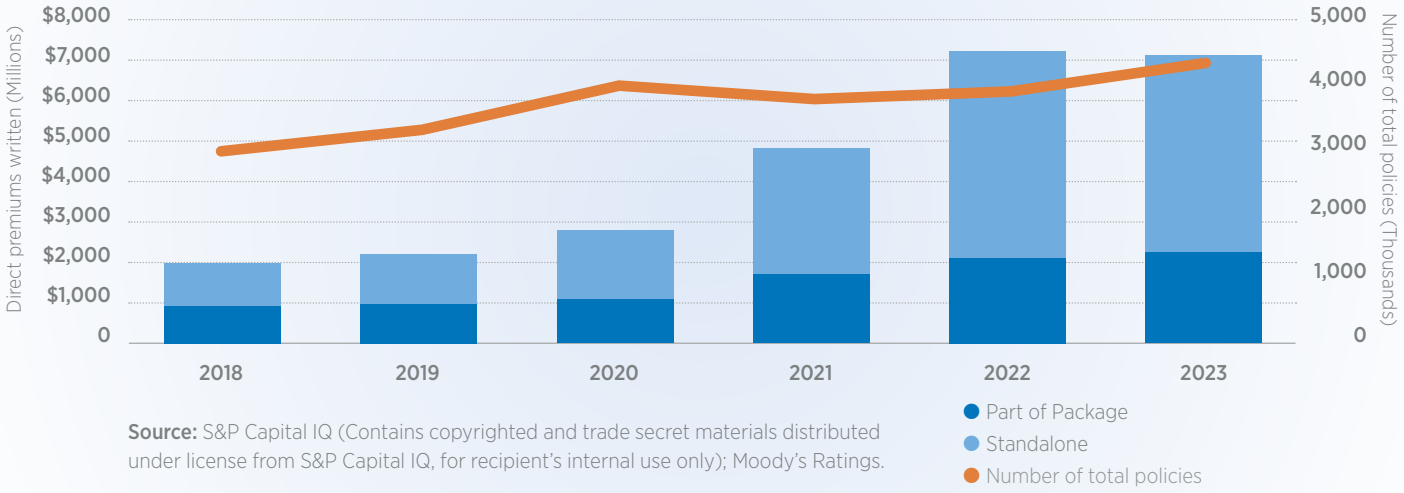
Insurance-Linked Securities (ILS)	Proportional Reinsurance Transactions	Catastrophic Bonds (Cat Bonds)
This allows for the cyber insurance carriers to transfer a portion of their cyber risk exposure to the capital markets.	Similar to ILS, this helps spread cyber risk from one cyber insurer to multiple parties in the capital markets.	These bonds are specifically designed to trigger payouts, backed by capital markets, after an extreme cyber event.

Primary insurers are also beginning to formalize the way they feed critical data to their cedents that serve to improve existing loss modeling tools. They are creating platforms that provide reinsurers with more detailed information from loss history, critical vulnerabilities, key security controls, and cyber risk service providers. We see the reinsurance market continuing to grow in 2025 and expect even more innovation around risk transfer solutions for both non-proportional and event-driven coverage.

LOOKING AHEAD — CYBER MARKET GROWTH PROSPECTS

Despite today's softening market conditions, we foresee a cyber insurance market that is poised for significant growth over both the near and far term. Policy forms will undoubtedly evolve along with emerging technology and a dynamic threat landscape. According to one study,[8] the global cyber insurance market saw premiums more than double over the past 5 years, reaching approximately $14 billion in 2023. Projections predict the market to reach $29 billion in premiums by 2027.

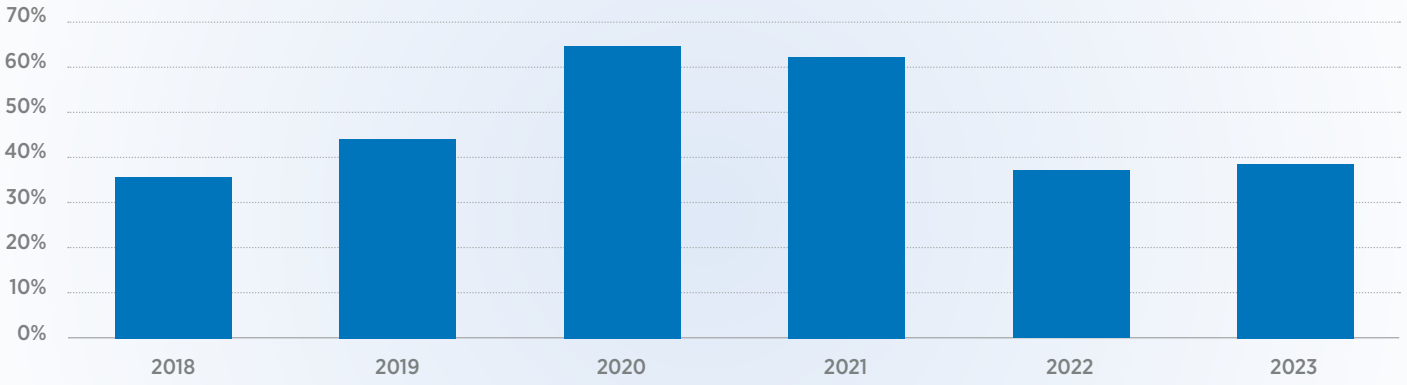
US CYBER INSURANCE DIRECT PREMIUMS WRITTEN LEVEL OUT AS PRICING SOFTENS WHILE THE NUMBER OF POLICIES CONTINUES TO INCREASE



Source: S&P Capital IQ (Contains copyrighted and trade secret materials distributed under license from S&P Capital IQ, for recipient's internal use only); Moody's Ratings.

Cyber insurance carrier profitability will help drive this growth through underwriting discipline and focus on effective security controls. Recent research indicates that carriers have emerged from challenging periods of 3 years ago to realizing favorable loss ratios, which could fuel growth further.[9]

AGGREGATE LOSS RATIO FOR US STANDALONE CYBER INSURANCE DROPS IN RECENT YEARS



Source: S&P Capital IQ (Contains copyrighted and trade secret materials distributed under license from S&P Capital IQ, for recipient's internal use only); Moody's Ratings.

Despite the changing cyber threat landscape, we expect the cyber insurance market to follow the trends of the past several years and continue its expansion in 2025 and in the years to follow. It will continue to mature as it pursues valuable insight into how threats manifest into claims and the most effective security controls that prevent and mitigate their effects. However, the market will need to be disciplined as it grows. It must be mindful of changing threats, rapidly evolving technology, and an increasingly unstable geopolitical global threat landscape. Cyber insurance carriers, brokers, reinsurance providers, data scientists, analytics experts, and cybersecurity vendors will all play key parts in its growth in the coming year.

[1]"Cost of a Data Breach Report." *IBM*. 2024. PDF file.

[2]"H1 2024 Crimeware Report." *Arete*.

[3]"New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying." *Coveware*, January 2024.

[4]"H1 2024 Crimeware Report." *Arete*.

[5]"Internet Crime Report." *Federal Bureau of Investigation*. PDF file.

[6]"Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting." *Department of Homeland Security Cybersecurity and Infrastructure Security Agency*, 4 Apr. 2024, PDF file.

[7]"DAIL — the Database of AI Litigation." Ethical Tech Initiative.

[8]"Sector in Depth Report." *Moody's Ratings*, 5 Sept. 2024. 2024. PDF file.

[9]"Sector in Depth Report." *Moody's Ratings*, 5 Sept. 2024. 2024. PDF file.

AJG.com **The Gallagher Way.** Since 1927.

Gallagher