2024 Cyber Insurance Market Conditions Outlook:

Cyber Market Stabilization and Lingering Turbulence

By: John Farley, Managing Director, Cyber

Gallagher

Insurance | Risk Management | Consulting

Introduction

After several years of rising premiums and capacity constriction, the 2023 cyber insurance market surprised many as softening conditions rippled through the marketplace in an impactful way. This was due in large part to the reduced frequency and severity of cyber claims in the last half of 2022. Theories behind the decrease in claim activity range from hacking groups in Russia and Ukraine being distracted by their own conflict to more sophisticated and disciplined underwriting to the improved cyber risk hygiene of insureds.

The past year brought welcome news to most cyber insurance buyers, as rates remained flat or declined and capacity came back to the market. Competition amongst cyber insurance carriers heated up, helped keep pricing contained, and drove capacity expansion. However, despite the favorable buyer's market, there remains an underlying concern in the underwriting community around systemic cyber risk. Discussions around the impact of a potential catastrophic cyber event will undoubtedly continue throughout 2024.

What we saw in 2023?

Last year's market was a fascinating tale of two competing forces. As we entered 2023, we began to see an uptick in cyber claim activity with an unexpected and significant resurgence of ransomware attacks, reversing the course of cyber loss trends in 2022. The hardest-hit industry sectors included healthcare, financial services, professional services, technology, education, and government. Some of the most impactful cyber-claims activity involved attacks on software providers in the supply chain. Wrongful data collection claims also increased and emerged as a serious cyber threat that often allows for private rights of action and results in regulatory enforcement.

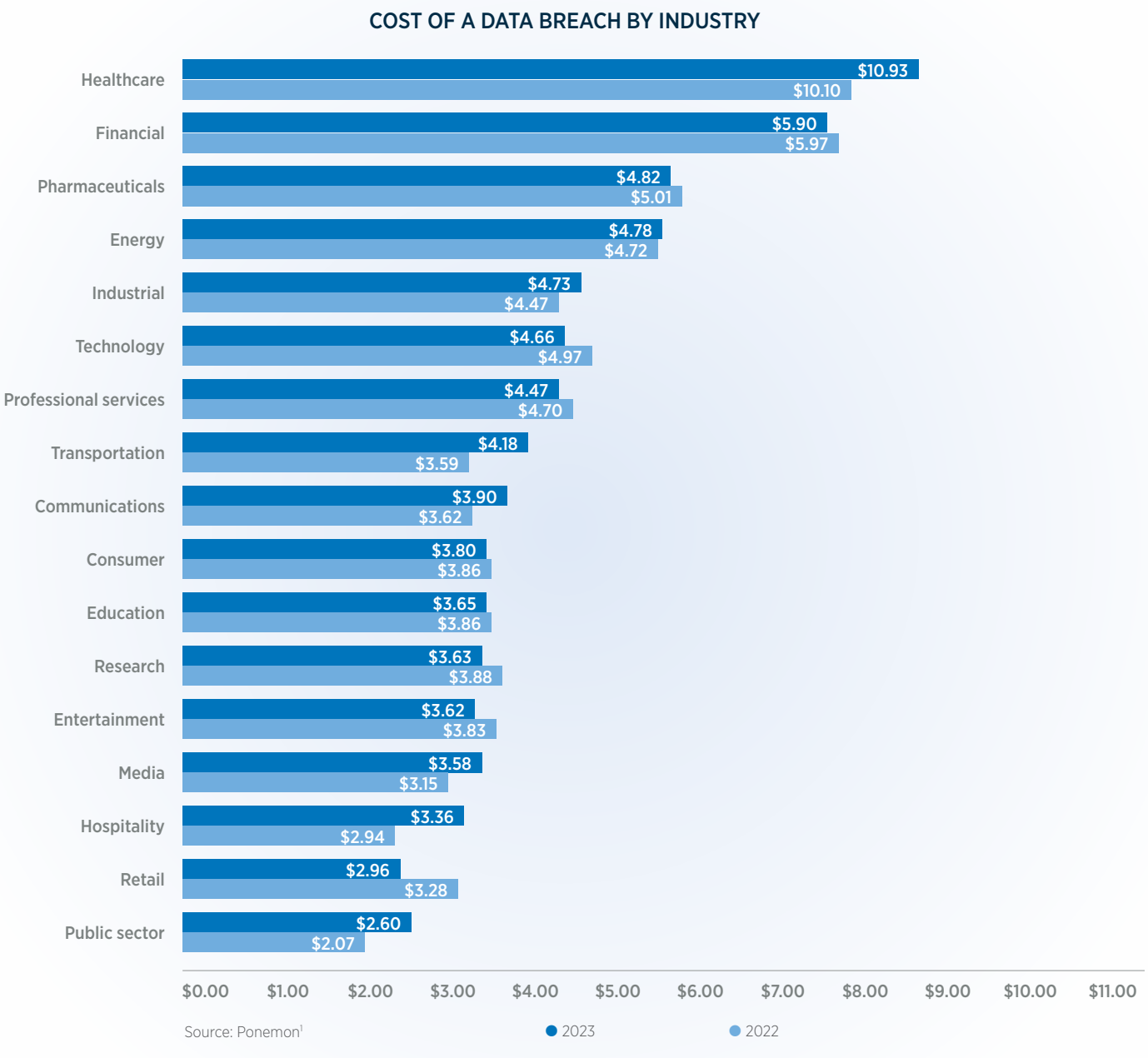
All the while, systemic risk concerns were heightened by two glaring factors. Increasing geopolitical tensions between well-funded nation-states, stoked fears of attacks on critical infrastructure. In addition, the sudden emergence and mass adoption of artificial intelligence technology began to force serious conversations around what it may mean for new cyber exposures and increasing systemic cyber risk.

While loss trends ticked higher, softening market conditions still managed to hold throughout 2023. This posed a particular challenge to the cyber insurance carriers that were competing to maintain and grow their client base while maintaining profitability.

CYBER CLAIMS TRENDS AND THE 2024 THREAT LANDSCAPE

The ransomware ecosystem continues to evolve, and we note changes as criminal affiliations have shifted. Many organized hacking groups are rebranding to avoid law enforcement scrutiny. We expect a continual introduction of new ransomware variants, increasing ransom demands, and all industry sectors to be impacted at some level. We also expect ransomware attacks to follow the ongoing trend of double extortion, where threat actors both encrypt and exfiltrate their victim's data, threatening to expose it if extortion is not paid.

Today's cyber claim trends were highlighted in several reports published over the past year. In July 2023, the IBM-Ponemon Cost of a Data Breach study revealed that the average cost of a data breach reached an all-time high of $4.35 million. This represents a 2.6% increase from the prior year.[1]



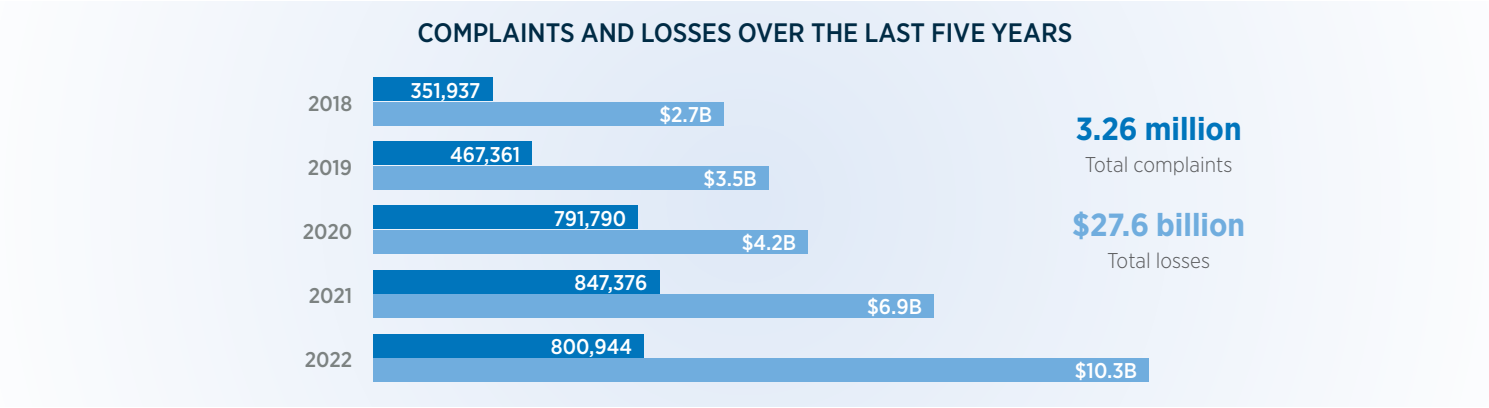
17%	$158K	73.6%	$20M
% of time a ransom is paid	Median ransom payment	Average discount % across all ransomware variants	Highest initial ransom demand

Source:[2] Threat_report_Q3_2023.pdf (hubspotusercontent-na1.net)

One cyber insurance carrier published a report[3] stating that 2023 Q3 ransomware activity increased by 95% compared with the year prior and 11% compared with the prior quarter.

The FBI's Internet Crime Report revealed that social engineering attacks continue to plague businesses both large and small across virtually all industry sectors. According to the report, there have been a staggering $10.3 billion in internet crime losses in 2022, increasing every year over the past five years. The losses were driven by Business Email Compromise ("BEC") schemes with losses over $2.7 billion.[4]

Over the last five years, the IC3 has received an average of 652,000 complaints per year. These complaints address a wide array of internet scams affecting victims across the globe.[3]



Another factor that could exacerbate cyber claims frequency and severity involves heightened regulatory risk. While our focus is on the regulators at the state and federal levels in the United States, regulatory risk may extend to other territories and be influenced by other global privacy regimes in 2024.

Many states have enacted comprehensive privacy laws,[5] and we expect more to follow in 2024. Most focus on data collection compliance obligations, and some allow for private rights of action in certain circumstances. We note the most significant claims activity is being driven by wrongful data collection allegations around both website tracking technologies as well as biometric data.

At the federal level, the SEC has led the way by imposing new mandatory reporting requirements for publicly traded companies around cyber incidents and overall cyber risk management practices.

The new mandates require these organizations to report "material" cyber incidents to the SEC within four business days and require annual reports to detail efforts made around cyber risk management. Recent litigation brought by the SEC is evidence of the commission's focus on specific language used in company disclosures and/or statements regarding this risk exposure. We suspect that this may be the beginning of a new wave of increased regulatory scrutiny that will undoubtedly raise expectations for managing cyber risk among the C-suite and boards of directors.

THE US FEDERAL GOVERNMENT RESPONSE

The Biden administration has been active on multiple initiatives and guidance around cyber risk. In March 2023, the White House launched its National Cybersecurity Strategy, which outlines a new approach to cyber threats along with a cohesive strategy that imposes responsibilities on both the public and private sectors.[6] It focuses on five key areas:

- Improving cyber defenses for operators of critical infrastructure.
- Disrupting threat actors.
- Enhancing the security standards of technology sold to organizations.
- Funding public investments to support cyber security improvements.
- Internationally focused strategies to combat cybercrime.

In July 2023, the White House released the National Cybersecurity Strategy Implementation Plan.[7] In this document, they operationalize the various goals set forth in the March 2023 document, with specific deliverables and timelines.

Learn more about NIST: Meeting the Challenges of the US National Cybersecurity Strategy

In October 2023, the White House launched the International Counter Ransomware Initiative.[8] This is a US-led alliance of 40 countries that vows to eliminate the funding of criminals by refusing to pay ransomware. Member countries will be able to access information sharing platforms that provide a "black list" through the US Department of Treasury that includes information on digital wallets being used to move ransomware payments. To date, there is no legal requirement to prevent organizations from paying ransom, and we expect any future mandate to that end would require legislation.

Also in October 2023, the White House issued the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,[9] establishing new standards for artificial intelligence (AI) safety and security. The executive order includes several key actions, plus important steps to take now:

- It requires developers of powerful AI systems to share safety test results and critical information with the US government.
- It mandates the development of standards, tools, and tests to ensure the safety and security of AI systems.
- It addresses the risks of using AI in engineering dangerous biological materials and establishes guidelines for detecting AI-generated content and authenticating official content.

CYBER INSURANCE PRODUCTS EVOLVE

The cyber insurance marketplace will continue to evolve in 2024 and reflect dynamic change as both technology and the threat landscape advances. There are several developments in policy wording that we are watching closely:

- **War and systemic risk exclusions:** Several recent and ongoing geopolitical conflicts are directly impacting countries that tend to have advanced cyber capabilities, and we expect underwriters to keep a watchful eye as activity continues to develop. There is a real possibility that these conflicts may extend the traditional means of combat from air, sea, land, and space to the cyber domain, and this has led to many cyber carriers revising the wording around war exclusions. Most are expanding the scope of the exclusion around war and imposing sub-limits around other systemic events. We are advising our clients to pay particular attention to wording specific to attribution, the level of harm in a claim scenario, whether war is formally declared or not, and wording that may impact coverage for parties not directly involved in a particular conflict or those impacted by the cascading effects of an attack on another party.
- **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 number of regulatory bodies have led to coverage constriction around costs for regulatory investigations, settlements, fines, and penalties.
- **Wrongful data collection:** As state, federal, and international privacy law has expanded in scope and complexity, so 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, such as the Biometric Information Privacy Act.

REINSURANCE: DRIVING GROWTH IN 2024

Reinsurers have emerged as a key figure in the growth of the cyber market, to whom primary carriers are ceding over 50% of their premiums.[14] They are tapping the capital markets, specifically insurance-linked securities, for their own backing and to ultimately expand capacity in a meaningful way. In 2023, one reinsurer issued three cyber catastrophe bonds totaling $81.5 million in coverage,[10] while another reinsurer issued a single $75 million fully collateralized catastrophe bond for systemic cyber events.[11] We expect more to follow in 2024 to meet the growing demand for cyber insurance.

Primary insurers, reinsurers, and capital markets will continue to rely heavily on advanced modeling tools to more precisely predict the frequency and severity of cyber events. This was evident in October 2023, when Lloyds published a study[12] on a hypothetical cyberattack on a major financial services payments system. It revealed potential global economic losses of $3.5 trillion. In this scenario, the three countries that experience the highest five-year economic loss would be the United States ($1.1 trillion), followed by China ($470 billion), and Japan ($200 billion).

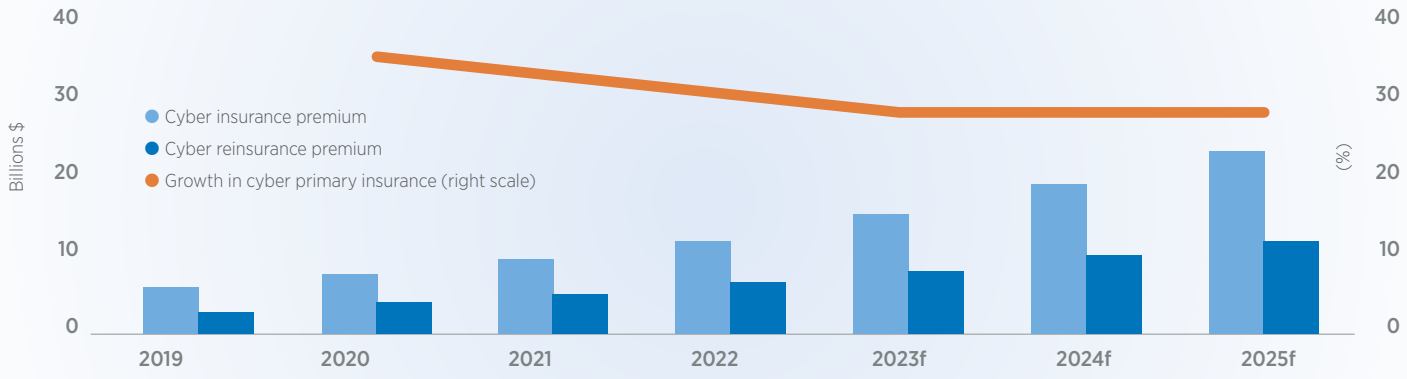
WHERE WE ARE HEADED

Emerging technology, most notably artificial intelligence (AI), may exacerbate an already formidable cyber threat environment. It will require efforts from the government, regulators, technology providers, and the insurance industry to fully understand the new risk before it can be managed. In the meantime, we remain focused on the various forms of AI usage and the risks that may emerge. Threat actors may use it to launch sophisticated phishing schemes, misinformation campaigns, and other attacks. AI adoption by business leaders could have unintended consequences, including but not limited to data bias, privacy liability, risks associated with intellectual property, and professional liability.

There exists the potential for several lines of coverage to be impacted beyond cyber insurance and technology Errors and Omissions policies. Losses may expand to Directors and Officers policies, employment practices policies, media liability policies, product liability policies, and professional errors and omissions policies in the near future.

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 2024 and in the years to follow.

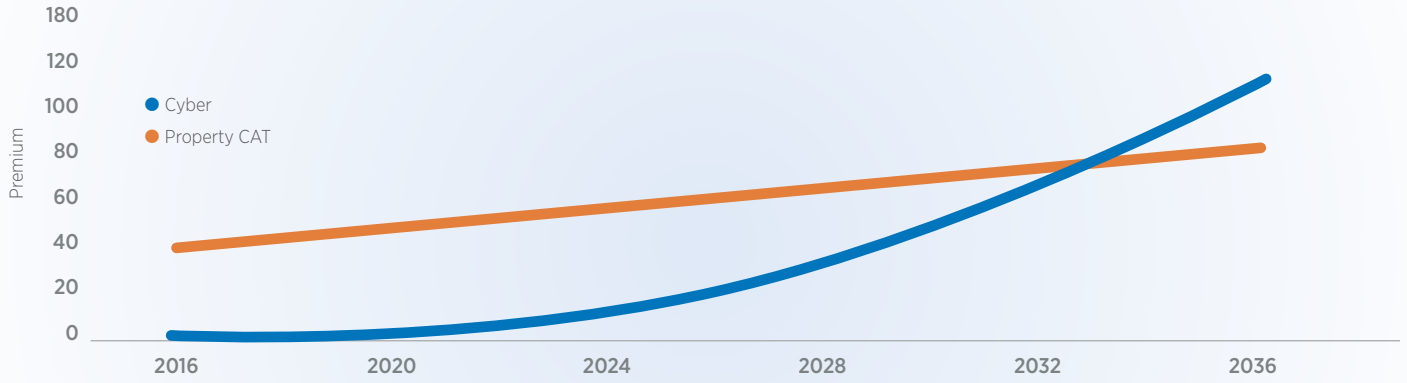
CYBER REMAINS ON A FAST TRACT
GLOBAL CYBER (RE)INSURANCE PREMIUM



f — Forecast. Sources: Munich Re, S&P Global Ratings

Gallagher Re's recent report, The Future of Cyber (Re)insurance,[13] predicts that if the market continues at its current pace, it will double in size every three years, leading to profound growth.

REINSURANCE PREMIUM PROJECTIONS — CYBER VS. PROPERTY CAT



Assuming average growth if 50% growth in cyber premium, in 2021 and an average of 25% for all subsequent years.

Assuming 46% premium being ceded to cyber reinsurance market in 2021, depreciating to 25% by 2040.

Assumed a growth rate of 3.9% for property for 2016–2028, deducing it to 3.5% for 2029–40 (ignoring cycles for simplicity).

In summary, as we look forward to 2024, we see a cyber market that has matured to a level where both applicants and providers of cyber insurance have gained valuable insight into how threats manifest into claims, and generally understand the minimum security controls required to help prevent and mitigate their effects. Much more needs to be done, and a growing number of professionals in the cyber insurance ecosystem will forge ahead with innovation around advanced underwriting and loss modeling tools. 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] Ponemon 2022 IBM Cost of a Data Breach Report(1).pdf.

[2] Threat_Report_Q3_2023.pdf (hubspotusercontent-na1.net).

[3] Q3 Ransomware Report: Global Ransomware Attacks Up More Than 95% Over 2022 (corvusinsurance.com).

[4] 2022_IC3Report.pdf.

[5] US State Privacy Legislation Tracker (iapp.org).

[6] Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy," *The White House*, 2 Mar. 2023.

[7] "White House National Cybersecurity Implementation Plan," *The White House*, Jul. 2023. PDF file.

[8] "Fact Sheet: Biden-Harris Administration Convenes Third Global Gathering to Counter Ransomware," *The White House.*

[9] "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," *The White House*, 30 Oct. 2023.

[10] Beazley Sponsors Third Cyber Catastrophe Bond, $16.5m Cairney III — Artemis.bm.

[11] Axis Completes Cyber Catastrophe Bond | Business Insurance.

[12] Lloyd's Systemic Risk Scenario Reveals Global Economy Exposed to $3.5trn From Major Cyber Attack (lloyds.com).

[13] Future-of-Cyber-Reinsurance.pdf (ajg.com).

[14] Reinsurers' Cyber Rates Expected To Rise as They Seek To Regain Profitability: *S&P (Insurance Journal).*

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

Gallagher