MEMORANDUM

TO: Members and Interested Regulators of the Pf p

This indicates a growing demand for cyber insurance coverage. The number of claims has also risen, with 33,561 reported in 2023. This increase reflects the rising frequency of cyber incidents.

The cyber insurance market has begun to stabilize with smaller rate increases and, in some cases, flat renewals.[2] However, the market has not reverted to the softer conditions seen in the years leading to the global pandemic of 2020. Positive factors supporting the stable cyber insurance market outlook include continued demand, increasing take-up rates for cyber coverage, and continual improvements in cyber hygiene. Insurers have switched their focus from pricing to managing systemic risk as they look to limit their aggregate exposure. There is a rising demand for cyber insurance among small and medium-sized enterprises, as 72% without cyber insurance say a major cyberattack could destroy their business.[3]

The cyberthreat landscape continues to break records as it becomes more volatile and complex. Businesses across all revenue bands have experienced an increase in cyber incidents, with companies earning more than $100 million seeing the largest uptick—a 20% increase in the number of claims and a 72% increase in claims severity compared to the second half of 2022.[4] Certain sectors, like health care and financial services, experienced higher claim costs partially due to the data they handle and the regulatory requirements they must comply with.

The cyber insurance industry has evolved significantly and has become a crucial component in the broader cybersecurity landscape. As cyber threats continue to grow in complexity and frequency, cyber insurance provides a vital safety net for businesses, helping to mitigate financial losses such as data breaches, ransomware campaigns, and business interruptions.[5] However, it is essential to understand cyber insurance is not a substitute for robust in-house cybersecurity measures. Instead, it should be viewed as a tool that complements and enhances overall cybersecurity posture. Effective cybersecurity requires a proactive approach that maintains regular risk assessments, employee training, and the efficient implementation of advanced security technologies.[6] Cyber insurance can support these efforts by providing protection against cyber threats and encouraging better risk management practices, but it cannot eliminate the need for strong internal defenses.

The data used to develop this report provides a snapshot of the cyber insurance market and the evolving cybersecurity landscape. The NAIC and its staff recognize that data values may change due to resubmissions and amendments made by reporting companies.

[2] https://www.everestglobal.com/us-en/news-media/features/2024/viewpoint/the-state-of-the-cyber-insurance-market
[3] https://cowbell.insure/wp-content/uploads/pdfs/Cowbell-Cyber-Round-Up-Q2-2023.pdf
[4] https://www.coalitioninc.com/announcements/2023-claims-report-mid-year-update
[5] https://www.ajg.com/us/news-and-insights/2024/jan/2024-cyber-insurance-market-conditions-outlook/
[6] https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Figure 3.

Figure 3 represents the domestic direct written premium for the U.S. market from 2019 to 2023. The domestic surplus lines wrote 60.4% of the direct written premium, representing a small (1%) growth in the domestic market share.

Figure 5.

Figure 5 re

Exhibit 1- Top 20 Admitted Groups[9]

2023 Rank	2022 Rank	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share	Cumulative Market Share
1	1	Chubb Ltd Grp	$ 573,582,701	53.8%	7.9%	7.9%
2	3	AXA Ins Grp	$ 487,195,706	62.6%	6.7%	14.6%
3	2					

Major Trends

In this section, we explore major cybersecurity trends shaping the cyber insurance market. It is important to note that this overview is not exhaustive and does not encompass all potential risks and threats in the cybersecurity landscape. These trends highlight the dynamic and evolving nature of cybersecurity challenges, underscoring the need for robust and adaptive cyber insurance solutions.

Ransomware

Ransomware continues to be a major threat, contributing significantly to the rise in claims as attackers become more sophisticated in their methods. The rise of Ransomware as a Service (RaaS) has lowered the barrier to entry for cyber actors. The financial impact of ransomware attacks can be significant, not just from the ransom payment but also from costs related to data recovery, business interruption, and reputational damage.[10] However, the percentage of companies affected by ransomware attacks that are paying the ransom has come down over time, and that should reduce claim severity averages.[11]

pe112.2 2.12.9 ( )0.1(t (c)Sep) Tdi-0.8 3cc (s)1 9.6 BT13 3 (E)nte1(c)12 (k)0un -33.1]J0tean -.3 (4.2) 3..2 -33.sh

Business Email Compromise

Business email compromise (BEC) incidents represent a substantial portion of claims. These attacks often result in financial losses due to fraudulent wire transfers and other deceptive practices.[12] These attacks typically involve phishing campaigns where attackers use social engineering to gain access to business email accounts to conduct

outages, including those caused by non-malicious events like human error, helps to ensure recovery from disruptions not resulting from a cyberattack.[17]

Like those found in other property insurance lines, U.S. cyber insurance policies typically include “war and hostile act” exclusions.[18] These exclusions stipulate that an insurer will not cover losses resulting from acts of war, terrorism, or other hostile actions.[19]

Often referred to as the “failure to maintain security” or “failure to follow” exclusion, some carriers include a specific exclusion that precludes coverage for claims resulting from an insured’s failure to maintain minimum or adequate security standards.[20,21]

Summary

Cyber insurance is a critical component of a comprehensive risk management strategy, providing financial protection and support during cyber incidents. Reacting to the post-COVID surge in ransomware attacks, insurance companies increased rates significantly and tightened terms and conditions, specifically by increasing deductibles and putting sub-limits within the policies. The result has been an improvement in underwriting processes and improved cybersecurity hygiene. Insurers’ and insureds’ operations have become more complex, interconnected, and dependent on technology and technology-related providers. The likelihood and impact of operational disruptions and the importance of operational resilience have increased. Effective risk management strategies, including using advanced cybersecurity tools and maintaining up-to-date software, are crucial for minimizing the impact of cyber incidents. Additionally, improved cyber-related business practices, including better backup procedures, rehearsed restarts for critical operations, and better strategies to deal with cyber actors—can help businesses protect themselves.

p-01c 0n(ra)1.63Tm.21e6 0

State insurance regulators continue to monitor and assess the market to better understand how the industry protects policyholders, including meeting with and hearing from subject matter experts an