NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Members and Interested Regulators of the Property and Casualty Insurance (C) Committee and Innovation Cybersecurity and Technology (H) Committee

FROM: NAIC Staff

DATE: October 15, 2024

RE: Report on the Cyber Insurance Market

This report examines the cyber insurance market using data from the NAIC's *Property & Casualty Annual Statement Cybersecurity and Identity Theft Supplement* (Cyber Supplement) and alien surplus lines data from the NAIC's International Insurers Department (IID). The Cyber Supplement requires U.S. domiciled insurers to report the following information on stand-alone cybersecurity insurance policies and coverage sold as part of a package policy:

- Number of claims reported (first-party and third-party).
- Direct premiums written and earned.
- Direct losses paid and incurred.
- Adjusting and other expenses paid and incurred.
- Defense and cost containment expenses paid and incurred.
- Number of policies in force (claims made and occurrence).

Note that insurers are only required to file direct premiums written and earned for cyber insurance coverage sold as part of a package policy if it is available or estimable.

The report discusses changes in the cyber insurance market, the cybersecurity landscape, and the reasons for these changes to help better understand the U.S. cyber insurance market—the largest cyber insurance market in the world.

Overview

The U.S. cyber insurance market accounts for 59% of the $16.66 billion in premium written for cyber coverages globally in 2023.[1] In the U.S., $9.84 billion of direct written premium (DWP) was reported for cyber insurance coverage, including domiciled insurers and alien surplus lines carriers writing coverage throughout the U.S. market.

The U.S. domiciled insurers reported $7.25 billion in DWP, up slightly over the $7.24 billion in DWP reported for 2022. After a significant decline in 2021, the number of policies in force increased 11.7% in 2023 to 4,369,741.

---

[1] https://www.howdengroup.com/news-insights/howden-predicts-global-cyber-insurance-premiums-could-exceed-usd-50-billion-by-2030

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 1.

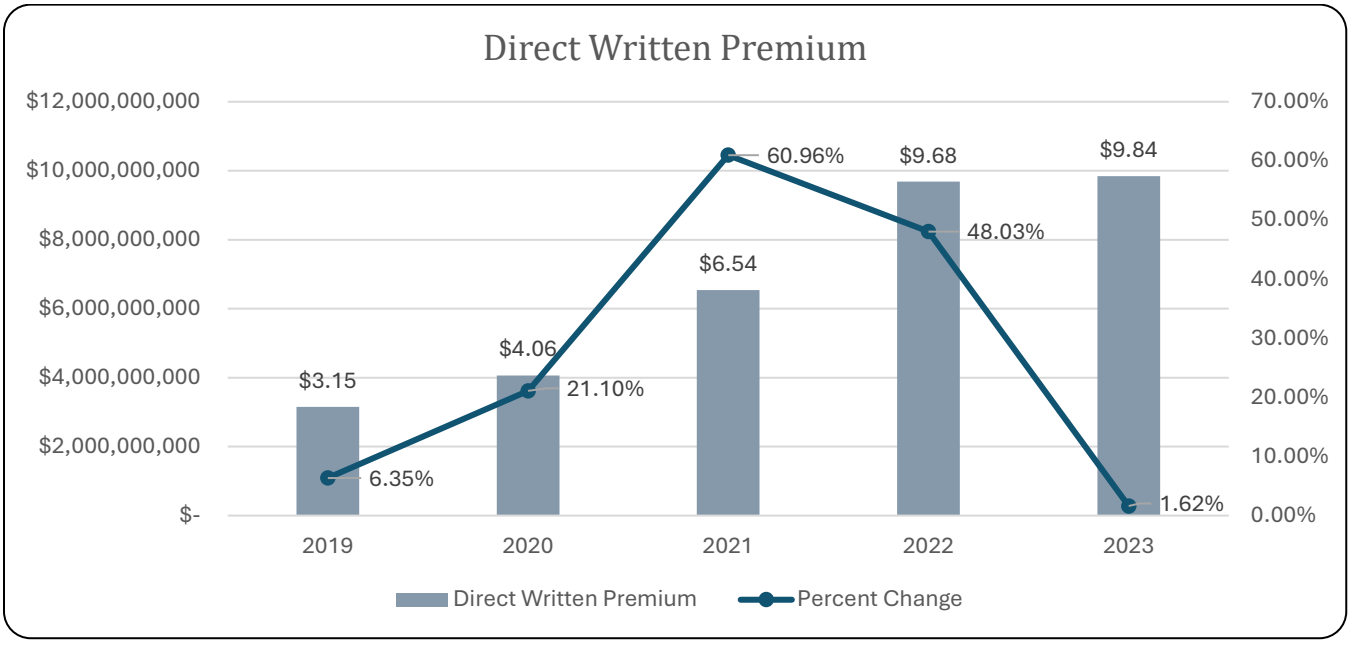


Figure 1 shows the domestic admitted surplus and alien surplus lines insurers writing cyber insurance coverage in the U.S. overall direct written premium increased 1.62% to a 2023 total of $9.84 billion written for cyber coverages.

Figure 2.[7]

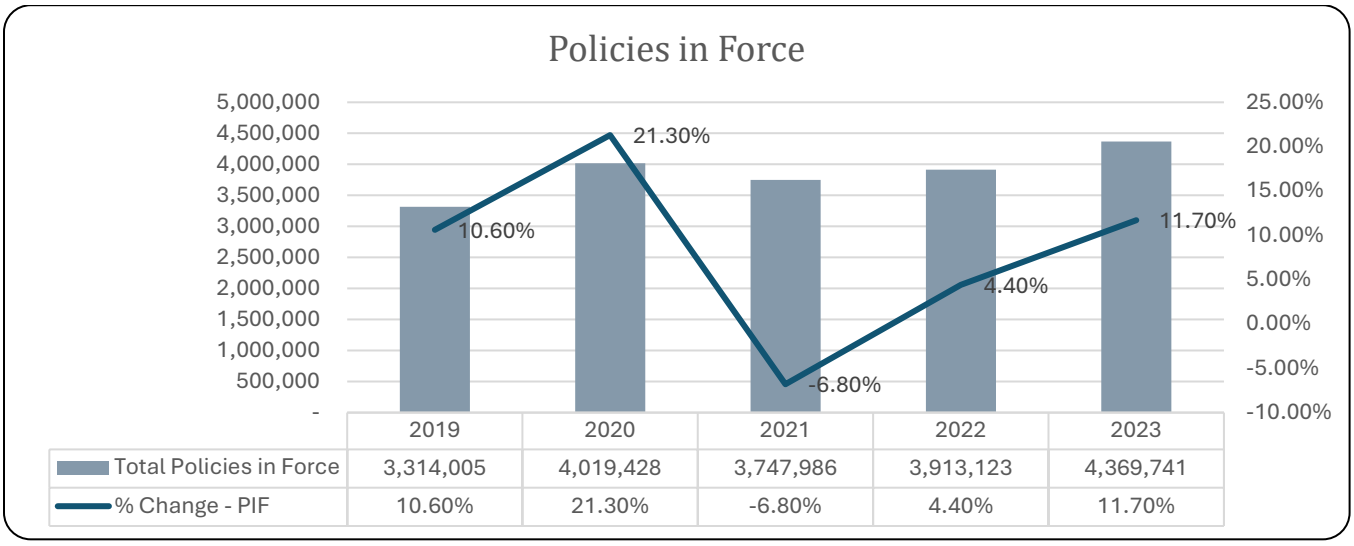
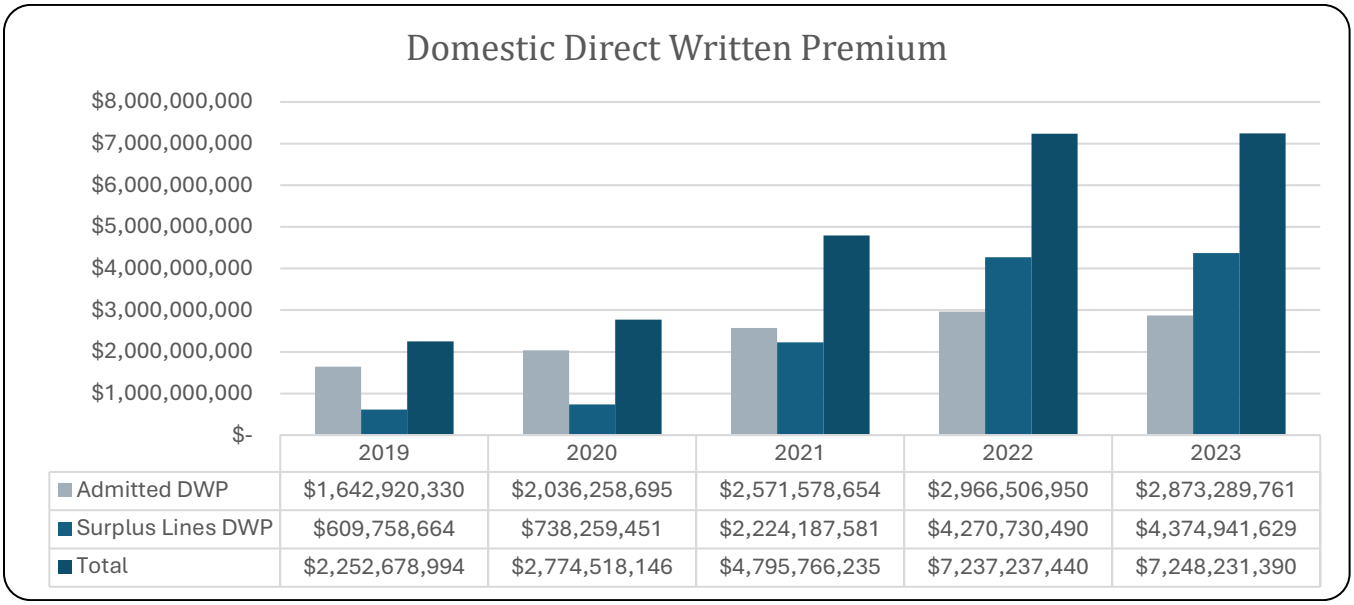


Figure 2 illustrates the number of policies in force from 2019 to 2023 and the rate of change by year. This figure does not include the number of policies in force in the alien surplus lines market. Following a near 6.8% decrease observed in 2021, policies in force surpassed the 4.01 million values in 2020. Policies in force increased 11.7% from 3.9 million to 4.3 million, signaling a growth in the comfort and stability of the cyber insurance market.

[7] Does not include alien surplus lines.

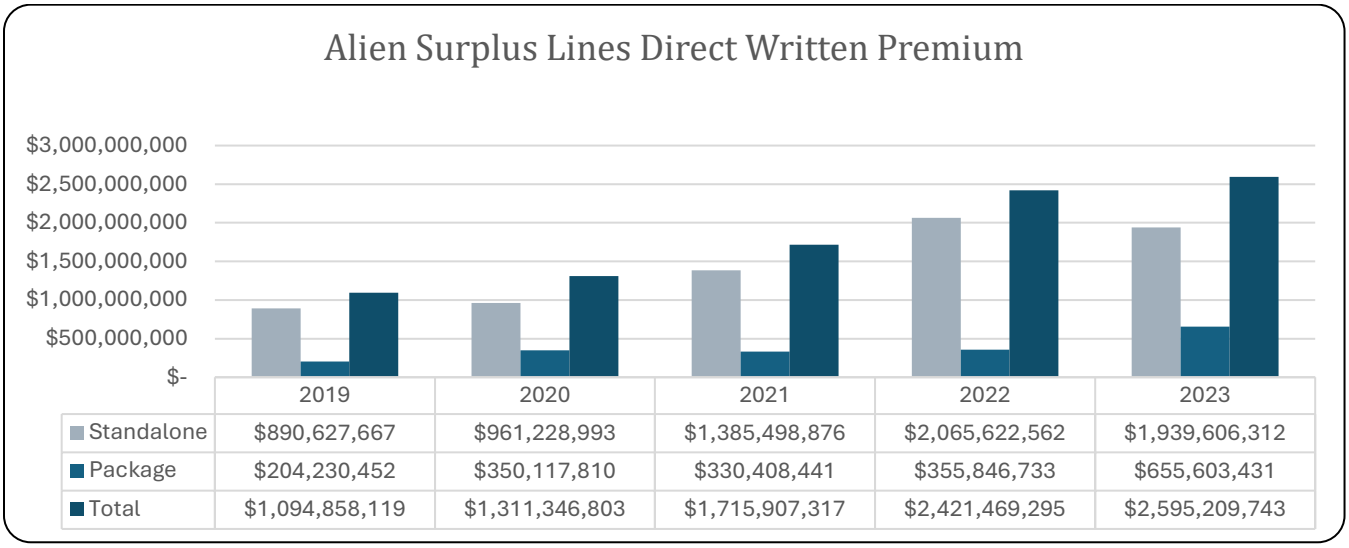
Figure 3.



	2019	2020	2021	2022	2023
Admitted DWP	$1,642,920,330	$2,036,258,695	$2,571,578,654	$2,966,506,950	$2,873,289,761
Surplus Lines DWP	$609,758,664	$738,259,451	$2,224,187,581	$4,270,730,490	$4,374,941,629
Total	$2,252,678,994	$2,774,518,146	$4,795,766,235	$7,237,237,440	$7,248,231,390

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 4.



	2019	2020	2021	2022	2023
Standalone	$890,627,667	$961,228,993	$1,385,498,876	$2,065,622,562	$1,939,606,312
Package	$204,230,452	$350,117,810	$330,408,441	$355,846,733	$655,603,431
Total	$1,094,858,119	$1,311,346,803	$1,715,907,317	$2,421,469,295	$2,595,209,743

Figure 4 shows the direct written premium from 2019 to 2023 for alien surplus lines, including standalone, package policies, and the totals. Alien surplus premium totals increased 7% for a 2023 total of $2.59 billion. A previous version of this chart reflected an incorrect value for 2019; a refiling occurred and was not reflected.[8] The value, as seen, is current and should be used going forward.

[8] 2019 previously reported a total DWP of $887,620,348. https://content.naic.org/sites/default/files/inline-files/Final2023CyberReport.pdf

Figure 5.

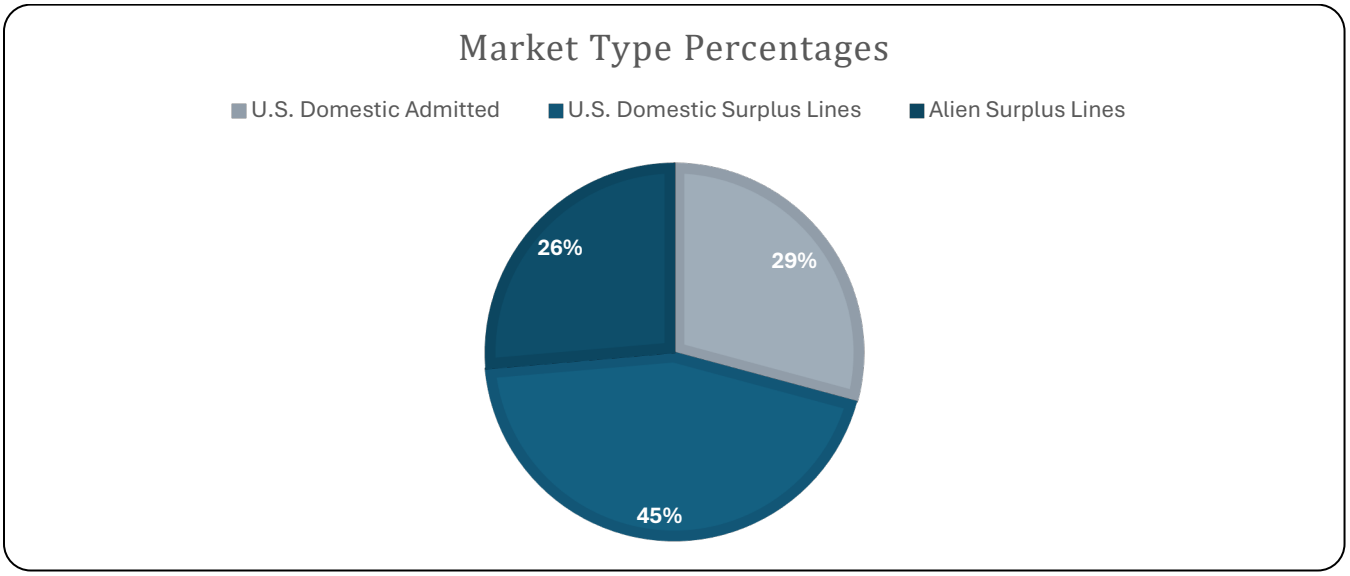
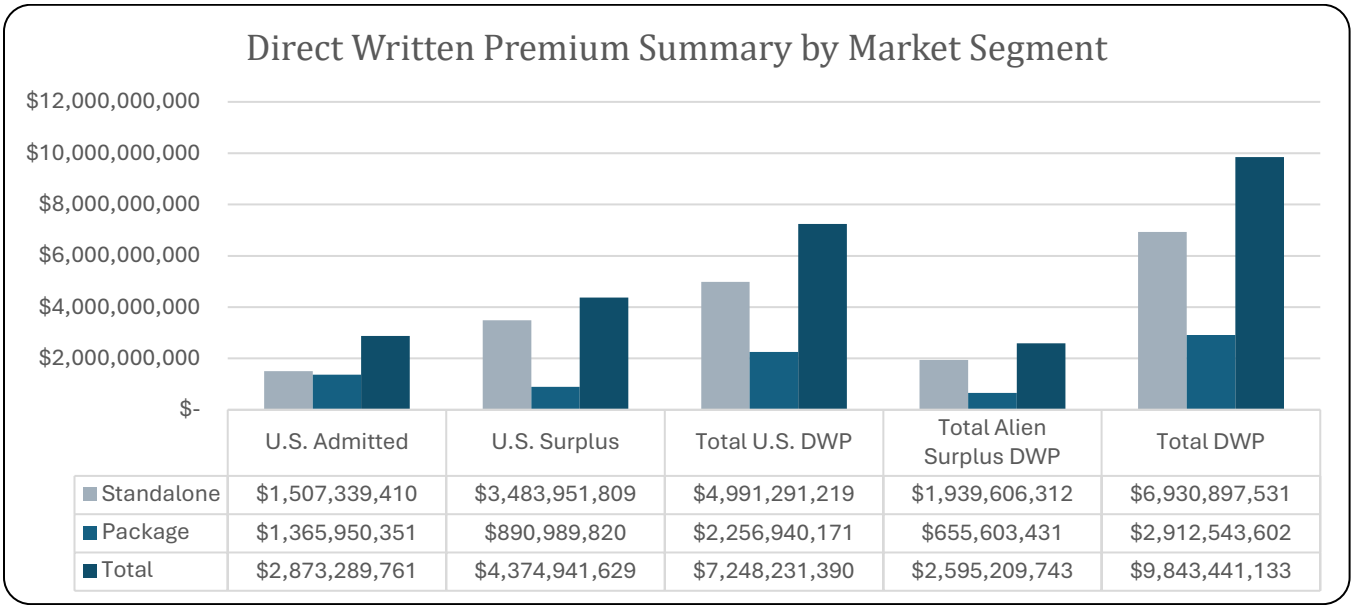


Figure 5 represents the U.S. market as shares of the total direct written premium for 2023, including admitted, domestic surplus lines, and alien surplus lines segments. Domestic surplus lines held 45% of the market share, an increase of nearly 9% from 2022.

Figure 6.



	U.S. Admitted	U.S. Surplus	Total U.S. DWP	Total Alien Surplus DWP	Total DWP
Standalone	$1,507,339,410	$3,483,951,809	$4,991,291,219	$1,939,606,312	$6,930,897,531
Package	$1,365,950,351	$890,989,820	$2,256,940,171	$655,603,431	$2,912,543,602
Total	$2,873,289,761	$4,374,941,629	$7,248,231,390	$2,595,209,743	$9,843,441,133

Figure 6 summarizes each market segment, the U.S. admitted and domestic surplus lines, and the total alien surplus lines direct written premium.

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	Fairfax Financial	$ 462,953,536	51.0%	6.4%	21.0%
4	6	St Paul Travelers Grp	$ 384,850,997	22.4%	5.3%	26.3%
5	4	Tokio Marine Holdings Inc Grp	$ 377,856,755	44.6%	5.2%	31.5%
6	12	Berkshire Hathaway	$ 289,300,031	47.1%	4.0%	35.5%
7	5	Arch Ins Grp	$ 282,135,643	58.1%	3.9%	39.4%
8	7	American Intrnl Grp	$ 274,377,152	79.3%	3.8%	43.2%
9	10	Sompo Grp	$ 262,947,950	44.9%	3.6%	46.8%
10		Starr Grp	$ 260,014,380	0.0%	3.6%	50.4%
11	11	CNA Ins Grp	$ 228,394,487	36.2%	3.2%	53.6%
12	8	Nationwide Corp	$ 226,520,441	27.6%	3.1%	56.7%
13	9	Zurich Ins Grp	$ 199,243,405	63.5%	2.7%	59.5%
14	15	AXIS Capital Grp	$ 185,267,064	37.8%	2.6%	62.0%
15	13	Liberty Mut Grp	$ 178,276,845	74.0%	2.5%	64.5%
16	20	Hartford Fire & Cas Grp	$ 174,847,045	11.3%	2.4%	66.9%
17	17	Ascot Ins US Grp	$ 174,481,380	30.1%	2.4%	69.3%
18	24	AmTrust Financial Serv Grp	$ 169,973,572	4.9%	2.3%	71.6%
19	16	Beazley Grp	$ 149,637,999	18.3%	2.1%	73.7%
20	22	Intact Financial Grp	$ 144,569,139	18.6%	2.0%	75.7%

Exhibit 1 represents the direct written premium and loss ratios for the top twenty insurer groups providing standalone and packaged policies in the U.S. admitted market.

[9] Does not include alien surplus lines.

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]

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 their criminal activity. Cyber insurance policies often include liability coverage for claims resulting from security breaches that lead to fraudulent fund transfers, providing a potential avenue for cover in BEC incidents.[13] Highlighting the substantial financial threat posed by these attacks, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) reported that BECs resulted in more than $2.9 billion of adjusted losses in 2023.[14]

Data Breaches

Reflecting the ongoing challenges businesses face in securing sensitive information, data breaches remained a significant driver of cyber insurance claims in 2023, with the health care, information technology (IT), and communications sectors being the most impacted.[15] Often leading to significant legal and regulatory consequences, these incidents involve unauthorized access to sensitive information or information systems. The associated costs could include notification expenses, legal fees, regulatory fines, and credit monitoring services for impacted consumers.

Exclusionary Language

Cyber insurance policies often include exclusionary language to limit the insurer's liability for certain types of risks. In 2024, these policies have increasingly incorporated language to address unplanned outages, particularly focusing on business interruption and contingent business interruption coverage.[16] Insurers have been observed more recently to include common triggers for coverage due to system failures caused by non-malicious acts, such as human error. This shift toward providing broader protection for businesses affected by significant technology

---

[10] https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf
[11] https://www.cloudwards.net/ransomware-statistics/
[12] https://library.cyentia.com/report/report_021198.html
[13] https://www.mcgriff.com/resources/articles/business-email-compromise.html
[14] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
[15] https://www.security.org/insurance/cyber/statistics/
[16] https://www.mosaicinsurance.com/resources/insights/~/technology-transformation-and-telematics-why-this-is-the-future-of-cyber-insurance/

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.

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 and evaluating the data needs of state insurance regulators. The regulators and NAIC staff seek to discuss and better understand considerations such as the availability, affordability, and pricing of cyber insurance products, disclosures, policy limits, policy language, trends in requirements, underwriting practices, and the role of reinsurance in the cyber insurance market.

[17] https://www.insurancejournal.com/news/national/2024/07/22/784918.htm
[18] https://www.fitchratings.com/research/insurance/russian-cyberattacks-may-test-insurer-war-exclusion-policy-language-01-03-2022
[19] https://www.darkreading.com/cyberattacks-data-breaches/cyber-insurance-and-war-exclusions
[20] https://www.gbainsurance.com/avoiding-cyber-claim-denials
[21] https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/navigating-common-exclusions-in-cyber-policies