NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Property and Casualty Insurance (C) Committee

FROM: NAIC Staff

DATE: Oct. 18, 2022

RE: Report on the Cyber Insurance Market

The NAIC collects data from insurers writing cyber insurance through its *Property/Casualty Annual Statement Cybersecurity and Identity Theft Supplement* (Cyber Supplement). Cyber Supplement data have been collected since 2016, and alien surplus lines data was collected beginning in 2017. This report focuses on the cyber insurance market by presenting data found within the Cyber Supplement and alien surplus lines data collected through the NAIC's International Insurers Department (IID). The report discusses changes in the cyber market and the reasons for these changes to help better achieve an understanding of the U.S. cyber insurance market.

Overview

Cybersecurity protection continues to be vital to U.S. businesses' effective and efficient operation. Businesses in the financial sector remain at risk for a cyber-attack. Insurers are not only susceptible to cyber-attacks, but also to losses incurred from claims linked to their cyber insurance products.

Data breaches in 2021 outpaced those in the prior year, increasing by 68%. Breaches involving personally identifiable information (PII), like Social Security numbers (SSNs), increased slightly from 80% to 83% in 2021.[1]

The healthcare industry rapidly moved to digital while the virtual work environment expanded. In 2021, nearly 50 million people in the U.S. faced a breach of their personal health information, the highest number to date. Healthcare data breaches have tripled over the past three years. The healthcare industry's move to digitized health records helped to accelerate these breaches.[2]

While the healthcare industry experienced numerous breaches, businesses in many industries have seen a rapid rise in ransomware and supply chain attacks. These increases helped contribute to the rise in the premiums charged for cyber insurance.[3]

Because of the increasing cybersecurity risks, businesses are facing a more demanding underwriting process. Insurers are more thoroughly examining a company's security controls, internal processes, and procedures concerning cyber risk. Additionally, underwriters are more cautious in examining an insured's risk presented by the third parties working or contracting with the insured.[4]

---

[1] Identity Theft Resource Center (ITRC). (2022). *Identity compromises: from the era of identity theft to the age of identity fraud.* www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[2] Leonard, B. (2022, March 23) *Health data breaches swell in 2021 amid hacking surge, POLITICO analysis finds*. POLITCO. https://www.politico.com/news/2022/03/23/health-data-breaches-2021-hacking-surge-politico-00019283

[3] Black Kite. (2022). A fight for coverage. *Cyber insurance risk in 2022.* https://blackkite.com/wp-content/uploads/2022/04/Black_Kite_CyberInsurance_Report_2022.pdf

[4] Woodruff Sawyer. (2022). *Cyber liability: Looking ahead to 2022*. https://woodruffsawyer.com/wp-content/uploads/2022/01/Cyber-Looking-Ahead-Guide-2022_Web.pdf

Virtual work, the increase in breaches of personal health information, ransomware, and supply chain attacks all contributed to the overall cyber insurance premium increases.[5]

Size of U.S. Cyber Insurance Market

The 2021 data shows a cyber insurance market, including both U.S. domiciled insurers and alien surplus lines insurers writing business in the U.S., of roughly $6.5 billion in direct written premiums. This reflects an increase of 61% from the prior year.

The chart below depicts the information collected from all years of data collection.

Year	Direct Written Premium Stand-Alone Cyber Policies - U.S. Domiciled Insurers (1)	Direct Written Premium Package Cyber Policies - U.S. Domicilied Insurers (2)	Direct Written Premium Stand-Alone Cyber Policies - Alien Surplus Lines Insurers (3)	Direct Written Premium Package Cyber Policies - Alien Surplus Lines Insurers (4)	Stand-Alone Policy Totals Direct Written Premium (All Insurers) (1+3)	Package Policy Totals Direct Written Premium (All Insurers) (2+4)	Total Direct Written Premium Written (1+2+3+4)
2015	483,197,973	932,645,734	*Not Reported	*Not Reported	483,197,973	932,645,734	1,415,843,707
2016	811,057,406	863,769,169	552,226,000	156,285,000	1,363,283,406	1,020,054,169	2,383,337,575
2017	994,259,551	896,424,050	765,129,000	431,423,000	1,759,388,551	1,327,847,050	3,087,235,601
2018	1,113,865,104	915,046,459	781,260,000	346,380,000	1,895,125,104	1,261,426,459	3,156,551,563
2019	1,263,214,669	998,799,630	890,627,667	204,230,452	2,153,842,336	1,203,030,082	3,356,872,418
2020	1,618,747,678	1,135,034,324	961,228,993	350,117,810	2,579,976,671	1,485,152,134	4,065,128,805
2021	3,151,977,648	1,675,285,505	1,385,498,876	330,414,781	4,537,476,524	2,005,700,286	6,543,176,810

NAIC Cybersecurity and Identity Theft Insurance Coverage Supplement

The Cyber Supplement requires U.S. domiciled insurers to report the following information on stand-alone cyber 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).

Total Premium Volume in Cyber Supplement

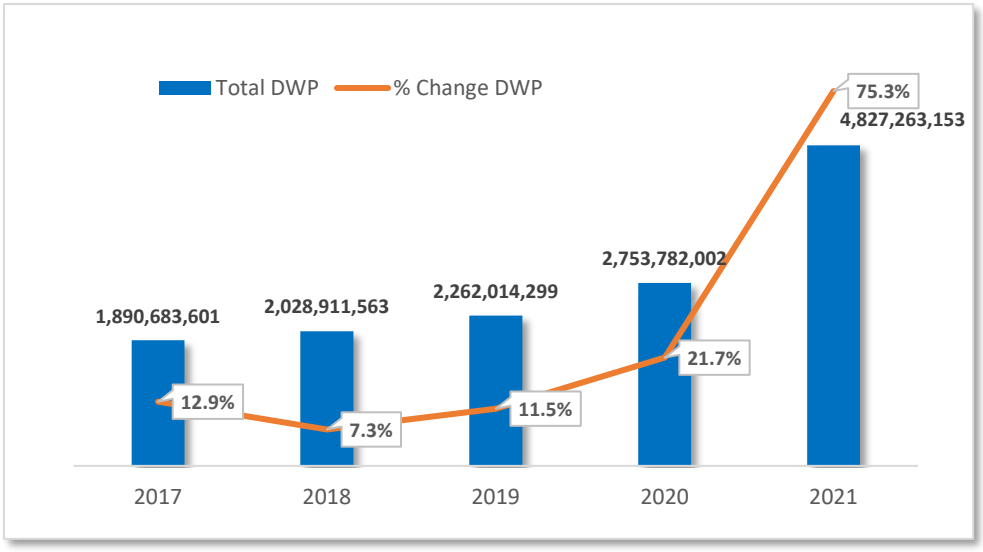
This year, 152 insurer groups representing 570 individual companies submitted data on the Cyber Supplement for the 2021 calendar year.

U.S. domiciled Insurers writing stand-alone cyber insurance products reported approximately $3.2 billion in direct written premiums, and those writing cyber insurance as part of a package policy reported roughly $1.7 billion in direct written premium.

U.S. domiciled insurers writing cyber coverage reported $4.8 billion in direct written premium in 2021. Direct earned premiums reported were $3.6 billion. Direct written premiums for the 2021 data year increased by 75.3% from the 2020 data year.

[5] Black Kite. (2022). *A fight for coverage Cyber insurance risk in 2022.* https://blackkite.com/wp-content/uploads/2022/04/Black_Kite_CyberInsurance_Report_2022.pdf

Figure 1. Direct Written Premium and Percent Change by Year (Does Not Include Alien Surplus Lines Data)



Loss Ratios

The top 20 groups reporting on the Cyber Supplement reported direct loss ratios in the range of -0.5% to 130.6%. Figure 2 depicts the average loss ratios over the past five years. The loss ratio for 2021 for the top 20 groups averaged 66.4%, down slightly from 66.9% in 2020.

Figure 2. Loss Ratios with Defense and Cost Containment (DCC) Stand-Alone and Package Policies Combined (Does Not Include Alien Surplus Lines)

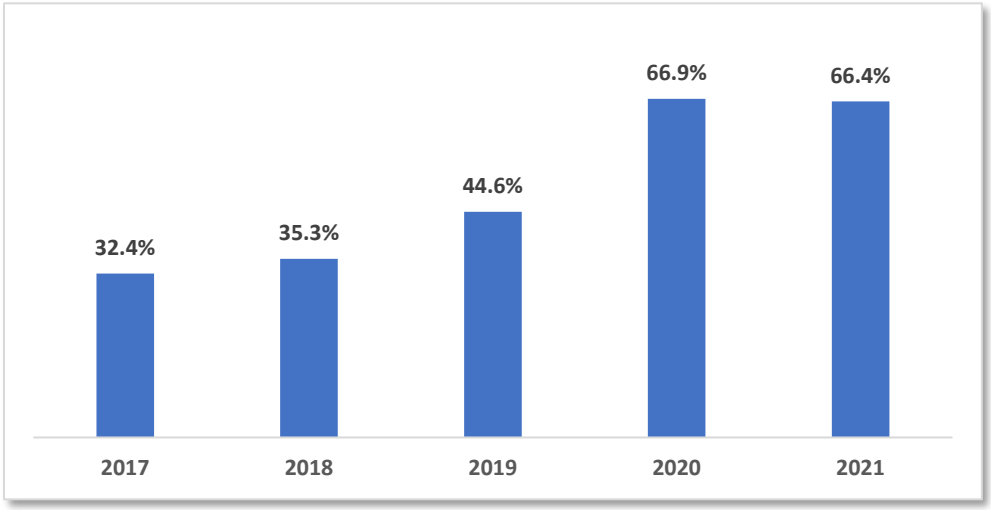


Exhibit 1 presents the loss ratios for the top 20 insurer groups. It is important to note that the cyber insurance market is still developing and growing. Increasing loss ratios in 2020 was one item triggering a substantial increase in premiums and premium growth in 2021, surpassing incurred losses. Current loss ratio improvements are apt to be linked to insurers' risk selection shifts and stricter policy terms and conditions.[6]

[6] Fitch Wire. (2022, April 13). *U.S. cyber insurance sees rapid premium growth, declining loss ratios*. https://www.fitchratings.com/research/insurance/us-cyber-insurance-sees-rapid-premium-growth-declining-loss-ratios-13-04-2022

Exhibit 1: Top 20 Admitted Groups (Does Not Include Alien Surplus Lines)

2021 Rank	2020 Rank	Group Number	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share
1	1	626	Chubb Ltd Grp	473,073,308	76.9%	9.8%
2	8	158	Fairfax Fin Grp	436,447,801	51.9%	9.0%
3	2	968	AXA Ins Grp	421,013,729	86.5%	8.7%
4	11	3098	Tokio Marine Holdings Inc Grp	249,785,218	43.8%	5.2%
5	3	12	American Intl Grp	240,613,748	130.6%	5.0%
6	*	3548	Travelers Grp	232,276,831	72.7%	4.8%
7	5	4942	Beazley Grp	200,877,555	38.7%	4.2%
8	7	218	CNA Ins Grp	181,382,785	87.5%	3.8%
9	*	1279	Arch Ins Grp	171,944,995	9.2%	3.6%
10	6	3416	AXIS Capital Grp	159,059,212	105.2%	3.3%
11	13	212	Zurich Ins Grp	151,865,004	76.9%	3.1%
12	14	111	Liberty Mut Grp	138,216,723	95.2%	2.9%
13	12	3219	Sompo Grp	133,519,577	54.3%	2.8%
14	10	23	BCS Ins Grp	132,043,119	80.1%	2.7%
15	*	91	Hartford Fire & Cas Grp	123,163,166	16.3%	2.6%
16	*	361	Munich Re Grp	119,989,106	69.0%	2.5%
17	20	181	Swiss Re Grp	103,827,837	32.7%	2.2%
18	*	501	Alleghany Grp	88,554,222	20.5%	1.8%
19	*	98	WR Berkley Corp Grp	81,249,260	36.9%	1.7%
20	16	31	Berkshire Hathaway Grp	71,365,401	-0.5%	1.5%

During 2021, the top 20 U.S. groups wrote 83% of the cyber insurance market, with written premiums totaling slightly more than $3.9 billion. In 2020, the top 20 groups wrote nearly the same percentage of the market. Six groups moved into the top 20 of market share in 2021 that were not among that group in 2020.

Standalone Policies Versus Package Policies

During 2021, insurers writing stand-alone cyber coverage reported approximately $3.2 billion in direct written premiums on the Cyber Supplement. The stand-alone cyber insurance direct written premiums for 2021 increased by 94.7% from the prior year, and the total number of stand-alone policies reported in 2021 increased by 31.8% from the number written in 2020.

The reported direct written premiums for cyber package policies totaled roughly $1.68 billion, which is an increase of 47.6% from the prior year, and the total number of package policies reported in 2021 decreased by 8.7%

Ransomware and Supply Chain

Ransomware attacks continue to escalate, growing by nearly 93% in 2021.[7] As ransomware increases in frequency and severity, it continues to pose a significant threat.[8] To date, the highest ransom paid was just under $40 million. The ransom was paid by an insurer. Notably, insurers are at risk for ransomware attacks, as they are generally large organizations holding a great deal of data. [9]

[7] Security. (2022, Feb. 28). *Ransomware attacks nearly doubled in 2021.* https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021

[8] Patel, R. (2022, Aug. 22). Ransomware attacks hit two out of three organizations in 2021: Here's what you need to know.*Forbes.* https://www.forbes.com/sites/forbestechcouncil/2022/08/22/ransomware-attacks-hit-two-out-of-three-organizations-in-2021-heres-what-you-need-to-know/?sh=768e050a65cf

[9] Bisson, D. (2021, Aug. 6). *Ransomware costs expected to reach $265 billion by 2031*. Security Intelligence. https://securityintelligence.com/news/ransomware-costs-expected-265-billion-2031/

Most businesses use third-party vendors, suppliers, or other types of providers. Frequently, these third parties have access to a company's information system. When a cybercriminal infiltrates a company's information system through a third party, it is called a supply chain attack.[10]

There are two types of supply chain attacks: 1) software supply chain attacks; and 2) hardware supply chain attacks. In the case of a software supply chain attack, cybercriminals insert some type of malicious code into software, causing all users of the software to be infected.[11] Hardware, a physical component, is compromised for the same purpose. Companies producing both hardware and software may be targeted by cybercriminals.[12]

Poor security practices by a third party in a supply chain may compromise a company's own security system. For this reason, businesses should use due diligence when evaluating the security of the third parties they use.[13]

The supply chain of cyber insurance is susceptible to a data breach or ransomware attack.[14] Of the numerous ransomware attacks occurring in 2021, supply chains and critical infrastructures became cybercriminals' targets.[15] Supply chain attacks rose by 430% in 2021.[16]

Cyber Insurance Underwriting and Rating Changes

Starting in 2020, cyber insurance began moving towards a hard market. This trend continued throughout 2021 and into 2022. Insurers responded to the hard market, in part, by increasing premiums.[17] The direct written premiums in the admitted market rose by 74% in 2021. Insurers saw a reduction in their loss ratios, in part because of premium increases.[18] Regardless of a company's size or industry segment, companies continued to see their premiums increase during the first quarter of 2022.[19]

There are multiple reasons for rising cyber insurance premiums. Cyber insurers began experiencing increasing loss ratios, primarily because of sizable claims payments for ransomware attacks. Claims payments also included business interruptions due to the attacks.[20] Social engineering, where a criminal deceives a person in order to gain access to confidential information, has become a top cyber security threat. Additionally, companies are not effectively managing third-party risk. In response, underwriters have begun analyzing supply chain networks more exhaustively to ensure sufficient security procedures are in place.[21]

Underwriting is evolving, and insurers are becoming more cautious when examining an insured's risk and the risk presented by third parties with whom they work and contract. Underwriters are reviewing a company's internal security controls and cyber-risk procedures with more scrutiny.

---

[10] Korolov, M. (2021 Dec 27). Supply chain attacks show why you should be wary of third-party providers. CSO. https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

[11] CrowdStrike. (2021, Dec. 8). *What is a supply chain attack?* https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

[12] Korolov, M. (2021 Dec 27). Supply chain attacks show why you should be wary of third-party providers. CSO https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

[13] Newton, E. (2022, Jan. 17). *The supply chain needs better cybersecurity and risk management.* Tripwire. https://www.tripwire.com/state-of-security/controls/the-supply-chain-needs-better-cybersecurity-and-risk-management/

[14] Black Kite. (2022). *A fight for coverage:* Cyber *insurance risk in 2022.* https://blackkite.com/wp-content/uploads/2022/04/Black_Kite_CyberInsurance_Report_2022.pdf

[15] Munich Re Global Cyber Risk and Insurance Survey 2022

[16] CrowdStrike. (2021, Dec. 8). *What is a supply chain attack?* https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

[17] Puckett, L. & Stachura, M., (2022). Spring/Summer Insurance Market Report *Cyber Where We Were: What We've Been Through Q1 2022.*

[18] Rundle, J & Uberti, D. (2022, May 18). *Cyber insurers raise rates amid a surge in costly hacks.* https://www.wsj.com/articles/cyber-insurers-raise-rates-amid-a-surge-in-costly-hacks-11652866200

[19] Puckett, L. & Stachura, M., Authors. Spring/Summer Insurance Market Report (2022 May) *Cyber Where we Were: What We've Seen Through Q1 2022.*

[20] Jones, N. (2022, March 18). *6 reasons cyber insurance prices are on the rise.* Egnyte. https://www.egnyte.com/blog/post/why-are-cyber-insurance-costs-on-the-rise

[21] Ibid

Insurers are implementing more restrictive coverage terms within cyber insurance policies. Additionally, insurers are prohibiting some prevalent cyber incidents and including mandatory sublimits. These steps indicate insurers are not wanting to bear the entire cost of a ransomware incident.[22]

The underwriting process is becoming more stringent, and it is likely premiums will continue to increase. To offset the increased cost of cyber insurance, policyholders may begin to take on higher self-insured retentions. This may also drive businesses to take on a more significant role in managing their cybersecurity risk.[23] Cyber insurance is one option available to address risk. However, underwriters do not believe that buying additional cyber insurance should be used as an instrument to alleviate risk.[24]

Additionally, Insurers are writing less business to help control their exposures.[25] 2021 brought about another decrease in available cyber insurance limits. These limits were often reduced to $1 million – $3 million, even at renewal.[26] For a company to retain the same policy coverages, it is forced to obtain more policies in order to keep the same coverage it carried in the previous year. [27]

Ransomware coverage will likely continue to have sublimits to limit the effect of cyber extortion on insurers. Overall, the modifications discussed in this section were needed to preserve a healthy cyber market in the coming years.[28] Expansion of the cyber insurance market may occur in 2023. This is due to declining loss ratios and better criteria for evaluating risk.[29]

Reinsurance

At the rate cyber insurance is growing, the market is on track to double in size every three years.[30] While more capacity is anticipated to enter the cyber reinsurance market, it is currently insufficient.[31] It is estimated that about 50% of cyber insurance premiums are ceded to the reinsurance market.[32]

Concerns like systemic risk, ransomware, modeling complexity around cyber risks, pricing, and profitability prompted the reinsurer's reluctance to participate in the cyber-reinsurance market. As insureds have implemented better cyber hygiene, ransomware loss frequency has declined, reducing some of this hesitancy.[33]

Summary

Demand for cyber insurance is growing. Marsh and McClennan indicated that the cyber insurance take-up rates for their clients in 2021 were at 50%, which is a 3% increase from the 2020 take-up rates.[34] While businesses are aware

[22] Puckett, L. & Stachura, M., (2022). Spring/Summer Insurance Market Report *Cyber Where We Were: What We've Been Through Q1 2022.*
[23] Ibid
[24] Black Kite. (2022). A fight for coverage: *cyber insurance risk in 2022.* https://blackkite.com/wp-content/uploads/2022/04/Black_Kite_CyberInsurance_Report_2022.pdf
[25] CY-FI The Future of Cyber (Re)insurance. (2022). https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf
[26] U.S. Cyber Market Outlook. (2021) https://www.rpsins.com/learn/2021/oct/us-cyber-market-outlook/
[27] Rundle, J & Uberti, D. (2022, May 18). *Cyber insurers raise rates amid a surge in costly hacks.* https://www.wsj.com/articles/cyber-insurers-raise-rates-amid-a-surge-in-costly-hacks-11652866200
[28] Risk Placement Services. (2021). *U.S. cyber market outlook*. https://www.rpsins.com/learn/2021/oct/us-cyber-market-outlook/
[29] Hall, J, Newman, I, & Peacock, E. (2022). *CY-FI: The future of cyber (re)insurance*. Gallagher Re. https://www.ajg.com/gallagherre/news-and-insights/2022/february/future-of-cyber-reinsurance/
[30] CY-FI The Future of Cyber (Re)insurance. (2022). https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf
[31] https://www.guycarp.com/insights/2022/06/guy-carpenter-erica-davis-discusses-capacity-capital-cyber-insurance-article.html
Cyber Insurance Market Overview: Fourth Quarter 2021. (2021 Dec. 7) https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html
[32] CY-FI The Future of Cyber (Re)insurance. (2022). https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf
[33] https://www.businessinsurance.com/article/20220614/NEWS06/912350516/Worst-may-be-over-for-tough-cyber-reinsurance-market
[34] https://www.insurancebusinessmag.com/us/news/breaking-news/cyber-insurance-why-marsh-has-cautious-optimism-for-the-rest-of-2022-414472.aspx

that cyber risk is a looming issue, it is not uncommon for policyholders to believe their current business insurance policy covers a cyber loss.[35]

More insurers have moved into the cyber insurance market. However, insurers with a consistently stable market presence are reducing capacity management restrictions and expanding the amount of business they can write. New entrants have generated an excess capacity of around $50 million.[36]

The war in Ukraine poses systemic risks and risks related to the supply chain. These risks have amplified concerns regarding aggregation. Insurers continue to examine war exclusions, territory restrictions, systemic risk, and secondary coverages like cybercrime or theft.[37]

While pricing disruptions are occurring in some industry sectors more than others, the abrupt increase in cyber premiums appears to be slowing. Assuming capacity expands and loss performance improves, the cyber insurance market in 2022 holds promise for those purchasing cyber insurance.[38]

Data analyzed for this report show that the cyber insurance market is growing rapidly, though much of that growth has likely been due more to premium rate increases than increases in take-up rates or broadening coverage. Regulators continue to assess the market in terms of how insurance is providing protection to policyholders.

In terms of future data collection, the Property and Casualty Insurance (C) Committee is considering strengthening the Cyber Supplement's instructions, providing insurers with more guidance for filing the *NAIC Property/Casualty Annual Statement Blank*. Additionally, there will likely be changes to the collection of policies on a claims-made or occurrence basis in the Cyber Supplement. The NAIC finds many insurers incorporate both into their policies. Such changes can improve the quality and utility of the data received, thus enhancing future analyses of the cyber insurance market.

[35] *https://www.securitymagazine.com/articles/97724-the-value-of-cyber-insurance-for-small-businesses#:~:text=It's%20common%20for%20small%20businesses,coverage%20in%20a%20grey%20area.*
[36] E&O and Cyber Market Review. (2022). https://www.aon.com/insights/articles/2022/eo-cyber-market-review-midyear-2022
[37] ibid
[38] ibid