NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Property and Casualty Insurance (C) Committee

FROM: NAIC Staff

DATE: November 3, 2023

RE: Report on the Cybersecurity Insurance Market

The NAIC collects data from insurers writing cybersecurity insurance through its *Property/Casualty Annual Statement Cybersecurity and Identity Theft Supplement* (Cyber Supplement). Supplement data have been collected since 2016, and alien surplus lines data was collected beginning in 2017. This report focuses on the cybersecurity insurance market by presenting data found within the Cyber Supplement and alien surplus lines data collected through the NAIC's International Insurers Department (IID). This data includes data from Lloyd's of London, as well as non-U.S. insurers.

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

Overview

The U.S. continues to account for the largest percentage of cyber insurance, with 56% of premiums written on affirmative cyber insurance.[1]

Protection against cyber-attacks continues to be important for businesses, and small businesses are no exception. Since 2022, small businesses have experienced a 28% increase in cyberattacks.[2]

Insurers writing cyber insurance continue updating their application process to ensure insureds manage risk and implement appropriate controls. The maturing cyber insurance market has seen insurers better recognize cyber threats and the elements of risk they wish to insure[3].

In 2022, the healthcare industry was most vulnerable to cyberattacks and experienced the most cyberattacks during the first half of 2023.[4] However, the financial services sector was not far behind. During the first quarter of 2023, healthcare saw 81 compromises and financial services saw 70 compromises. The attack vectors during the first quarter included cyberattacks, system and human errors, physical attacks, and supply chain attacks.[5]

Additionally, healthcare and public health experienced the costliest data breaches in 2022.[6] As with other industries, healthcare is challenged by third-party data breaches as healthcare organizations use more third-party providers to manage administrative functions.[7]

All sectors of business face dynamically changing cybersecurity risks. Therefore, underwriters continue to react, and expect insureds to have the appropriate security controls, internal processes, and procedures in place for cyber risk.

---

[1] S & P Global
[2] https://www.idtheftcenter.org/wp-content/uploads/2023/10/ITRC_2023-Business-Impact-Report_V2.1-3.pdf
[3] https://www.rpsins.com/-/media/files/rpsins/rpsins/learn-articles/rps-2023-cyber-market-outlook.pdf
[4] ibid
[5] https://www.idtheftcenter.org/wp-content/uploads/2023/04/20230413_Q1-2023-Data-Breach-Analysis.pdf
[6] https://www.beyondidentity.com/blog/data-breaches-are-more-costly-these-10-industries
[7] https://www.hipaajournal.com/2022-healthcare-data-breach-report/

Total Premium Volume

This year, 151 insurer groups, representing 629 individual companies submitted data on the Cyber Supplement for the 2022 calendar year.

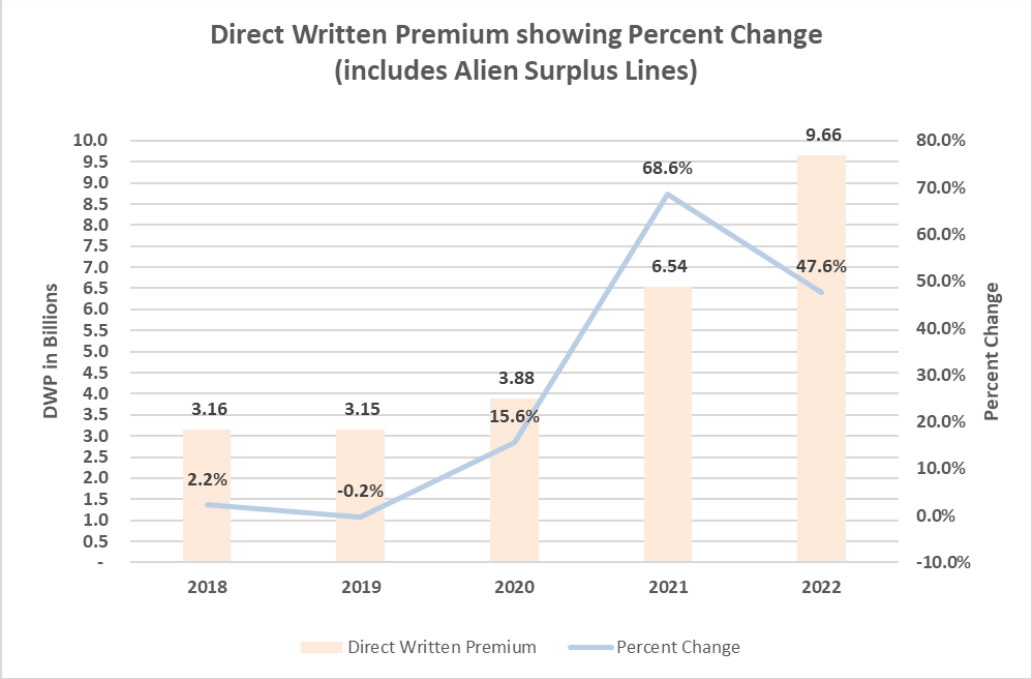
The 2022 data show a cybersecurity insurance market, including U.S. domiciled insurers and alien surplus lines insurers writing business in the U.S., of roughly $9.7 billion in direct written premiums, reflecting an increase of 47.6% from the prior year.

U.S. domiciled insurers writing cyber coverage reported approximately $7.2 billion in direct written premiums in 2022. Direct earned premiums reported were $6.3 billion. Direct written premiums for the 2022 data year increased by 49.9% from the 2021 data year. The differences in direct written premiums in the cyber insurance market have been dramatic in the past couple of years. The continued rise in ransomware and the number of costly cybersecurity events partly drove the increase in cyber insurance premiums in 2021. While cyber insurance prices grew in 2022, they grew at a slower rate.

Alien surplus lines insurers reported approximately $2.4 billion in direct written premiums in 2022, which is an increase of 41.1% from 2021.

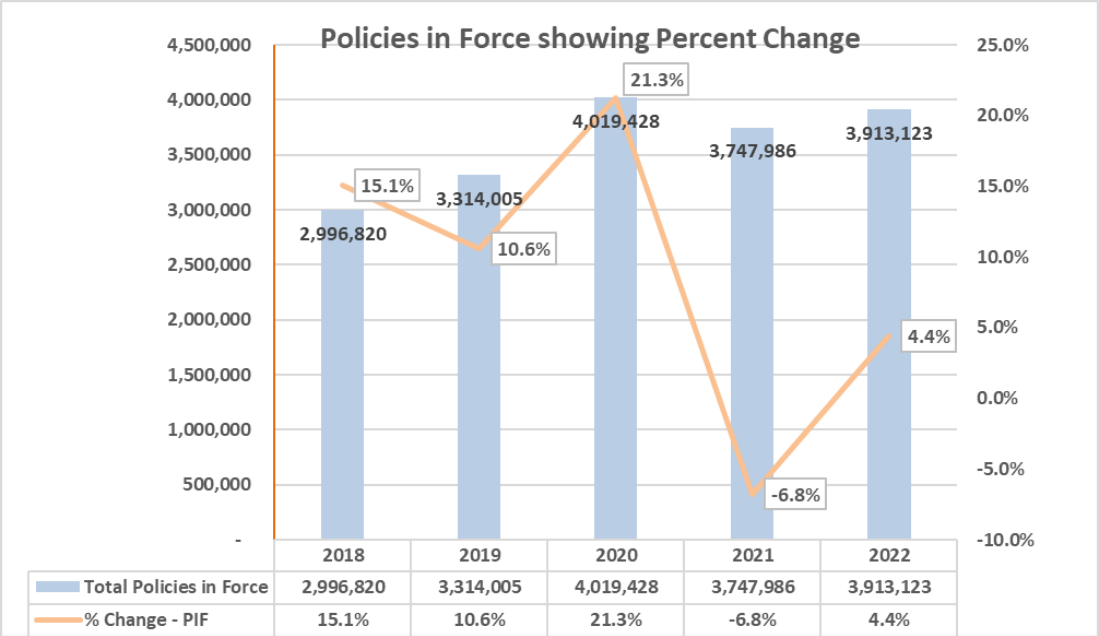
Figure 1 shows the domestic direct written premium from 2018 to 2022 and the yearly percent change. These numbers contain the domestic surplus lines, the admitted market, and the alien surplus lines market.

Figure 1: Direct Written Premium and Percent Change by Year



While the direct written premium increased in 2022, it did not rise at the same rate as the policies in force. The number of policies in force in the admitted and domestic surplus lines market grew by 4.4% from 2021 to 2022. However, it is worth noting that fewer cyber insurance policies were in force in 2021 and 2022 than in 2020. Figure 2 illustrates the number of policies in force from 2018 to 2022 and the rate of change by year. This figure does not include the number of policies in force in the alien surplus lines market.

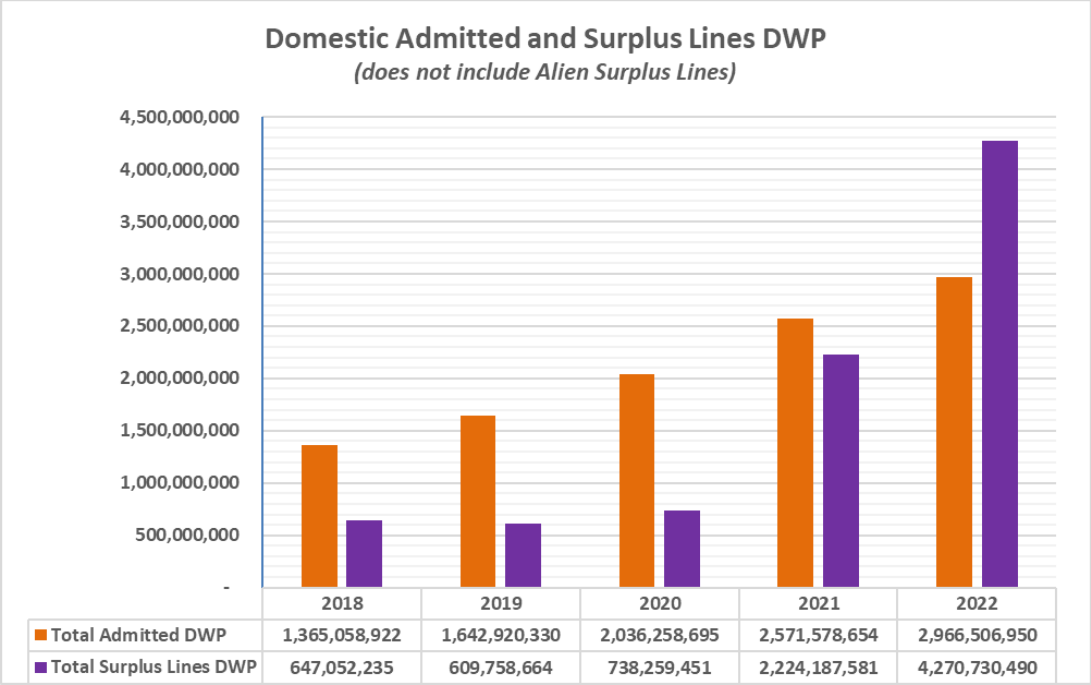
Figure 2: Policies in Force and Percent Change by Year*



Does not include Alien Surplus Lines Data

The domestic surplus lines market writes approximately 41% of the U.S. cyber insurance market, while the admitted market writes about 59% of the market. Figure 3 illustrates the growth trends of the domestic admitted and surplus lines market.

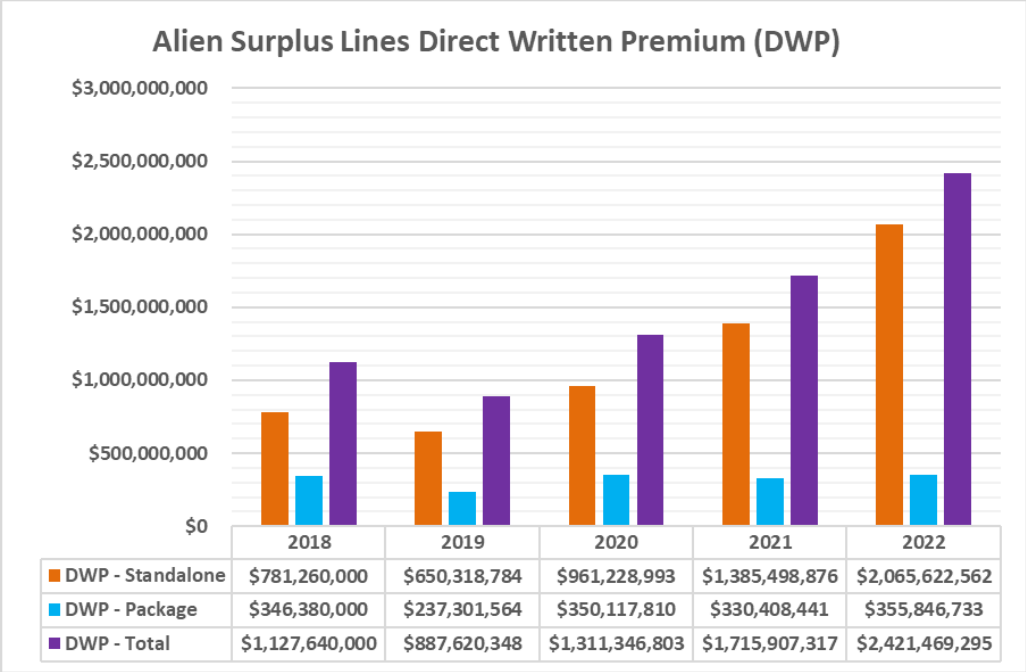
Figure 3: Direct written premium in the domestic admitted and surplus lines market*



Does not include alien surplus lines data

Figure 4 illustrates the direct written premium from 2018 to 2022 for standalone policies, package policies, and the total direct written premium for the alien surplus lines market. The direct written premium decreased in 2018 and 2019 but began increasing in 2020. Direct written premiums grew by 41.1% in 2022.

Figure 4: Direct Written Premiums for Alien Surplus Lines 2018–2022



	2018	2019	2020	2021	2022
DWP - Standalone	$781,260,000	$650,318,784	$961,228,993	$1,385,498,876	$2,065,622,562
DWP - Package	$346,380,000	$237,301,564	$350,117,810	$330,408,441	$355,846,733
DWP - Total	$1,127,640,000	$887,620,348	$1,311,346,803	$1,715,907,317	$2,421,469,295

Figure 5 shows the percentage of admitted, domestic surplus lines, and alien surplus lines markets that are held by the U.S. market. The U.S. admitted market holds 38.5% of the market, followed by the U.S. domestic surplus lines market, holding 36.4% of the market. Alien surplus lines account for 25.1% of the market.

Figure 5: Market Type Percentages

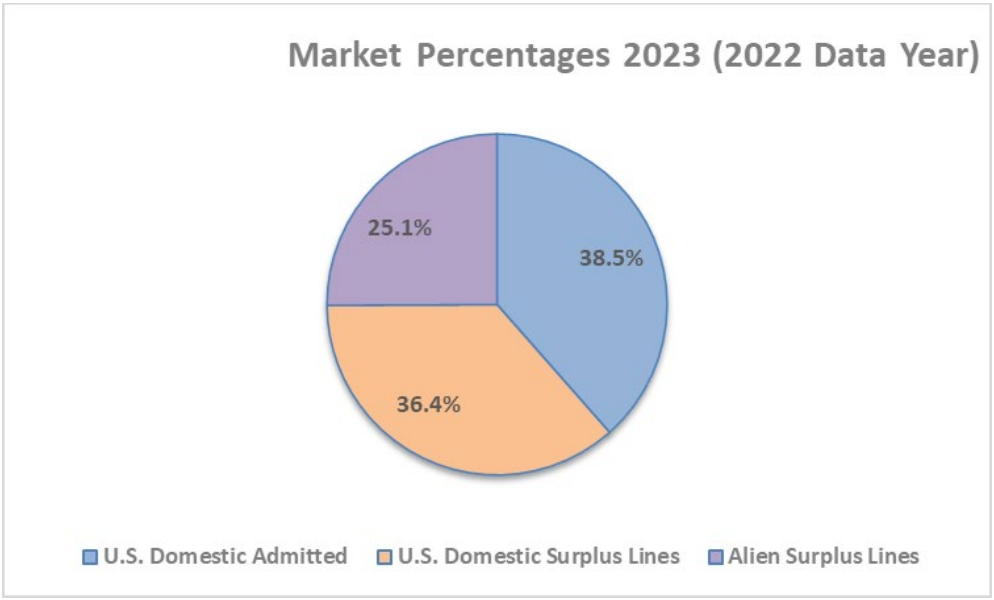
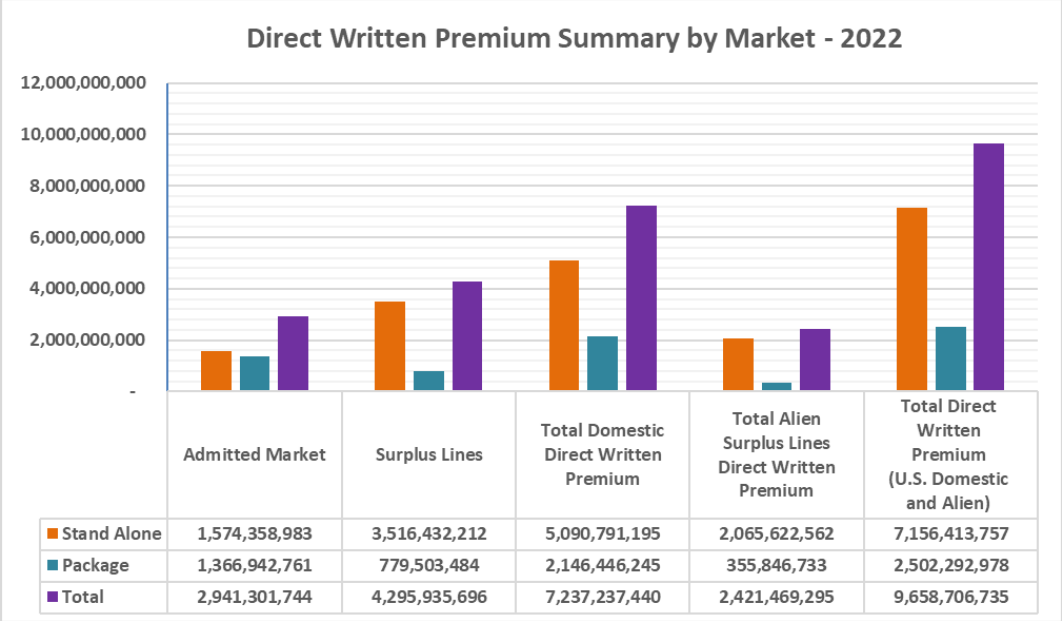


Figure 6 shows the market summary for the admitted and domestic surplus lines premiums, as well as the alien surplus lines premiums.

Figure 6: Market Summary



	Admitted Market	Surplus Lines	Total Domestic Direct Written Premium	Total Alien Surplus Lines Direct Written Premium	Total Direct Written Premium (U.S. Domestic and Alien)
Stand Alone	1,574,358,983	3,516,432,212	5,090,791,195	2,065,622,562	7,156,413,757
Package	1,366,942,761	779,503,484	2,146,446,245	355,846,733	2,502,292,978
Total	2,941,301,744	4,295,935,696	7,237,237,440	2,421,469,295	9,658,706,735

Loss Ratios

The top 20 groups in the cyber insurance market reported direct loss ratios in the range of 10.7% to 85.9% in 2022. The loss ratio for 2022 for the top 20 groups averaged 44.6%, down from 66.4% in 2021.

Exhibit 1 presents the direct written premium and loss ratios for the top 20 insurer groups. It is important to note that the cybersecurity insurance market is still developing and growing. Increasing loss ratios in 2020 and 2021 were partly responsible for triggering a substantial increase in premiums and premium increases in 2021 and 2022. Current loss ratio improvements can be linked to insurers' risk selection shifts and stricter policy terms and conditions.[8]

[8] Fitch Wire. (2022, April 13) US 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*

2022 Rank	2021 Rank	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share	Cumulative Market Share
1	1	Chubb Ltd Grp	604,926,658	53.8%	8.6%	8.6%
2	2	Fairfax Financial	562,995,303	54.0%	8.4%	17.0%
3	3	AXA Ins Grp	527,441,693	66.2%	8.0%	24.9%
4	4	Tokio Marine Holdings Inc GRP	367,607,130	57.8%	5.1%	30.0%
5	9	Arch Ins Grp	346,374,212	52.3%	4.3%	34.3%
6	6	St Paul Travelers Grp	315,324,617	34.8%	4.4%	38.7%
7	5	American Intrnl Grp	299,011,690	47.6%	4.2%	43.0%
8	34	Nationwide Corp	257,312,784	12.5%	3.7%	46.6%
9	11	Zurich Ins Grp	252,514,546	68.2%	3.8%	50.4%
10	13	Sompo Grp	247,978,386	50.1%	3.1%	53.5%
11	8	CNA Ins Grp	228,933,184	26.5%	3.4%	56.9%
12	20	Berkshire Hathaway	228,495,397	48.1%	3.3%	60.2%
13	12	Liberty Mut Grp	208,204,580	57.5%	2.9%	63.2%
14	17	Swiss Re Grp	207,013,991	19.6%	2.9%	66.1%
15	10	AXIS Capital Grp	195,746,593	85.9%	1.5%	67.6%
16	7	Beazley Grp	174,628,461	19.6%	2.9%	70.5%
17	22	Ascot Ins US Grp	166,556,438	30.2%	1.8%	72.3%
18	32	Randall & Quilter Investment Grp	161,653,538	10.7%	1.9%	74.3%
19	27	Markel Corp Grp	152,886,167	40.1%	1.4%	75.7%
20	15	Hartford Fire & Cas Grp	152,339,006	15.5%	2.2%	77.9%

**Does not include alien surplus lines*

In 2022, the top 20 U.S. groups wrote 77.9% of the cyber insurance market, while in 2021, the top 20 groups wrote 83% of the market. Beyond the top four groups, some of the insurers writing in the cyber insurance market in 2022 have shifted rank.

Standalone Policies Versus Package Policies—U.S. Domiciled Insurers

During 2022, insurers writing standalone cyber coverage reported approximately $5.1 billion in direct written premiums. The standalone cybersecurity insurance direct written premiums for 2022 increased by 61.5% from the prior year, and the total number of standalone policies reported in 2022 increased by 31.8% from those written in 2021.

The reported direct written premiums for cybersecurity package policies totaled roughly $2.1 billion, which is an increase of 28.1% from the prior year, and the total number of package policies reported in 2022 increased by 4.9%

Ransomware

Cyberattacks and the use of ransomware continue to increase, albeit there have been short periods of a slowdown in the use of ransomware.

Ransomware attacks increased in 2022, prompting businesses to purchase cyber coverage and implement stronger cybersecurity controls.[9] Artificial intelligence (AI) adds to the complexity of the expanding cyber world as new exposures continue to arise.[10] Cybercriminals have utilized ChatGPT and other platforms to build their own large learning models (LLMs). Additionally, threat actors are using some of the non-existent libraries recommended by ChatGPT, by infiltrating the suggested resources with malicious capabilities.[11]

[9] Cyber Insurance Premiums Surge by 50% as Ransomware Attacks Increase. Muñoz, Marnie (AUTHOR) Bloomberg.com. 6/14/2023, pN.PAG-N.PAG. 1p."
[10] (AM Best)
[11] https://www.securitymagazine.com/articles/100009-first-half-of-2023-sees-more-ransomware-victims-than-all-of-2022

More refined cyberattacks have led to a shift in how cybercriminals approach ransomware attack negotiations. Currently, if a business receives ransomware and does not pay the ransom or involves a forensic firm, the trend is for cyber criminals to delete or sell data on the dark web. Cybercriminals want to stop a business' operation, so they focus on attacks that inhibit a company from operating.[12]

Ransomware as a Service (RaaS) has complicated the ransomware problem. RaaS allows bad actors to buy subscriptions to utilize already-developed ransomware tools. In return, the subscriber pays a percentage of the ransomware collected to develop the ransomware programs.[13]

Data Compromise Trends

While 2022 saw fewer data compromises, 2023 had surpassed the record set in 2021 by the end of September. The rising number of these compromises is partly due to a sharp rise in zero-day attacks. A zero-day attack takes advantage of an unidentified vulnerability that a person in charge of a network would not know to patch or fix. Those in charge of fixing vulnerabilities or flaws have zero days to do so. The number of breaches reported and the number of people affected is likely higher than reports show.[14]

Since 2019, trends show less reporting of complete details concerning data breaches, making the data less definitive. The missing information surrounding data compromise results in entities and individuals needing help to make important decisions about assessing the risk of a data compromise. Additionally, following a data compromise, the lack of information regarding data breaches limits an entity's ability to take appropriate actions.[15]

Cyber Insurance Underwriting and Rating Changes

As the cyber insurance market has matured, insurers have refined their underwriting approach. They better understand the threats and the type of cyber risk they want to insure. Of course, the higher an organization's revenue, the more system security an underwriter requires.[16]

While the cyber insurance market hardened in 2020 and 2021, the market is beginning to see some correction. In 2022 and into 2023, cyber insurance prices were beginning to stabilize.[17] Direct written premiums in the admitted market increased by approximately 50% in 2022, whereas premiums increased by slightly more than 75% in 2021. The number of policies in force decreased by 6.8% in 2021, whereas they increased by 4.4% in 2022.

To limit their exposures, insurers are implementing endorsements around security measures. For example, one of these endorsements references critical known vulnerabilities in the National Vulnerability Database (NVD). The insured initially has 30 to 45 days to patch the vulnerability without seeing their cyber coverage affected. Coverage restrictions occur and increase every month following the initial grace period. Additionally, some endorsements may incorporate coinsurance.[18]

Insureds increased their self-insured retentions (SIR) due to premium increases in early 2022. However, as premiums became more reasonable, brokers began to see insureds decrease their SIRs.[19]

Insurers continue implementing more restrictive coverage terms for cybersecurity insurance policies for certain cyber risks. With the increase in frequency and severity of cyber insurance claims, insurers are beginning to add lower sublimits into their policy wording. Sublimits can be as low as $100,000 or as high as $1,000,000, depending on the insurance policy. Some policies also add a lower aggregate limit and a sublimit for an event triggered by ransomware.[20]

---

[12] https://www.rpsins.com/-/media/files/rpsins/rpsins/learn-articles/rps-2023-cyber-market-outlook.pdf
[13] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
[14] https://www.idtheftcenter.org/wp-content/uploads/2023/07/20230712_H1-2023-Data-Breach-Analysis.pdf
[15] https://www.idtheftcenter.org/wp-content/uploads/2023/10/ITRC_2023-Business-Impact-Report_V2.1-3.pdf
[16] https://www.rpsins.com/-/media/files/rpsins/rpsins/learn-articles/rps-2023-cyber-market-outlook.pdf
[17] ibid
[18] ibid
[19] https://www.marsh.com/us/services/cyber-risk/insights/us-cyber-purchasing-trends.html#:~:text=Cyber%20insurance%20pricing%20increases%20moderated,likely%20to%20purchase%20cyber%20insurance
[20] https://www.rpsins.com/-/media/files/rpsins/rpsins/learn-articles/rps-2023-cyber-market-outlook.pdf

Reinsurance

S&P Global believes that reinsurers will continue to play an essential role in developing a viable cyber insurance market. In 2022, primary cyber insurers in the United States ceded slightly more than 50% of their cyber insurance premiums to reinsurers. The reinsurance market will play a significant role in supplying capital and capacity supporting additional premium growth. Using Guidewire's Cyence model, S&P concluded that the reinsurers they rate would not have a huge impact on their capital.[21] In 2022, reinsurers experienced low profitability. Additionally, these reinsurers faced underwriting losses in their cyber insurance portfolios; loss ratios slightly exceeded 100%, falling short of primary cyber insurance writers.[22]

S&P noted cyber insurance heavily depends on reinsurance and believes reinsurers will continue to play a significant role in the cyber insurance market's growth. While the primary cyber insurance market begins to soften, this may not be the case for reinsurance. Reinsurers have made higher rate adjustments throughout the first half of 2023.[23]

However, primary cyber insurance underwriters likely will be able to keep from passing the increased reinsurance costs on to policyholders.[24]

Exclusions

Like any other insurance policy, cyber insurance uses exclusions and coverage limitations to limit exposure.

Most cyber insurance policies typically include a retroactive date. A retroactive date specifies the length of time a policy will cover a loss based on this date on a claims-made policy. A policy will not cover a claim occurring before the retroactive date. Businesses must ensure the retroactive date makes sense when purchasing a cyber insurance policy.[25]

Losses occurring from an act of war are typically excluded. However, many insurers make exceptions for cyber terrorism. The wording in exclusions should be read carefully to avoid any gaps in coverage, and the insured may want to purchase separate coverage for cyber warfare, cyber extortion, etc.[26]

A cyber policy may also exclude bodily injury and loss or damage to property, including computer hardware. Other types of policies, such as property or liability policies, typically cover these types of loss. However, some cyber insurance policies may provide extended coverage for property or liability losses if the damage is due to a cyber event. Extended coverage generally applies when a business has exposure to bodily injury or physical property damage due to a cyber event.[27]

If critical national infrastructure fails, cyber insurance ordinarily is not covered under a cyber insurance policy. According to the Cybersecurity & Infrastructure Security Agency (CISA), critical infrastructure includes those assets, systems, and networks that provide functions necessary for the way of life. It is important that a business understands the items that are and are not covered under its cyber insurance policy.[28]

Failure to maintain security measures is another common exclusion to cyber insurance policies. An insurance policy's terms may require an insured to maintain appropriate procedures and controls to protect against cyberattacks. For example, insurers may require an insured to use two-factor authentication and patch its computer systems in an acceptable timeframe. A company may wish to hire a professional to help with the complicated process of applying for cyber insurance.[29]

[21] https://www.spglobal.com/ratings/en/research/articles/230829-global-cyber-insurance-reinsurance-remains-key-to-growth-12813411
[22] https://www.carriermanagement.com/news/2023/08/30/252566.htm
[23] https://www.spglobal.com/ratings/en/research/articles/230829-global-cyber-insurance-reinsurance-remains-key-to-growth-12813411
[24] ibid
[25] https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/navigating-common-exclusions-in-cyber-policies
[26] ibid
[27] ibid
[28] ibid
[29] ibid

Cyber events and losses usually cross state or country borders. This means an insured will want to be sure which countries and territories the cyber insurance policy covers. If a particular country or territory in which an insured requires coverage is excluded from a cyber insurance policy, this coverage should be discussed with the insurer.[30]

This list of exclusions is not meant to include every possible exclusion. However, the exclusions discussed are common exclusions insureds see when purchasing a cyber insurance policy.

Summary

The cyber insurance market continued to be challenged in 2022. However, the market is starting to show signs of improvement. The take-up rates for cyber insurance coverage increased and continue to grow. Additionally, cyber insurance remains an essential part of a business's risk management strategy.[31]

While insureds are seeing lower premiums during the first half of 2023, it is important to note that insurers are tightening policy language and restricting coverage by exclusions.

Insureds are also held more accountable for their cyber hygiene to receive coverage. The application process has become more complex, which includes endorsements that reduce coverage if businesses do not patch known vulnerabilities in a timely manner.

Technology is ever-changing, making cyber insurance a dynamic product. As technology changes, businesses need to have coverage to meet these emerging changes. However, at the same time, insurers must determine the amount of risk they wish to undertake.

[30] ibid

[31] https://www.insurancejournal.com/news/national/2023/05/15/720816.htm#:~:text=The%20overall%20take%2Dup%20rate,%2C%20with%20healthcare%20at%2056%25.