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

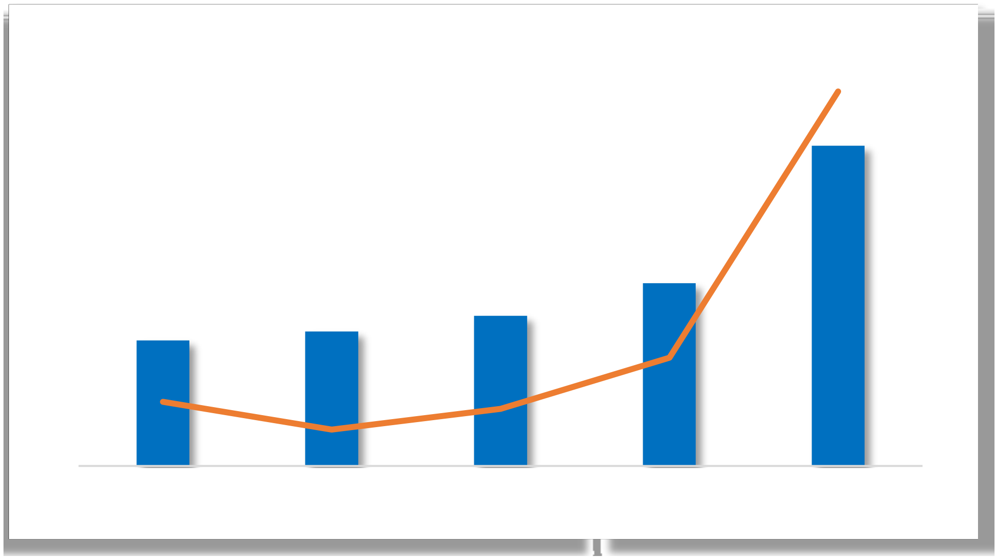
The 2021 data shows a cyber insurance market, including both U.S. domiciled insurers and alien surplus lines insurers writing business in the U.S., of roughly $6.5 billion in direct written premiums. This reflects an increase of 61% from the prior year.

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

NAIC Cybersecurity and Identity Theft Insurance Coverage Supplement

a ac aow

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

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.

1 1.02;

Insurers are implementing more restrictive coverage terms within cyberinsurance 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]

of*reB7cu2C 27of*reB7cu2C 27

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
2.6 6s)-1)9[(s-3/(e5cu)5i)ac)e6as(s a)t2gJT(h0)2.1)(fG-6s/(e52b)5a.9 d (r)3r)6(1)2t(up-l6t5(y a)e)98(e C2.12h)-6.12r5-1.6(h)e1//6e1h/ce