Cyber Insurance:
State of the Risk

INSURANCE INFORMATION INSTITUTE
Affiliated with The Institutes

Market continues rapid growth in face of increasing need for customer risk management.

Despite making up an estimated 1 percent of U.S. property/casualty insurance premiums in 2022, cyber insurance is expected to continue to be one of the fastest-growing segments in P/C. Two primary factors may be at work:

- The ubiquitous threat of data breaches and cyber-attacks
- Insurers have made strides in clarifying policy coverage and exclusions, improving risk managers' understanding of product value and helping insurers better manage costs and rate stability

The global cyber insurance market tripled in volume in the last five years to gross direct written premiums of $13 billion in 2022, according to the Swiss Re Institute (SRI). Market growth is expected to boost premiums to $23 billion by 2025. Re-insurers heavily support this market by providing capital and increased capacity to deal with accumulation risk, according to S&P Global. Across global reinsurance groups, the gross combined ratio was 107 percent and the net combined ratio 101 percent in 2022 for the cyber business they reinsured.

AM Best's analysis of the U.S. market in "U.S. Cyber: First Hard Market Cycle Brings a Return to Profitability" shows standalone direct premiums written (DPW) jumping by 50 percent YoY in 2022 to $7.2 billion. Loss ratios also improved in 2022 from 2021, with a fall of 23 percentage points to 43 percent on standalone policies and a shift of 18 percentage points to 48 percent on packaged policies.

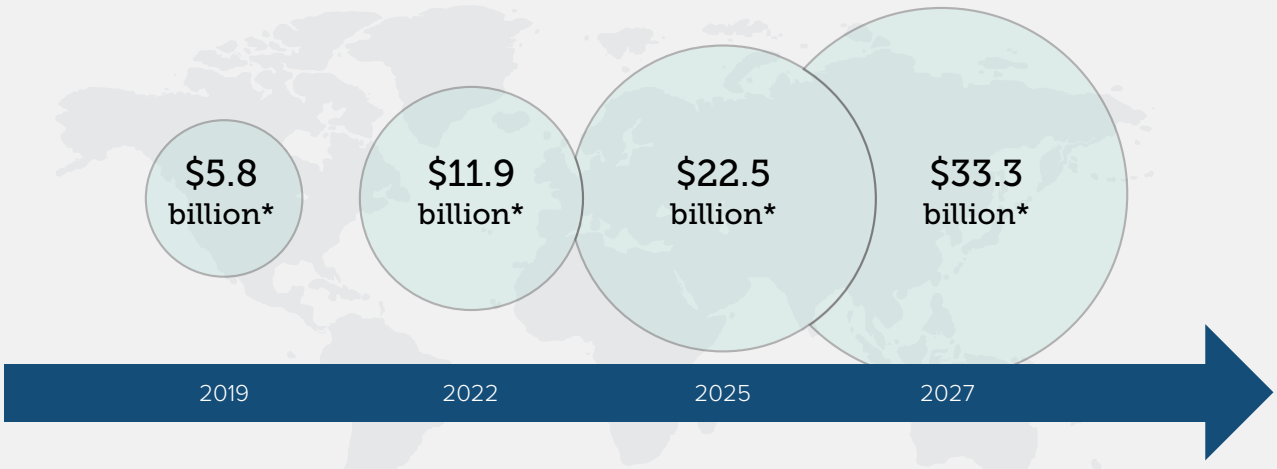
Key Facts

- Cyber insurance returns to profitability and remains the fastest-growing segment of the P/C market following two years of challenges
- The U.S. accounts for 56 percent of premiums written globally on affirmative cyber insurance
- Small and medium businesses can face as much as three times the risk of cyber attacks
- The first cyber catastrophic (CAT) bond emerged in 2023

For larger insureds, standalone policies emerged as the preference. Standalone policies account for more than 70 percent of premiums written, with the 2022 total standalone DPW increasing by 61.5 percent from the prior year, and the total number of standalone policies reported in 2022 increased by 31.8 percent from those written in 2021. Following the hard market of 2020 – when surplus lines companies maintained a 25 percent market share – cyber premiums written by surplus lines insurers have since increased by more than 500 percent, now representing nearly 60 percent of total cyber market premium.

Global cyber insurance market: demand continues to grow.

*Estimates by Munich Re, direct premiums written (DPW), U.S. dollar



Data breach costs rise while cyber security budgets remain relatively tight.

In 2023, the average data breach cost for organizations climbed higher than ever to $4.45 million, according to IBM's Annual Data Breach Report. This figure is a 15 percent increase over 2020, but only 2.3 percent over 2022. About 95 percent of study participants experienced more than one breach.

Only 44 percent of respondents in the 2023 Global Study on Closing the I.T. Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud said they are "very effective or highly effective in keeping up with a constantly changing threat landscape."

Despite ever-rising costs and the threat of repeat incidents, only about half of breached organizations in the IBM study were planning to increase cyber security spending. Nonetheless, organizational expenditures appear to have risen 70 percent over the past four years.

Cyber risk factors continue to increase in number and complexity.

Early data indicates 2023 broke the record set in 2021 for cyber breaches. The Ponemon Institute study revealed that "63 percent of respondents say their security teams lack visibility and control into all the activity of every user device connected to their I.T. infrastructure."

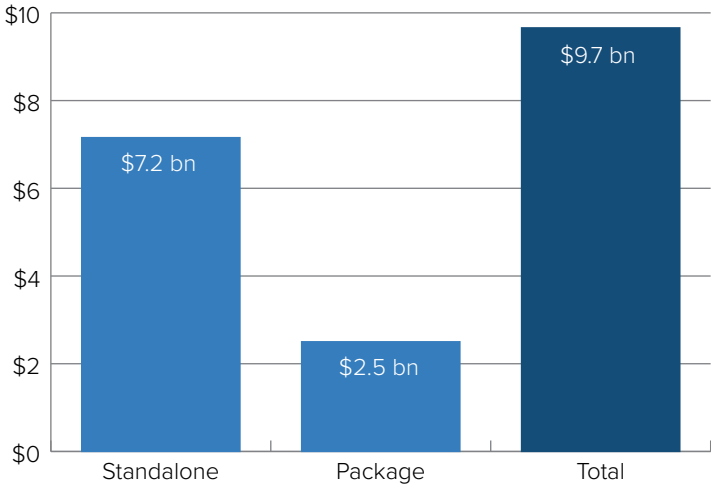
Key exposures are fueled by the continued expansion of technology and practices such as increasing use of:

- Internet of Things (IoT)
- "bring your own device" IT models and remote working
- cloud data storage
- artificial intelligence (AI) to boost capacity for data theft and exploitation of system vulnerabilities

Ransomware attacks remain a significant challenge. While reporting a "decline in ransomware claims during 2022," AM Best reveals that "first-party claims remain close to 75 percent of the nearly 27,000 reported claims as business e-mail compromise claims increased."

Verizon's 2023 Data Breach Investigation Report indicates that ransomware continues to be one of the top factors present in

Total direct written premiums cyber insurance 2022 (billions).



Source: NAIC, S&P Global

breaches, "holding statistically steady at 24 percent." Also, 95 percent of attacks show a financial motive regardless of whether ransomware is involved. Responsibility for 83 percent of breaches can be attributed to external actors, with 49 percent involving stolen credentials and 12 percent phishing.

IBM's annual study showed that 82 percent of breaches impacted data stored in the cloud and that organizations with high levels of security system complexity experienced higher costs than those with low or no security system complexity – $5.28 million vs. $3.84 million in 2023.

Opportunities emerge for improved predict and prevent strategies.

Organizations are becoming more aware of how to use AI and automation tools to improve the speed of identification and containment of cyber vulnerabilities – by as much as 108 days (according to IBM's 2023 study). While viewed by some as competition to cyber insurance, the proliferation of cyber warranties can motivate technology vendors to remain vigilant in monitoring their products, potentially lowering the risk of attacks and inherent costs. Insurers are taking a more sophisticated approach to underwriting and fortifying policy wording and exclusions. Nonetheless, they need more robust data on attacks and breaches in order to predict and manage liability. Federal agencies have announced plans to improve incident reporting frameworks.