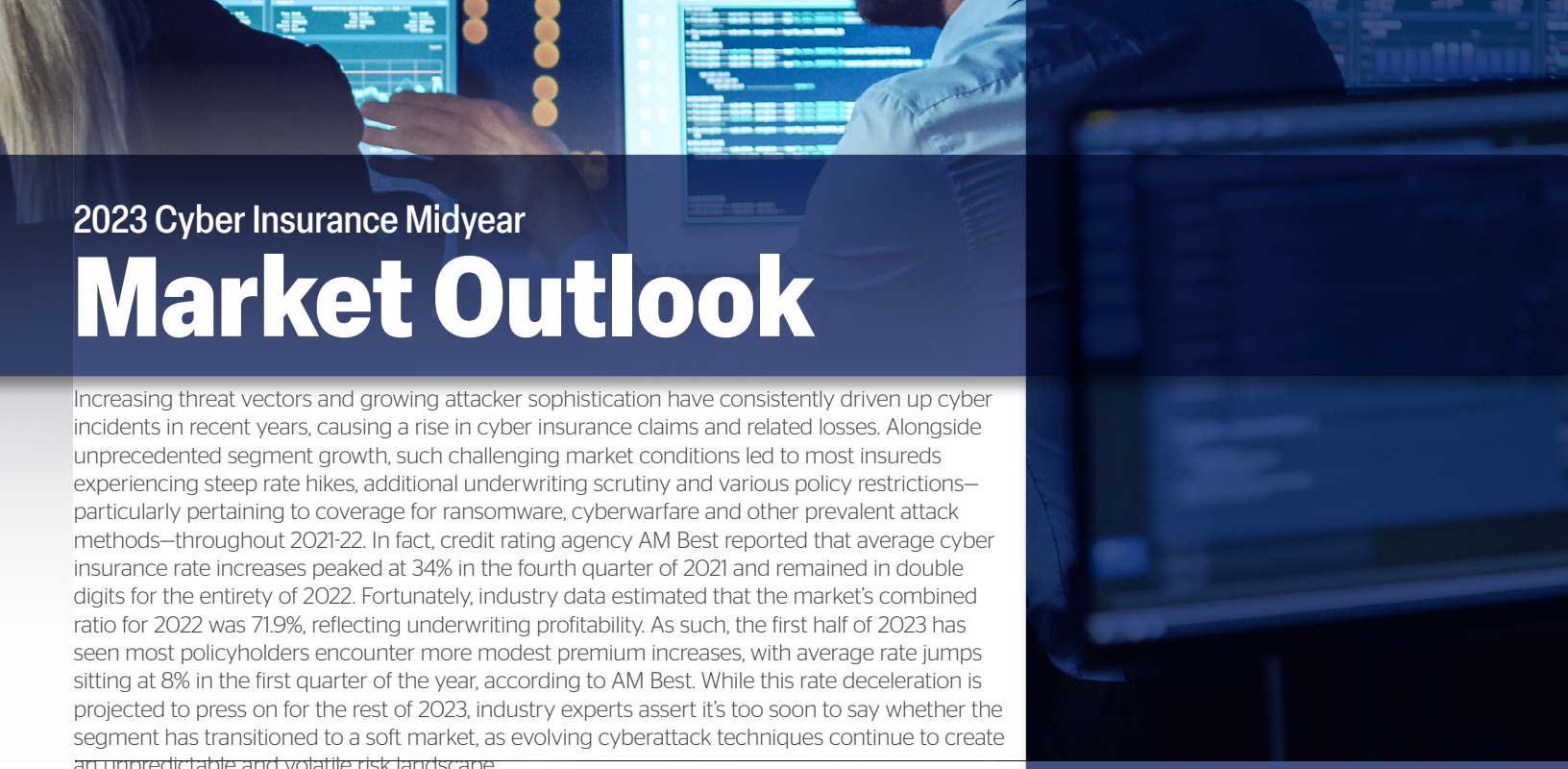

2023 Cyber Insurance Midyear

Market Outlook

Increasing threat vectors and growing attacker sophistication have consistently driven up cyber incidents in recent years, causing a rise in cyber insurance claims and related losses. Alongside unprecedented segment growth, such challenging market conditions led to most insureds experiencing steep rate hikes, additional underwriting scrutiny and various policy restrictions—particularly pertaining to coverage for ransomware, cyberwarfare and other prevalent attack methods—throughout 2021-22. In fact, credit rating agency AM Best reported that average cyber insurance rate increases peaked at 34% in the fourth quarter of 2021 and remained in double digits for the entirety of 2022. Fortunately, industry data estimated that the market's combined ratio for 2022 was 71.9%, reflecting underwriting profitability. As such, the first half of 2023 has seen most policyholders encounter more modest premium increases, with average rate jumps sitting at 8% in the first quarter of the year, according to AM Best. While this rate deceleration is projected to press on for the rest of 2023, industry experts assert it's too soon to say whether the segment has transitioned to a soft market, as evolving cyberattack techniques continue to create an unpredictable and volatile risk landscape.

Developments and Trends to Watch

- **Market growth—**Even amid unfavorable market conditions, the cyber insurance space experienced record-setting growth over the last few years by nearly tripling in size and outpacing all other lines of commercial coverage, according to industry research. AM Best reported that direct premiums written in the segment surged by 50% to $7.2 billion during 2022, while standalone cyber coverage jumped by 62%. Such growth is likely due to increased cyberthreats and associated losses' impacts on businesses across industry lines, thus fueling a rising demand for coverage. Furthermore, many businesses now have no choice but to purchase cyber insurance in light of numerous state laws and industry standards mandating such coverage. As the market continues to expand and premium pricing starts to moderate, however, it's important for policyholders to keep in mind that most cyber insurers have remained cautious when it comes to taking on greater risk, therefore sticking to strict underwriting measures.

- **Geopolitical risks and war exclusions—**Nation-state cyberattacks remain a top concern, especially as geopolitical challenges (e.g., the Russia-Ukraine conflict) contribute to global cyberwarfare worries. According to a recent report from the World Economic Forum, 93% of cybersecurity experts and 86% of corporate executives said they believe geopolitical instability will likely cause a catastrophic cyberattack in the coming years. Complicating matters, coverage for cyberwarfare has become more difficult to obtain. In particular, international insurance marketplace Llyod's of London issued a new bulletin in August 2022 requiring its insurers to revise their standalone cyber insurance policies' war exclusions to specifically prohibit coverage for losses stemming from nation-state cyberattacks. These requirements went into effect on March 31, 2023. Going forward, it's possible that more insurers will follow suit and implement similar coverage exclusions.

- **Elevated ransomware concerns—**Ransomware attacks continue to impact businesses of all sizes and sectors, serving as a primary loss driver in the cyber insurance space. What's worse, new attack methods and the widespread circulation of malicious code have made ransomware incidents even harder to defend against. Although these attacks somewhat moderated in 2022, this trend didn't last long; ransomware-related claims significantly increased in the first quarter of 2023, according to the latest industry data. In response, a growing number of insurers have started requiring policyholders to demonstrate effective cybersecurity measures and incident response protocols aimed at mitigating ransomware attacks to receive coverage for associated losses.

Tips for Insurance Buyers

- Consult insurance experts to review cyber coverage options and find a policy that suits your company's needs.
- Utilize loss control services offered by insurers to help strengthen organizational cybersecurity policies and procedures, especially those for minimizing ransomware and cyberwarfare exposures.
- Keep workplace systems secure by utilizing a virtual private network, installing antivirus software, leveraging access controls and encrypting all sensitive data. Document all cyber risk management strategies clearly.

HORST INSURANCE