

## Cyber Market Update

Notable Updates in the  
Cyber Marketplace



### Q3 2021: A Tipping Point?

The cyber insurance market is experiencing severe conditions. According to some reports, ransomware events are up 300%. After the Acer and CNA events, demands are now regularly in the tens of millions of dollars. With this level of increased frequency and severity, major markets are pulling back capacity while some carriers are no longer writing any new business. Certain carriers have pulled out of the cyber market entirely. 2021 will prove to be a tipping point for the market to correct and offer a sustainable product, or more dramatic changes will be necessary.

Focused on smaller and middle-market insureds, InsurTech's approach to underwriting is winning the cyber race and has resulted in loss ratios well below the industry average. Going forward, similar approaches will need to be deployed in the large account space. Cybersecurity maturity, disciplined underwriting, and adoption of quantification analytics to differentiate one insured from another will be key to building large cyber insurance programs that are priced efficiently and sustainable over the long term.

### A Closer Look at the Market

Insureds can expect to see a combination of market reactions and strategies moving forward.

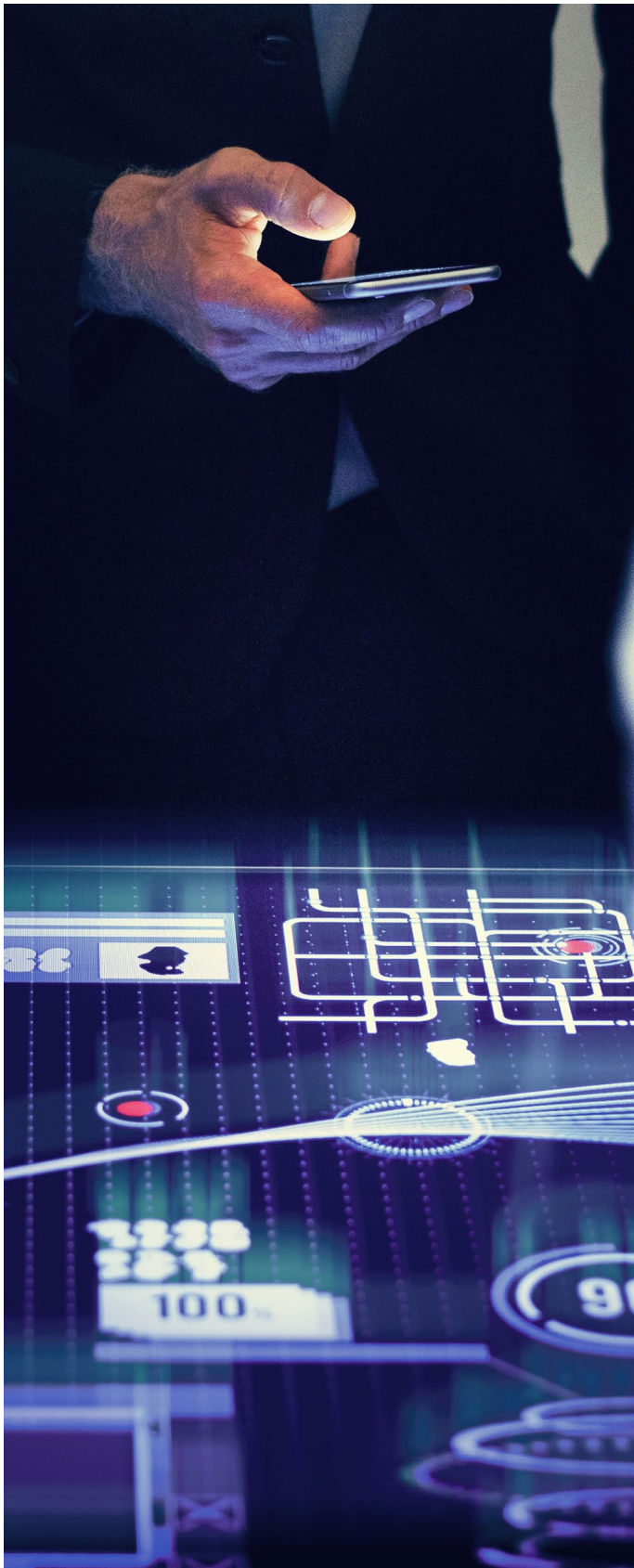
#### Capacity (Limits)

- Market capacity has decreased by over \$135M.
- Major markets have reduced their maximum lines from \$50M to \$25M, and more commonly only offering \$10M at the most.
- More capacity has entered the InsurTech space, creating greater competition for the middle-market, but they are becoming more selective.

#### Premium

- Increases of 40%+ have become a minimum, even without any loss history.
- It is not uncommon to see increases of 100% or more with no significant changes in exposure.
- Expect further increases if there is recent loss history or less than fully mature IT security controls, even without carrier payout.

*Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.*



## Applications

- Supplemental applications are required for ransomware, operational technology, and biometrics.
- Certain carriers have created scoring tools informed by application responses that will be used to indicate coverage and rate quotes.

## Retentions and Co-Insurance

- Carriers are increasing minimum retentions and waiting periods.
- SIRs are increasing with some markets requiring increases of up to 500% or imposing minimums of \$1M.
- Some markets require co-insurance and a sublimit for certain coverages, including ransomware and contingent business interruption.

## 2021 Cyber Loss Trends

- Ransomware attacks continue to deplete market capacity and severely impact insureds. While the number of victims paying ransoms is shrinking somewhat, demand frequency and severity continue to increase.
  - The average ransomware payment increased 43% in 2021.
  - Single ransomware payments have been as high as \$40M.
- The Colonial Pipeline attack has drawn attention to the perils of Operational Technology (OT) risk and the potentially expansive impacts of ransomware attacks.
- Supply chain risks such as with Microsoft Exchange and SolarWinds have resulted in increased concern from the market and insureds about systemic losses. Supply chain attacks are expected to continue throughout 2021. The market fear is that this could have an enormous effect on their book if it affects a significant number of their insureds.