# Market Review: Cyber Risk

*An update for Alternative Asset Managers*

EPIC Alternative Asset Management Services

Alternative Asset Managers can expect 5-10% premium increases at renewal coupled with an uptick in underwriting scrutiny. This change is due to the current cyber threat landscape and workforce conditions stemming from COVID-19 as well as an overall firming of the global insurance marketplace.

Almost overnight, the world moved to cyberspace. Public and private entities quickly transitioned employees to a remote work environment, schools implemented virtual learning, and healthcare providers began relying more heavily on telemedicine. Not everyone was completely ready to move to cyberspace from a security standpoint. Dispersed and distracted employees are being supported by IT resources that are stretched thin. Cybersecurity was a priority pre Covid-19 and now the pandemic has created more vulnerabilities.

In a recent report, A.M. Best said the cyber insurance market will continue its upward pricing momentum in the medium term during COVID-19, amid rising frequency and severity of claims.

## Market Overview

The Global Cyber Insurance market was approximately $7 Billion (USD) in 2019 and is expected to increase to $27 Billion (USD) by 2025. It remains strong, with ample capacity and active competition with 70+ markets offering stand-along cyber insurance. Capacity remains abundant but there is some hesitation related to primary or low excess positions on large towers. Carriers are treading lightly with high-risk classes of business such as retail, transportation, hospitality, healthcare and financial institutions, especially considering the current crisis.

Recent premium rate hardening in the U.S. commercial lines market carried over to the cyber market in 2019, with the Council of Insurance Agents & Brokers fourth-quarter commercial market survey reporting a 2.9% increase in rates for cyber policy renewals. However, 2020 cyber premium growth will be moderate due to decreases in underwriting exposures resulting from the sharp economic downturn tied to the coronavirus pandemic.

Privacy issues and compliance concerns are causing many underwriters to be more conservative and detailed in their risk analysis. Some markets are introducing sub-limits or other coverage restrictions around Business Interruption Coverage – both Direct and Contingent. For example, one insurer has moved to sub-limit their ransomware coverage and in some cases is aiming to reduce their exposure by cutting limits of liability on select risks. Other insurers are restricting coverage for employee-owned devices. Overall, the underwriting process has lengthened considerably and **insureds should anticipate increased scrutiny from underwriters** as they assess data protection controls, security measures and compliance with a heightened regulatory landscape.

## Threat Landscape

Alterative Asset Managers possess high amounts of sensitive client and non-public private information that make them a prime target for cyber criminals. The number of threats has increased as investment and private equity firms become more dependent on outsourcing and adopt new technologies to support operations. A firm's wellbeing faces serious risks regardless of the target, size and motive of future attacks. It's vital to be aware of common threat types targeting the broader Alternative Asset Management community.

| Top Risks | | Top Impacts | |
|---|---|---|---|
| Ransomware/Malware | Hacktivism | Business and Operational Risk | Regulatory Risk |
| Social Engineering | Insider Threats | Reputational Harm | Investment Risk |

# Market Review: Cyber Risk

*An update for Alternative Asset Managers*

EPIC Alternative Asset Management Services

## Emerging Risks

- Proliferation of Cybercrime
  - Increasingly sophisticated attacks using AI, deep-fake audio/video
  - Ransomware 2.0/"Big Game Hunting": More targeted and broad-based attacks, with bigger demands and wider implications
  - Impact of **COVID-19**: Cybercriminals exploitation of vulnerabilities created by the sudden and rapid movement to "remote" work environments necessitated by the pandemic
- Regulatory Environment
  - Broad based International and U.S./state-level privacy regulations: Breach v. Privacy Coverage
  - SEC's focus on Information Security: A priority in the 2020 Examination Priorities and OCIE Risk Alerts
  - General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and multiple other states with copy-cat (or more restrictive) regulations pending – MA, NY, NV, VA and others
- Connectivity
  - Transition to 5G Network connectivity will create new exposures and vulnerabilities (specifically as respects internet-connected devices); and may trigger new regulation
- Move to address "Silent Cyber"
  - Domestic and International insurers are taking affirmative steps to eliminate or narrow their prospective coverage for "silent cyber" exposures
- Cyber Representations and Warranties
  - Two of the most frequent newly appearing representations in purchase and sale agreements, according to the latest ABA Deal Point Study, are related to information privacy and security

## Impact of Covid-19 on Cyber Insurance Market

- Impact has started but still not fully known
- Potential for spike in claim frequency/severity
  - Continued proliferation of cybercrime – ransomware attacks
  - Companies response to attacks may not be as effective given a fully remote work environment which could be overburdened
  - IT Depts and Executive = higher costs to respond, remediate and recover from malicious attacks
  - Increased claim frequency/severity could impact premiums, limits, capacity
- Business Interruption Coverage – Direct and Contingent
  - Introduction of sub-limits, other coverage restrictions, increased underwriting
- Definition of Computer System & Underwriting of BYOD/Remote Working
  - Supplemental applications pertaining to remote work environment & BYOD policies and accompanying **coverage restrictions**
- Sub-limits on Social Engineering Crime coverage
  - Sometimes depending on the carrier, this may be a two (2) policy solution (Cyber / Cyber Crime)

## Conclusion

Given the current market environment, we are now seeing increases in both self-insured retentions as well as premiums (+5-10%). This change is due to increased claims and losses stemming from the new generation of ransomware attacks and increased cyber vulnerabilities stemming from COVID-19. In certain cases, insurance carriers are restricting coverage terms and reducing limits of liability.