Market Review 2.0: Cyber Risk

An update for Alternative Asset Managers // Second Edition

EPIC Alternative Asset Management Services

Cyber threats in the alternative investment industry are growing increasingly larger and more sophisticated. Alternative Asset Managers and in some cases their respective Portfolio Companies, have worked closely with Cyber Security vendors to help defend against and mitigate the effects of Cyber Incidents. Putting together a robust Cyber Security program requires a multi-faceted approach. Creating an incident response team, performing regular tabletop exercises coupled with other vendor due diligence are just some of the strategies being implemented. For most managers, Cyber Insurance has become an integral and key component of a firm's Cyber Security Program. Our July 2020 Cyber Risk Market review outlined the early implications, threats, emerging risks and impact of the COVID-19 pandemic. The below commentary includes a cyber insurance market update and cyber risk considerations for 2021.

COVID-19 and Work from Home

COVID-19 continues to impact the cyber threat landscape. The global shift from the corporate office setting to working remotely has increased the exposure and probability of phishing and hacking attempts. Purplesec, a leading cybersecurity firm, asserts that cybercrime is up 600% due to the COVID-19 pandemic. As a result, insurers expect claims and losses related to this shift to continue to rise, as organizations and their cyber infrastructure are still more vulnerable than usual due to the current work from home environment.

The Ponemon Institute, a pre-eminent research center dedicated to privacy, data protection and information security policy, published a report in October 2020 titled *Cybersecurity in the Remote Work Era: A Global Risk Report* that details the current environment of increased cyber risks. Some key findings below:

- The remote work force has significantly reduced the effectiveness of organizations' security posture.
- Credential theft and phishing/social engineering are the most frequent types of cyberattacks since COVID-19.
- IT security budgets and in-house expertise need to increase.

Threat Landscape 2.0

Our July 2020 report outlined the top risks and impacts facing Alternative Asset Managers. Alternative Asset Managers possess high amounts of sensitive client and non-public information that make them a prime target for cyber criminals. The number of threats has increased exponentially as investment and private equity firms become more dependent on outsourcing and adopt new technologies to support operations. Our top three cyber risks are as follows:

- Ransomware
    - Ransomware is malicious software that infects a computer system and blocks access to it or your data until a ransom is paid. The inability to access critical systems, the publication of investor details, or dealing with the technology and legal sides of a ransomware attack can derail many companies.
    - Costs surrounding ransomware attacks continue to rise year over year. See below for the 2020 Purplesec statistics:
        - Average payment increased 104%
        - Downtime increased 200%
        - Average cost of an attack was $133,000
- Social Engineering
    - Social engineering attacks involve psychological manipulation of employees into performing actions or divulging confidential information. These attacks typically involve phishing scams that use email, social networks, and more. According to a 2021 IBM report, the financial services and investment industry was the most attacked industry.

- Reputational Risk
    - A cyber event can have a profound impact on a firm's reputation. According to a survey at PwC, 87% of consumers "will take their business elsewhere if they don't trust a company is handling their data responsibly." This fact is concerning for asset managers and their ability to attract future investors.

Cyber Market

Our July 2020 update predicted alternative asset managers will see cyber insurance premium increases at their next renewal. At the time of this publication, Cyber Insurance premiums are now expected to increase 10% to 30%. These increases are due to the current threat landscape, increased costs surrounding cyber events and rising reinsurance premiums.

Heavily exposed industries will experience renewal rates on the higher side: health care, higher education, public entities, manufacturing, financial institutions, construction, and large media and technology companies. These industries have an increased risk profile and are targeted with greater frequency.

Primary capacity generally remains strong, with active competition and over 70+ markets offering stand-alone Cyber Insurance. However, there now is some hesitation related to primary or low excess positions on multi-layered insurance programs. Furthermore, insurers are seeking higher rates on line for excess layers given the competitive primary pricing and ever increasing risk profile. As such, there is currently less interest and ultimately less competition to compete for excess positions where the pricing is unattractive.

As you may know, pricing is not linear in layered insurance programs. Traditionally, each excess layer will charge a fixed percentage of the underlying policy premium. This is also referred to as a "Rate on Line" (ROL). Currently the ROL for excess positions is between 60 and 70% of the underlying policy premium. ROL's as well as rate per million continue to trend sharply upwards and remain largely dependent on the specifics of any particular risk. Larger organizations with a significant number of client records consisting of personally identifiable information, or companies who are susceptible to possible business income and extra expense losses may see ROLs in excess of 75% or higher.

In some cases, we have seen inverted towers, where the top excess layer is more expensive than middle layers on a program. This happens when a minimum rate per million is achieved and the program flattens out. Minimum rates per million for Cyber coverage are in the $6,000 - $8,000 range. Inversion usually happens on towers of more than $50,000,000.

Underwriters continue to be more conservative and detailed in their risk analysis. As a result, buyers should continue to expect the underwriting process to take longer and prepare accordingly. Insureds should continue to anticipate increased scrutiny from underwriters as they assess data protection controls, security measures and compliance in a heightened regulatory environment.

Further Cyber Risk Considerations

Given the recent uptick in M&A activity, Alternative Asset Managers need to be aware of potential issues related to M&A activity. Companies should engage their IT staff early in the acquisition process to evaluate risks. The potential for reputational and financial harm from a cyber incident could have impacts on a firm's valuation.

Additionally, the worldwide rollout of 5G networks will continue in 2021. Increased bandwidth and speed will facilitate the world's transition to a cloud-based society and expand the use of "Internet of Things". Companies will now need to invest in greater and more sophisticated levels of monitoring for their networks, controls and technology in order to address these increased exposures.