LOCKTON
UNCOMMONLY INDEPENDENT

Cyber Market Update

February 2022
EXTERNAL

Background

Maintaining the trends seen over the past 24 months, the cyber market is continuing to harden: premiums and self-insured retentions are increasing, while limits are reducing.

Driven by a larger number (and higher average cost) of claims, it is no surprise that insurers are scrutinising risks more than ever before, raising the floor for minimum controls across the board, with most underwriters seeking greater assurances around cyber security controls. As a result, mitigating controls such as privileged access management, patching management, and SIEM (Security Information and Event Management) systems have become the latest entrants to the laundry list of required baseline controls for cyber coverage.

The appearance of the java based log4j/log4shell zero-day vulnerability in November 2021 further reminded the market of how cyber risk does not always come in the form of targeted attacks and can arise from what many would have considered to be simple, non-risk software.

Claims Environment

The primary driver of the current market cycle is the increasingly harsh claims environment. Using information from the London Cyber Claims Team, data from the last 5 years of claim show:

- Since 2017, claim frequency has been increasing at an average of 13% year-on-year however, total loss has increased at an average of 80% over the same period.
- As a proportion of all claims the team has witnessed, those arising from external actors (such as data theft, malware, and social engineering) have increased 59% between 2019 and 2020.
- Ransomware-specific claims were the cause of about 5% of claims notified to Lockton in 2018, accounting for 10% of the total incurred. By contrast, in 2020, ransomware claims accounted for 17% of all claims, and for more than 80% of the total costs incurred.

Market Impact

It is evident as to why underwriters have been forced to demand a higher level of mitigating controls, specifically around those relevant to ransomware. The following is a brief analysis of the impact across the Lockton portfolio from a premium, retention and coverage perspective, specifically looking at the past three months:

- Average premium per million dollars of limit has increased by 161% year-on-year, with some companies experiencing increases in excess of 500%.

- Primary retentions have increased upwards of 125% on average, with some medium-sized firms ($/£ 250m – 1bn revenue) experiencing increases upwards of 345%.

- The average capacity deployed by insurers per layer has decreased by 21% across the board.

- With premiums increasing so significantly, insurers are meeting budget expectations merely by underwriting their renewal book. Consequently, insurer appetite for new business tends to be limited to those companies which have golden standards of security controls. These include strong minimum protocols such as Multi Factor Authentication (MFA) for remote desktop protocol, robust backup procedures, endpoint protection, privileged access management (PAM) and incident response/business continuity plans.

- High-risk industries in particular, are under the insurers' microscope following higher than average frequency and severity of claims. These include law firms, manufacturing, healthcare, retail, and financial institutions.

Although the current outlook may seem bleak, there are steps that can be taken to minimise the risk of non-renewal or vastly increasing premiums and retentions. Essentially, the best strategy is to prepare your application early, preferably around three to four months before renewal. Doing so allows your broker to prepare the insurers, whilst giving time for the inevitable back and forth owing to questioning and negotiations, avoiding any last-minute surprises or gaps in cover.

What You Can Expect

When approaching the market to place your cyber insurance, your broker will typically follow the below process:

- Renewal invitation Three to four months before renewal, your broker will invite you to fill out the required documentation. These forms allow insurers to attain a sense of an organisation's security controls and operating procedures relevant to a cyber policy and typically include:

    - a full Cyber Proposal Form which outlines:
        - all standard base controls for network security
        - how organisations handle their critical and sensitive information
        - business interruption mitigation controls
        - breach incident management
        - claims history (with details of any claims and the remediation following the incident).

    - a Ransomware Supplemental Application to highlight ransomware mitigation controls including:
        - MFA for all connections to the network by employees and vendors
        - Internal MFA to access any critical information or privileged access
        - PAM protocols
        - Frequent training for staff and employees
        - End-of-Life software inventory and strategies to decommission or segregate
        - End-point protection products securing all endpoints / servers
        - Strong back-up protection and storage, back-ups to be stored offline (physical) or to be stored on a separate network.

- a Biometric Supplemental Application if the insured collects or stores any biometric information.
- a 'Known Vulnerabilities' Supplemental Application if the insured has been affected by any known vulnerabilities, for example SolarWinds, Accellion, Microsoft Exchange Server, Kaseya.

- Market approach Once complete, your broker can begin discussions with insurers, choosing those best suited to your cover requirements and company profile.

- Questions and negotiations Given the increased scrutiny around risk, insurers are likely to answer further questions about your organisation and its security. If insurers are happy with the risk, negotiations can begin with relation to coverage, premium and retention.

- Wrapping up Once negotiations are complete, your broker (or possibly the insurer and the broker) will prepare all the relevant documents with a view to ensuring coverage is in place for the required period.

Although the process may seem cumbersome, gathering as much information as early in the process as possible, will certainly assist Lockton in attaining most favourable terms. Your broker is always available to host a call answering any questions about the forms, the process or your policy generally.

What is the Forecast?

On a positive note, there has been some change in capacity within the market. New insurers are entering the cyber market increasing capacity, specifically for companies above $1bn in revenues.

After canvassing opinion from various insurers, we are of the view that triple digit rates will not last for the entirety of 2022. It is widely believed that this historical level of rate increase will continue to apply for Q1 and Q2, but we expect a downwards pressure as we head towards Q3 and Q4.

Recently the Insurance Insider published predictions from Beazley which indicated that its anticipated blended premium per million of coverage rate increases for 2022 will be between 60% and 75%. This coincides with our thinking.

Global Cyber & Technology Team, London