Cyber Market Environment

December 2021

The cyber insurance market has hardened considerably throughout 2021 with major changes to available limits, higher retentions and premiums. Ransomware attacks and an increase in remote work have been driving factors in the hardening market and increased cyber claims. We do not expect market conditions to soften in 2022.

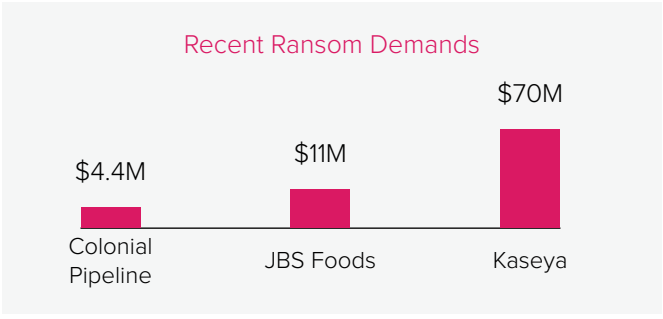
Throughout this report we'll explore the latest in this year's cyber market as well as key cybersecurity actions you can take to ensure your business is prepared.

Underwriting Trends

Ransomware is the leading cause of cyber loss today with frequency and severity increasing at an alarming pace.

Insurers are underwriting more selectively and require complete and acceptable applications prior to binding.

Underwriters are requiring baseline internal IT security controls for preventing ransomware attacks (see Key Cyber Security Requirements) and risk management controls.



Ransom demands of $1M or more are now more common. For example, the demand on the recent attack on Kaseya is reported at $70M. JBS meat supplier paid an $11M demand. Colonial Pipeline paid a $4.4M demand, yet the Department of Justice recovered approximately $2.3M of it.

Supply chain risk has also increased dramatically. The SolarWinds breach highlights how a breach at one company can have a much larger impact across the economy and the cyber marketplace. Underwriters are asking questions around use of SolarWinds software and Microsoft Exchange, and risk mitigation efforts. Related exclusions may be added.

Cyber Market Environment

Renewal Process

Start early allowing the underwriting process as much time as possible.

Provide complete applications 45-60 days in advance. Carriers require their own forms to be completed, so anticipate there may be various forms and follow up questions.

Participate in underwriting meetings as needed, including discussion with CISO or Head of IT.

Complete all subjectivities prior to binding.

Premium/Capacity Trends

- The cyber market is hardening fast with rates increasing 100%+ in most cases.
- Larger companies with revenues $1B+ are experiencing rate increases 200%+, and reduced capacity.
- Without full MFA across the enterprise, clients risk non-renewal or significant rate increases, retention hikes, coinsurance, or reduced coverage. Full MFA is a non-starter for most insurers.
- Carriers are cutting primary capacity limits, and sublimiting key coverages such as Cyber Extortion, Cyber Crime, Contingent Business Income, Hardware Replacement, and others.
- Policy layers of $10M limits, which were typical in the past, are being reduced to $5M making the need to have twice as many carriers on a program to secure the same total limits.
- Given the increasing severity of losses, excess insurers may seek higher increased limit factors than they have in the past, which means rate increases will be higher on a percentage basis than the primary layer.

Cyber Market Environment

Key Cyber Security Minimum Requirements

1. Full multi-factor authentication (MFA) across the enterprise - email, remote access, and privileged users.
2. Endpoint protection (EPP) and endpoint data and response (EDR) protection.
3. Plan for end-of-life or end-of-support products replacement. Products still in use must be kept segregated from the network.
4. Backup data must be kept separate from your network (offline) or in cloud designed for this purpose.
5. Frequent security awareness training for employees.
6. Business Continuity Plan with recovery time objectives.
7. Disaster Recovery Plan.
8. Cyber Incident Response Plan.

Be Prepared to Act Fast

- Be sure your Cyber Incident Response Plan is kept up to date with important contact information.
- Keep a copy of the Plan both online and offline in case your system is unavailable.

Report a potential claim as soon as possible to:
ClaimsGroup@theabdteam.com

Newfront

newfront.com | 650-488-8565