Commercial Property & Casualty Market Outlook

Cyber and Executive & Professional Risk Solutions

Addendum to the 2020-2021 Market Outlook

Product Line/Market Update*	Q2 2020	Q4 2020-2021 Updated (YOY)
Network Security & Privacy (Cyber)	Up 5% to 20%	15% to 50%
Technology/Miscellaneous Professional Liability (MPL) Network Security	N/A	15% to 50%

*Any insurance placement that includes cyber and privacy coverage components will experience some form of hardening.

Cyber Insurance Update

In 2019, the cyber insurance industry saw increased ransomware activity. In the fourth quarter of 2020, an unprecedented number of cyber incidents affected the insurance market, some of which included:

- The SolarWinds supply chain cyber event.[1]
- A historical spike in ransomware attacks. The healthcare sector alone faced a 40% surge, while year-over-year growth for municipalities grew by 50%.[2]
- A dour cyber re-insurance cycle.

Given these events, the cyber market has gone from hardening to historically hard. Overall, insurers are managing the limits (capacity) they deploy, increasing self-insured retentions, and underwriting more thoroughly and technically. This includes the removal or limitation of previously negotiated coverage.

Note: SolarWinds is a developer of business software. In December 2020, SolarWinds acknowledged that hackers inserted malware into a service that provided software updates for its Orion platform. To date, SolarWinds indicates that roughly 18,000 of its customers were impacted. It has further been detailed that the intrusion also compromised third-party supply partners like Microsoft.

Premium and SIR Changes

Primary Layers

- +15% to +50%, with a complete submission and optimal ransomware controls and no material loss events
- Over +50%, if losses and/or sub-optimal internal information security controls and processes are presented

Excess Layers

- +15% to 35%, no losses/complete submission and optimal ransomware controls
- +50%, if losses and/or sub-optimal internal information security controls and processes are presented

Minimum Self-Insured Retentions (SIRs) Sought

- -$250K to $500K for middle market companies
- $1M or more for large companies

Year-over-year increases in trigger times for business interruption coverages

- 100% to 200%

[1]https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details
[2] https://www.ibm.com/security/data-breach

Additional Underwriting Requirements

Insurers are focused on insured controls, which may be analyzed in a ransomware/extortion supplement — now widely required by cyber insurance carriers. Controls include:

- Multifactor authentication (MFA) controls
- Patch management processes
- Backup procedures
- Vendor management IT controls
- Presence and use of endpoint detection and response (EDR)
- Regulatory expansion, both in U.S. and internationally
- Specifically, the use and presence of any SolarWinds software

Insurers are consistently engaging the services of third-party vendors to perform noninvasive perimeter technical scans and alerting insureds. The goal is to proactively identify potential vulnerabilities that may create a potential breeding ground for a cyber event.

Insurers are scrutinizing loss runs/loss information on applications, looking for:

- Details of any event(s)
- Costs incurred and paid
- Remediation steps taken to prevent the reoccurence of a similar loss/event

IMPORTANT

A complete submission must include, at minimum, an appropriate application and ransomware/extortion supplement. Insurers are unlikely to quote a risk without a complete underwriting submission.

Insureds with poor ransomware controls will likely experience higher premium increases, reduced deployed capacity, or higher SIR.

Policy Wording Changes

For ransomware controls and mitigation techniques, insurers typically classify a risk in any of these four categories:

- Best in Class
- Above Average
- Average
- Below Average

For average or below average categorization, insurers may insulate themselves by:

- Adding a ransomware exclusion
- Reducing limits/capacity and increasing the retention of relevant coverage sections for ransomware events
  - Applying a form of coinsurance percentage for relevant coverage sections for ransomware events in response to the aggregate exposure potentially posed by the spike in network intrusions
- Evaluating any of the following:
  - Coinsurance for contingent (dependent) business interruption/extra expense
  - Increased waiting periods for cyber property coverage sections
  - "Specific Event" exclusions for events that can potentially impair multiple networks at once
  - Infrastructure exclusions
- Where included, reevaluating the underwriting and limits deployed for local cyber and cyber/errors and omissions (E&O) policies
  - Insurers are aligning the underwriting of local cyber policies with the underwriting of master cyber policies

Cyber Insurer Appetite Changes

In 2020, insurers experienced a spike in ransomware events and a massive increase on the dollar impact of these events. While ransomware affects all industries, insurers are managing their exposures (reducing the deployed capacity or increasing the overall SIR) in certain hard-hit industry verticals, including:

- Municipalities
- Manufacturers
- Educational institutions
- Professional services firms (e.g., law firms)
- Public officials/entities
- Airlines
- Healthcare

How USI Can Help

To help clients mitigate the effects of the hardened cyber market, we can:

- Engage strategic resources, many exclusive to USI, aimed at evaluating and improving their cyber hygiene and profile
- Lead a deliberate placement process, which will shape the conversation around their risk profile
- Leverage customized terms experience and our expertise identifying viable cyber insurers
- Provide analytical input around questions of limits, claims impact, and cyber underwriting concerns

How Can We Help?

To help clients navigate these challenging times, USI has implemented a STEER (Steer Through Epidemic & Economic Recovery) Task Force. This cross-functional team is working to provide timely COVID-19 information, understand cross-industry and geographic impact and evolving responses, and to develop and deliver tailored solutions to help clients steer through this epidemic challenge and economic recovery.
For additional resources, tools and information, please visit our COVID-19 resource page: www.usi.com/public-health-emergencies.

USI | STEER
Steer Through Epidemic & Economic Recovery