Threats Driving the Current Cyber Market

Malicious Attack/Ransomware

- Hackers in network; malware and viruses; phishing scams (ransomware); physical theft of hardware and paper.
- Significant increases in severity and frequency since 2019
- Average ransomware payment for 2021 Q3 - $139,739 (up 3% from Q2 2021)*
- Credential Access remains top tactic for network infiltration *. Carriers have almost universally adopted MFA as required security tool to access Cyber Liability insurance.

Employees & Business Partners

- Any of the above can occur to a business partner with whom data is shared with.
- Rogue Employees
- Negligence related to the use and storage of data; failure to follow or learn policies and procedures; loss of portable devices; mis-mailing of paper; and/or unencrypted emails to the wrong recipient(s).

Privacy Regulations

- GDPR - fines continue to increase
- BIPA (IL Biometric Information Privacy Act) – litigation and settlements continue to rise
- CCPA (California Consumer Privacy Act) – similar state laws on the horizon requiring additional compliance for corporate use of protected information

Supply Chain

- Event impacting critical applications, software, or infrastructure utilized by organizations.
- Aggregation concerns are causing decreases in traditional capacity offerings by Carriers
- Recent examples include: Log4j, SolarWinds, Microsoft Exchange, Accellion, and Kaseya

** Sources: Ransomware attackers down shift to 'Mid-Game' hunting in Q3 (coveware.com)*

Cyber Q4 Market Update

Metric	Q4 2021 YOY Change	Q4 2021 Commentary	12 Month Forecast	12 Month Forecast Commentary
Pricing	▲ 100% (Minimum)	Cyber claims continue to increase in frequency and severity causing carriers to increase rate needs across all industries (with the biggest swings affecting the following industries: municipalities, technology, healthcare, education and manufacturing). Further, with loss size continuing to increase, excess carriers continue to increase rate need faster than primary. Increases were typically between 100% and 300%.	▲ 100% to 250% (Minimum)	Ransomware, privacy regulation (e.g., BIPA), and supply chain cyber risk continue to be at the forefront of claims and actuary concerns. Rates are expected to continue to increase throughout 2022 as more claims are submitted.
Limits	▼	Carriers continued to manage their capacity to $5M or below across their portfolios. Sublimits are becoming more common and should be expected especially for ransomware and dependent business interruption.	▼	We expect this trend to continue throughout 2022. Carriers will continue to strategically deploy capacity for accounts that maintain favorable cyber hygiene. Cyber extortion /ransomware limits will continue to be sublimated with a potential coinsurance.
Retentions	▲	Carriers continued to seek retention increases on tougher industry classes, companies lacking controls, or with claims activity. Waiting periods are also rising on the Business Interruption coverages. In some instances, between 24 and 48 hours. Coinsurance is becoming a standard clause for ransomware.	▲	We expect this trend of increased retentions, higher waiting period and coinsurance to continue.
Coverage	▼	Carriers continued to reduce or exclude ransomware coverage when controls are less favorable. Carrier scrutiny around media liability and regulatory cover for biometric related information increased. Carriers continue to focus on increased underwriting scrutiny and overall cybersecurity controls.	▼	Trend continues toward more restrictive policy wordings and coverages especially around ransomware. Clients will need to focus more on cyber hygiene controls (particularly MFA, EDR, email filtering, secured/tested backups and PAM solutions), as well as media and biometric information handling to gain coverage.
Carrier	▼	Continued tightening of underwriting guidelines including the mandatory need for favorable ransomware responses. Coverage will be paired down when controls are lacking. MFA and EDR has become a critical component in the underwriting process. Emergence of several new MGA/MGUs in the marketplace which could help replace capacity or markets that are pulling out of specific industries.	▼	Carriers will emphasize the requirement for quality ransomware and cybersecurity controls. Use of non-invasive scans (Bitsight, Security Scorecard and Cyence) during the underwriting process will continue and questions about findings/potential issues (i.e. open ports) will need to be remediated. Additional questions around vendor management, business continuity plans and employee training will continue to be part of the underwriting process.
Claims	▲	Significant increase in frequency and severity of cyber claims, especially ransomware continued. Social engineering/financial fraud claims continue to target companies in all industries. Large ransomware events such as those affecting C.N.A., Colonial Pipeline and JBS demonstrate the likelihood these attacks will continue in all industry classes.	▲	Cyber claims activity is expected to continue to increase. The impact of large/headline cyber events will impact carriers capacity and underwriting changes well into 2022. The continued work from home environment and return to work will continue to test cyber infrastructure across various industries leading to increased claims activity.

Cyber Security Controls of Underwriter Focus

Claims severity and frequency has caused a severe hardening of the Cyber Insurance Market. Before approaching Carriers it is important to have a comprehensive understanding of the security controls our markets deem important. Lacking many of these controls could result in the loss or reduction of coverage. Please engage your IT and brokerage team early.

Detection & Prevention

- Multifactor authentication for remote access, privileged accounts and administrative access.
- Endpoint Detection & Response (EDR)
- Email filtering and screening for potentially malicious attachments/links
- Web Monitoring

Testing & Backups

- Encrypted backups
- Backups kept separate from the network in an offline and/or cloud service location
- Regularly tested backups for restoration and recovery

Protected Network

- Privileged Access Management (PAM)
- Network Segmentation
- Hardening baseline configuration
- Regularly patched systems and applications
- Consistent vulnerability scans
- End of Life System management

Cyber Response & Awareness

- Employee Cyber Awareness Training
- Annual penetration testing and system review
- Tested Cyber Incident Response (CIR) plan
- Vendor and Third-Party Risk Management