Market Update Q3 2022 – Cyber & Technology

State of the Market

- Increase in frequency, severity and sophistication of Ransomware
- Business interruption driving losses
- Double, triple extortion now common
  - ✓ Double extortion: encryption + data exfiltration account for over 70% of ransomware attacks
  - ✓ Triple extortion: encryption + data exfiltration + harassment of clients, employees, patients, suppliers of victim company
  - ✓ Quadruple Extortion on the horizon: encryption + exfiltration + denial of service attack + customer/client harassment.
- Ransomware focus on industries where paying ransom is imperative to health and safety (healthcare, energy, govt)

Coverage Trends: Pricing, Terms & Conditions

- Substantial price increases continue on larger accounts – but also recognition from insurers this cannot continue – expectation that rate of increase will soon decrease
- Rate of increase for smaller accounts decreasing
- Most insurers reduced capacity to a maximum of $5mln
- Coinsurance and/or sublimits for ransom related losses common
- Increasing number of insurers declining accounts without MFA or other security measures or imposing coinsurance/sublimits
- Markets focus on assessing and limiting exposure related to Ukraine-Russia conflict.

Legal & Regulatory Developments

- Increasing number of domestic broad-based privacy regulations will become effective in 2023 and ready for enforcement
  - ✓ Virginia Consumer Data Privacy Act (effective Jan 2023)
  - ✓ Colorado Privacy Act (effective July 2023)
  - ✓ Utah Consumer Privacy Act (effective Dec 2023)
  - ✓ CA Privacy Rights Act (effective Jan 2023)
  - ✓ CT Personal Data Privacy (effective July 2023)
- In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
- Biometric regulation, similar to Illinois BIPA, is pending or passed in many states - private cause of action is the trend.

Emerging Risks & Trouble Spots

- Business email compromise, email and/or social engineering remain the most common attack vectors
- Attacks on Critical Infrastructure is a rapidly growing area of concern
- Multiple vendor breaches in billing services, charity management and time-keeping also created substantial incidents and actual losses across their entire client base
- Supply chain attacks continuing to cause substantial disruption
- Increase in regulatory actions and third-party litigation connected to breach events and other violation of broad privacy regulations.