PARKER SMITH & FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

CONSTRUCTION PRACTICE GROUP

AUGUST 3, 2021

WHY AND HOW DID THE CYBER INSURANCE MARKET HARDEN OVERNIGHT?

Greg Lagreid
Account Executive
Parker, Smith & Feek

Erin Burns
Executive Vice President
INSUREtrust

This is a question many insureds are pondering as they are running into seemingly brick walls at their renewals. After battling hard markets in other lines of insurance over the past few years, most policyholders have not seen cyber premiums increase significantly until recently. This is in addition to potentially reduced limits and coverage. The short answer to the title question is ransomware. The long answer is…ransomware.

Ransomware attacks have been steadily increasing in frequency, severity, and sophistication. Long gone are the days of extortion for just a few hundred dollars. Now, hackers are demanding millions of dollars in cryptocurrency with established negotiating strategies. In addition to the extortion for access back to systems, they are holding the sensitive data exfiltrated from the systems hostage as well. In many cases, organizations have little choice but to pay the ransoms, decimating insurers' bottom lines practically overnight. There is no time to reserve for these losses, watch claims develop for months or years at a time, and then have actuaries model the corrective action needed over the next two or three years to protect insurers' balance sheets. Capital is there one day and gone the next, without warning. Compounding this issue for insurance companies are insureds that elect not to pay the ransom and restore their systems from backups (assuming they exist and are unaffected). With the average downtime of 23 days from a ransomware attack, significant losses are coming from forensics costs, loss of income, and extra expenses incurred, all of which can be covered in **properly placed** cyber policies.

Market Reactions

How have insurers reacted to this dynamic? Pretty drastically, but most will say it is necessary for them to continue to write business. As an industry, carriers are addressing their responses differently, but there are some constants throughout the group.

ABOUT PARKER, SMITH & FEEK

Parker, Smith & Feek is a private brokerage firm driven by client service. We offer a range of services, including commercial insurance, risk management, surety, employee benefits, and personal insurance. PS&F is ranked nationally as one of the 40 largest privately held risk management and insurance brokers. We are committed to serving the community and proud to be one of the top corporate philanthropists in the region.

LEARN MORE

Construction Practice Group
Our Services

CONTACT US

Email
Tel: 800.457.0220

FOLLOW US

continued >

- *Rates are increasing across the board and **fairly significantly**.* Well-controlled, loss-free accounts are still seeing double-digit rate increases. Poorly controlled accounts are commonly seeing 40%, 50%, or even higher. Carriers have also increased minimum premiums across the board.
- A good account is no longer defined by having an excellent IT department and no claims. Very technical controls are critical for insureds to implement prior to their renewals to be viewed as a good risk. A few key controls that are consistent across the market:
  - » Multifactor authentication (MFA) for remote access, cloud applications (including email), Remote Desktop Protocol (RDP), and network administrators.
  - » Protection and segmentation of backups.
  - » Endpoint detection and response.
  - » Regular employee training and testing.

Insurance companies also are managing limits and retention. Gone are the days of $10 million limits with a $25,000 retention. Most carriers are limiting their maximum capacity at $5 million except on well protected larger risks, and others are implementing minimum retentions for different levels of capacity. For example, it is unlikely you will see lower than a $100,000 retention of a $10 million limit from any one carrier.

Why Does This Matter for Contractors?

There has been a misguided assumption in the industry that banks, retailers, and companies holding consumer information were the only ones at risk for a major cyber incident. Those days are gone as cybercriminals have shifted towards the easiest targets they can find. In addition to stealing confidential information, many of these cybercriminals are now locking up critical computer systems and demanding hefty ransoms to unlock them, as mentioned above. As we have seen recently with the Colonial Pipeline, JBS Foods, and many others, all business sectors can be targets of cyberattacks.

In the recent past, there have been many examples of cyber losses within the construction industry:

- A large general contractor used a third-party cloud service provider to store information. When the cloud service provider experienced a major breach, the contractor was left defending itself and suffered a large loss of nearly $1 million.
- A cybercriminal hacked into an electrical contractor's network when they noticed it was susceptible to attack. The estimated loss was just under $500,000.
- A concrete contractor's CEO opened a phishing email containing malware that penetrated their network, and a regulatory investigation followed. The cost of the loss and fines was around $200,000.
- A highway contractor's employee lost his tablet while on a job site. The tablet was stolen, and sensitive data was removed. Many subcontractors filed lawsuits against this contractor, resulting in a loss of nearly $200,000.

A robust cyber liability insurance policy is a key risk management tool for contractors, along with the strong internal controls previously mentioned. Many property insurance policies and some general liability policies will throw in some form of cyber/data liability coverage, but it is often very narrow in scope and does not provide adequate protection. As such, all contractors should consider a standalone cyber liability policy as part of their overall risk management strategy. This risk is not going away any time soon, so reach out to an experienced risk manager to learn more.

References and Resources

1. Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound, Coveware, Inc. https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound?rq=2021