AMWINS®

Security is Key to Accessing
Public Entity Cyber Liability Insurance

In the last 24 months, more has changed for public entity insurance coverage than in the past 24 years combined, and it has almost everything to do with cyber security and cyber liability insurance.

Public entities are particularly vulnerable to cyberattacks because their budget allocation for cyber security is often less robust than other industries and hackers can more easily access their systems. Additionally, public entities provide crucial services to a large and diverse constituency, so business disruption is especially problematic for them.

These complications combined make public entities prime targets for ransomware attacks and extortion because entities are more likely to pay the ransom to avoid lengthy or dangerous (e.g., police and fire protection) disruptions.

The growing prevalence of ransomware has changed the landscape of the cyber insurance marketplace dramatically.

What began as concerns over compliance with Payment Card Industry Data Security Standards (PCI) and an industrywide focus on insurance products for first-party privacy/data breach exposures, has quickly morphed into a business continuity backstop with high recovery costs.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.

As a result, some carriers have pulled out of the marketplace entirely and non-renewed most all tough risks (pools, high limits, etc.), while others have reduced capacity on renewals. The carriers remaining in the market often require ransomware supplementals to even consider risks.

Pricing has skyrocketed, retentions have been adjusted, limits have been cut, and making matters even more difficult, underwriting requirements for security controls have become mandatory (no multi-factor authentication (MFA) on your network means no quote).

Public entities who have not budgeted for improvements to cyber safeguards are finding they are woefully unprepared to seek coverage in the current marketplace.

This article explores the state of the cyber insurance market and how public entities can access the limited coverage available by improving their cyber security and adding safeguards.

State of the Market

The July renewal rush was a picture like the day after an earthquake or hurricane—damage all around and everyone evaluating where they stand. More carriers have opted to stop quoting, shifting instead to excess only, or restricting their appetite to a narrow band based on size or population.

Submissions, however, have not slowed down as clients who need coverage are seeking it even in this distressed market. With capacity continuing to shrink and moratoriums on new business, finding alternate cyber options or replacing lost capacity has become even more challenging.

Current Trends

- Aggregate limits rarely exceed $5M, often smaller.
- Retentions are significantly higher—often $1M+ even for risks that were accustomed to $50K or $100K. Minimums are $250K-500K for mid-market clean risks.
- Many carriers will not drop down over sub limits on underlying carriers, which poses a problem for key coverage like e-crime and ransomware
- Carrier scans are being used more frequently in underwriting, but there are often weak spots that can be outdated or inaccurate. Some carriers will share their scans on request.
- Very few markets are available for pools due to the challenge of securing separate apps and carrier willingness to review them. Many carriers will not underwrite pools.
- Risks without proper controls get declined and those with losses are frequently declined.

Threat actors are moving faster than insureds and carriers and it can be difficult to put controls in place to avoid attacks, but the message from the market is clear—clean up the security controls and spend money on safeguards, or cyber insurance may not be available.

What Can Retail Brokers Do to Help Clients?

Retail brokers need to educate insureds on the current state of the market to avoid surprises for upcoming renewals, help insureds understand the services available to improve cybersecurity, and package submissions to make the insureds a more attractive risk to carriers.

Market

Carriers have a sharp focus on organizations that have implemented controls and safeguards. Insureds that don't address MFA, domain servers, remote desktop protocol (RDP), and patches will continue to be without options, especially if they renew later this year.

The primary security control that insurers are looking for today is MFA. Underwriters are looking for MFA to be deployed for remote access (whether through a VPN or otherwise) for email, on privileged IT accounts, and for securing backups.

Ideally, underwriters also want insureds' risk mitigation practices to include endpoint detection and response (EDR) tools, system and organization controls (SOC), comprehensive business continuity and disaster recovery planning, as well as frequent testing and training exercises.

Services for Improvement

Insureds with coverage currently in place should contact their carrier and see what cyber security assessment services are available, whether complimentary or for a fee, to review their security controls and help them implement changes so they are set up for their next renewal. Most carriers have risk services and links to vendors with services.

Insureds with restricted coverage (e.g., low limit or no ransomware) should consider hiring outside vendors to conduct a full assessment of their systems. The spend is anywhere from $5K to over $100K, but the review should provide more than just a best practices list—make sure it includes specific suggestions tailored for the insured's system, as well as help implementing the changes.

Submissions

It's important for insureds to put their best foot forward, so submissions need to detail all the risk management practices the insureds are implementing.

If the risk management controls that underwriters are looking for are not revealed in the insureds' submissions, or if the security and disaster recovery posture is not satisfactory, underwriters are either declining the business altogether or applying onerous sub limits and/or coinsurance for ransomware.

Those policy restrictions are then applied to all claims where the genesis is ransomware. So, the sub limit and/or coinsurance not only applies to the ransom payment itself, but also extends to the business interruption losses, data restoration losses, etc.

Takeaway

It's nearly impossible to predict the next move of cyber criminals and how it will impact organizations. We also can't know how the insurance marketplace will react—whether carriers will continue to have an appetite for public entity risk or how they will manage their cyber risk portfolio.

What we can do is keep our insureds updated on the current coverage restrictions we are seeing and advise them to choose risk management strategies that help protect them from exposures. We can also help connect current and potential insureds with assessment services that will address system shortcomings and help make insureds a more attractive risk to carriers.

About the Author

This article was authored by Dave Weller, EVP and Professional Lines specialist with Amwins Brokerage in Los Angeles, CA.