AMWINS®

Want Access to Public Entity Cyber Liability Insurance?
Make Sure You Have Security Measures in Place

Two years ago, pricing for public entity insurance coverage skyrocketed, retentions were adjusted, limits cut, and underwriting requirements for cyber security controls became mandatory. And while the general perception is that the market has leveled out and softened a bit, that just doesn't hold true for public entities.

The reality is that only those insureds with top tier, platinum level cyber security are seeing flat or even decreased premiums. And even then, the insured must check all the boxes for controls.

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.

For risks that fall short of top tier or are lagging in cyber security levels, premiums and retentions will continue to be inflated, and key coverage will carry a low sub limit for ransomware/extortion, systems failure, dependent business interruption, etc.

What we now refer to as "Cyber Liability" began as website content and concerns over compliance with Payment Card Industry Data Security Standards (PCI), as well as an industrywide focus on insurance products for first-party privacy/data breach exposures. Over the last two years, it has quickly morphed into a business continuity backstop with high recovery costs due to extortion, ransomware and email compromise.

CONTACT

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

LEGAL DISCLAIMER

Courtesy of Amwins Group, Inc.

State of the Market

Public entities who have not improved cyber safeguards since our last report are finding they are woefully unprepared to seek coverage in the current marketplace. The message is clear: clean up security controls and spend money on safeguards, or cyber insurance may not be available.

We haven't seen many new carriers enter the space except for top tier risks, and only insureds with top-of-the-line cyber security measures are likely to see flat rates or premium reductions at renewal. However, some carriers have begun to selectively write risks they want to consider, likely the result of premiums at acceptable levels and more groups having better controls in place than last year.

Most public entities can also expect to see sub-limits for key coverage (ransomware/extortion, systems failure, dependent business interruption, etc.), limits management, increased or stable retentions, and if they qualify, flat rate or minimal rate decreases.

Current Trends

- Aggregate limits rarely exceed $5M, often smaller.
- Retentions are stabilizing but not coming down.
- 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.
- Public entity pools and school pools continue to have limited niche carriers with a burdensome underwriting process and complex coverage triggers. Solutions exist but are not openly offered in the marketplace.
- Risks without proper controls (such as multi-factor authentication/MFA, EDR and many others), as well as those with losses, are frequently declined.

Retail brokers should educate insureds on these trends to help avoid surprises for upcoming renewals, aid insureds in understanding the services available to improve cybersecurity, and package submissions to make 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.

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

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

Services for Improvement

As carriers are implementing more aggressive risk security services as part of the renewal process, insureds must show active improvement in their cyber defense measures.

Insureds with coverage currently in place should contact their carrier to determine what cyber security assessment services are available to review their security controls and help them implement changes so they are set up for their next renewal. Almost every carrier offers complimentary services to help insureds improve their cyber security measures, including online educational material, direct conversations with internal risk assessment teams, and third-party vendors (sometimes for a fee). If you need help evaluating and improving your security posture, click the box to the right to learn more.

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 $5,000 to more than $100,000, and the review should provide more than just a best practices list—make sure the review includes specific suggestions tailored for the insured's system, as well as help implementing the changes.

Amwins offers our clients discounts with industry-leading cyber security service providers.

Submissions

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

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

Those policy restrictions are then applied to all claims where the genesis is ransomware. Therefore, 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

Given that public entity cyber markets are limited and highly specialized, underwriters tend to decline brokers without public entity expertise. They just don't have the bandwidth to work through accounts that are not prequalified.

Partnering with a Professional Lines Public Entity specialist from Amwins to review a risk, access markets and evaluate a carrier's coverage offering and services can make the difference. We understand that communicating expectations and sharing details about the state of the public entity marketplace are key to managing the public entity cyber liability cycle and helping insureds become a more attractive risk to carriers.