AMWINS

State of the Market: A Focus on Cyber

In a time where many insurance segments remain entrenched in a hard market, cyber continues to be the exception, with renewals coming in at level or below expiring pricing. Although claim activity continues to increase, underwriters are approaching placements and renewals with a positive mentality. And until loss ratios begin to produce widespread concern, we anticipate conditions will remain soft.

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.

09.24

Pricing and capacity

Just a few years ago, carriers were increasing rates well into the double digits on both new and renewal business, with difficult classes (such as manufacturing and municipalities) seeing spikes of 40% or more. There was ample capacity, but carriers were managing that capacity more carefully, requiring brokers to layer in order to get larger deals done. Ransomware was a key concern, with sublimits often being applied to the coverage, while MFA was the key control underwriters sought (including off-line backups and syncing to the cloud).

Conditions began to change by late 2022 and, since early 2023 the Cyber market has softened considerably. Many insureds have seen a reversal of fortunes from the hard market with decreases in premiums of 30% or more, depending on the size and complexity of the risk.

Underwriting appetite has expanded as well, and we are seeing more carriers consider higher-risk operations (e.g., casinos, payment processors, fintech, cannabis and crypto). Municipalities are still difficult due to a general lack of cyber controls, but more underwriters are willing to quote competitive rates as well as terms and conditions than a few years ago.

Along with significant decreases in rates, terms and conditions have improved as well. Insurers are more willing to eliminate sublimits and coinsurance, including on ransomware. Capacity has increased, both from new entrants as well as existing carriers showing a willingness to offer up to $10M. We are seeing higher sublimits for cybercrime including phishing and social engineering as well as reputational harm loss, dependent business income loss and dependent system failure.

Pricing and capacity (continued)

Despite the overall improvement in terms, conditions and pricing, retailers and buyers should be aware that not all cyber forms are created equally. While the current product may seem to be commoditized (especially compared to its early days), new and recycled coverage variations and restrictions are entering policy forms buried deep within the wording. Specifically, many markets that write direct to retailers inundate their quotes with restrictive endorsements and exclusions.

When comparing quotes, look for the following coverage issues:

- **"Reimbursement" ransomware language instead of "pay on behalf" of the insured.** A reimbursement provision can create a cashflow crunch, particularly for small- and medium-sized businesses that fall victim to attacks.
- **"Unsupported software" exclusions** returning to the cyber space (not just tech E&O).
- **War exclusions.** Insurers remain concerned about the growing potential for cyber incidents as a result of cyber warfare. These exclusions lack standardization across policy forms, so it's important to review them carefully and understand the effects.
- **Restrictions on where data is stored** (i.e., requiring contracts in place with vendors for coverage to apply).
- **Social engineering callback provisions** (i.e., denial of coverage if certain verification protocols are not followed by the insured), including onerous smaller sub-limits for client phishing, invoice manipulation and telecom fraud / crypto jacking.
- **Restriction on what/whose funds/money/securities are covered**, in-addition to "other property" losses being excluded.
- **Exclusions for biometric privacy violations**
- **Exclusions for website tracking, pixel tracking and illegal surveillance**
- **Inordinately long waiting periods for business income loss** (and system failure related to Business Income Loss), dependent business income loss (and system failure related to dependent business income loss) and reputational harm loss.

Claims trends

The biggest concern in the cyber space continues to be ransomware due to the severity of demands and payouts, unpredictability in targets and rising frequency. As reported in our **2024 market outlook**, there has been surge in ransomware claims and "double extortion" attacks (holding data hostage for payment as well as threatening to release sensitive data publicly or on the dark web).

However, there are mitigating factors to this trend. First, businesses continue to harden their defenses against ransomware, including putting stronger multifactor authentication (MFA) controls in place. This is important because human error and vulnerability continues to be a key attack vector for cybercriminals. Additionally, although ransomware attacks are up, payments are down. Ransomware attacks involving payments **decreased by 46% in 2023**, with the decline in payments attributed in part to "enhanced cyber resilience" including both defense against and recovery from attacks.

The industry continues to watch an increase in class action lawsuits surrounding wiretapping, illegal surveillance, pixel tracking, biometrics and California Privacy Act claims. Some carriers have moved to exclude these claims in their coverage forms. Many other carriers are providing sub-limits for biometrics and excluding outright any intentional unlawful tracking of protected information. We are seeing an inundation of class action privacy lawsuits related to these areas, as well as allegations of illegal wiretapping and illegal surveillance especially in sectors like health care, consumer-oriented companies and technology software as a service (SAAS). Further, we are seeing a rise in TCPA and solicitation type suits being directed at companies for targeted data collection and targeted advertising.

Be on the lookout

Non-IT dependent business interruption looks to be an area of future focus. Not all dependent vendors are exclusively IT in nature. The cyber underwriting marketplace has once again stepped up with evolving wording to cover dependencies on non-IT products and services suppliers affected by a cyber peril, but coverage scope and limits available vary across the marketplace.

Retail agents should be on the lookout against pushing non-IT dependent business interruption and system failure updates. Standard markets are now only beginning to offer these coverages, but we typically see them sublimited drastically compared to the policy aggregate. NOTE: This can be an area of coverage that can be a cause of confusion, so it's important to continue to press education surrounding this topic as well as ask the necessary questions to ensure that an insured doesn't have a financial loss exposure to non-IT dependent business interruption vendors.

Takeaway

We expect the market to remain soft, particularly as underwriting, processing and servicing efficiency grows in the small- to mid-size space. However, there are areas of concern, as described, which could cause market conditions to change.

Further, system risks for larger accounts and specific vendors continue to give the industry pause and concern, especially for large scale vendors like Microsoft Azure, Google Cloud, **CrowdStrike** and Palo Alto Networks. And there is wide variability of coverage among different carriers and products.

In this ever evolving and complex sector, Amwins continues to press to expand coverage for insureds, evaluating and analyzing carrier terms and conditions for our retail agent partners.

Partnering with a wholesaler like Amwins, one that understands the marketplace and has the underwriter relationships and solutions to write and retain business, is crucial. We remain on the forefront of the evolution of cyber insurance products with offerings such as **Amwins IQ** and **Amwins DNA** while our specialty brokers are focused on the cyber space, with crucial and intimate partnerships with both our carrier and cyber partners.

Insight provided by:

- Matt Donovan, RPLU, EVP with Amwins Brokerage in Atlanta, GA
- Charles Grodecki, RPLU, EVP with Amwins Brokerage in Charlotte, NC
- Steve Vallone, EVP with Amwins Brokerage in Lafayette, CA