AMWINS®

CrowdStrike Outage: Market Impacts and Coverage Implications

Last week, CrowdStrike rolled out a content update that was linked to crashes and outages affecting more than 8.5 million Windows devices. Businesses across the globe in industries ranging from banks, airlines, healthcare providers, telecommunications, and more were affected by the outage.

Although most systems are up and running again, it is impossible to know yet the full extent of the damage, and possible lingering effects.

Reflecting the current softening trends in the cyber market, Amwins **proprietary** benchmarking data shows that among the heavily affected industry sectors, the median rate per million ranges from $3.2K to $7.3K. With 56% of our insureds purchasing a $1M cyber limit, these losses could have a material impact on loss ratios if even a portion are covered under their respective cyber programs.

If insureds are unsure how insurance coverage may come into play, they should contact their retail broker to review their policy wording and discuss claims reporting. Amwins' professional lines teams are here to provide our retail partners with support and guidance on coverage issues related to this event or upcoming renewals that may be impacted by losses.

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.

Market effects

As with any event, carriers are grappling to understand the full extent of the issue and how it may impact their books.

We have already begun to see an emphasis on maintaining the integrity and sustainability of the cyber and technology E&O marketplace as well as certain carriers including exclusions for losses arising out of the CrowdStrike incident.

Based on the particulars of this event and past experience, we also expect to see the following market response:

- Additional exclusions around systemic events and relating loss.
- A push for clarity and consistency in approach around business interruption and system failure wording within cyber policies.
- Shared losses across other lines of coverage as the market seeks to determine the extent of liability, including but not limited to Technology E&O (or other E&O) and Directors & Officers Liability.

Amwins is here to help

Even with robust security protocols and training for employees, there still exists the threat of loss from a cyber incident. Cyber insurance provides another backstop for losses in such an event – but not all policies are created equal.

That's why having an experienced wholesale broker on your side to help you navigate a cyber event can lead to a more efficient claims process and lead to a better result for your clients.

As true cyber insurance specialists, the brokers in Amwins national professional lines practice group stay vigilant for our clients, and offer the following advantages:

1. Adept at navigating policy wording and market trends to secure the right coverage for accounts of all sizes and complexities.
2. Exclusive amendatory endorsements with key carrier partners to ensure consistency and quality in our cyber and technology E&O product offerings.
3. **Proprietary digital quoting platform** to streamline the quote process and offer competitive, vetted, and comprehensive quote options on a given risk.
4. Exclusive cyber solutions, and continually strive to develop innovative products and offerings as the market allows – standard is not our baseline!
5. **Proprietary benchmarking reports** with granular detail on cyber purchasing trends among accounts Amwins places, including limits purchased, common SIR's, and rate trends over time (for insureds with and without claims, and those with and without certain security controls).

For those affected by the CrowdStrike event

There are a number of potential coverage implications for affected entities resulting from this incident. It is important to note that cyber policies vary greatly and may not all apply uniformly (or at all) depending on the paper, form, or particular wording of each policy.

Business Interruption and System Failure

For impacted businesses, losses are growing largely due to system downtime. Inability to access their networks or systems not operating at full capacity due to a cyber event are typically covered under the system failure or business interruption sections of the cyber policy. This is further bifurcated into direct and dependent business interruption – whether suffered by a direct loss or degradation due to the insured's own actions or resulting from the outage of a business on which the client depends.

Many cyber policies carry full or sub-limited coverage for business interruption as well as expenses for interruption to first- or third-party networks.

Things to consider when reviewing cyber policies include:

- How long does the event need to last for the business interruption coverage to be granted? Waiting periods can vary both in time period and dollar amount.
- Do losses stop being calculated when the business' network is back up or when their operations are back to pre-outage conditions?
- Is there coverage for extra expenses incurred to revive systems – or simply for lost income/profits?

Claims Reporting

It is critical to advise insureds to do the following as soon as possible after an alleged or actual cyber event is discovered.

1. **Notify the insurer promptly.** Many cyber policies have limits on when an incident must be noticed to an insurer (often triggered by the discovery of an incident by an executive or employee). Insurers add these requirements so that their position is not prejudiced by latent reporting. With the time-sensitive nature of cyber claims, this point is critical.

2. **Engage their broker.** If there is a suspected incident, it is important for an insured to discuss with their broker what may be covered under the policy; notify the carrier according to the guidelines of the policy terms and conditions; and work with the breach coach to determine what next steps may be required.

3. **Detailed documentation.** It is also important to keep detailed documentation of the situation – as it is discovered, and as it evolves. Crucial facts for business interruption claims include, but are not limited to:

    - What happened
        - How and when was the incident discovered?
    - Impacted systems
        - When and how greatly were systems impacted?
        - o Which systems / networks were affected?
        - o For how long?
    - Effects on the business
        - What was the result of the degradation in systems? Was there lost revenue? If so, how much?
        - Were extra hours required from staff or third-party vendors to restore systems and bring them back online?

Don't hesitate to contact your Amwins professional lines broker with any questions or account needs during this time. We will leverage our full arsenal of expertise, market relationships, and resources to deliver the best result for you and your clients.