U.S. Risk, LLC

NEWS ALERT

Last week's CrowdStrike software update caused outages for millions of Microsoft Windows users, cost the economy potentially billions of dollars, and launched cyber policy claims for numerous businesses worldwide.

CYBERSECURITY: POST CROWDSTRIKE EVENT MANAGEMENT

Not all companies have adequate coverage for major disruptions. While many do, especially larger organizations, it will require a closer look to make sure any potential claims are handled properly.

Now's the time to review current cyber insurance coverage. Determine what policy(ies) provide coverage. Check notice of loss requirements, limitations, and any other coverage considerations.

- A well-crafted cyber policy should include broad business interruption coverage for losses caused by system failures of a vendor. But there are numerous limitations such as those providing coverage only to certain vendors/providers or only covering up to a sublimit.
- Payouts will be affected by individual policy wording, proof of financial loss, retentions, and deductibles.
- Waiting periods can come into play, typically with 12 hours being the most common.

› Take Steps Now

- Notify the cyber insurer as soon as possible of a potential loss to preserve your rights. Policyholders have already begun to notify insurers of system failure and business interruption claims and they are only expected to grow during the days ahead.
- Identify what the scope of impact has been on the business, and what it's predicted to be moving forward. Include specifics such as the exact time frame the disruptions occurred. Determine what specifically was affected, the amount of loss, what was normal and customary income vs. during the outage, which vendors were affected. Taking a tight measurement of damages now can help you optimize recovery.
- With the fix already provided by CrowdStrike, IT teams should already have addressed any disruptions, but crisis management and communications may still be needed to surround the restoration activities.

If you have questions about current policies or would like a policy review, contact one of our U. S. Risk cyber specialists.