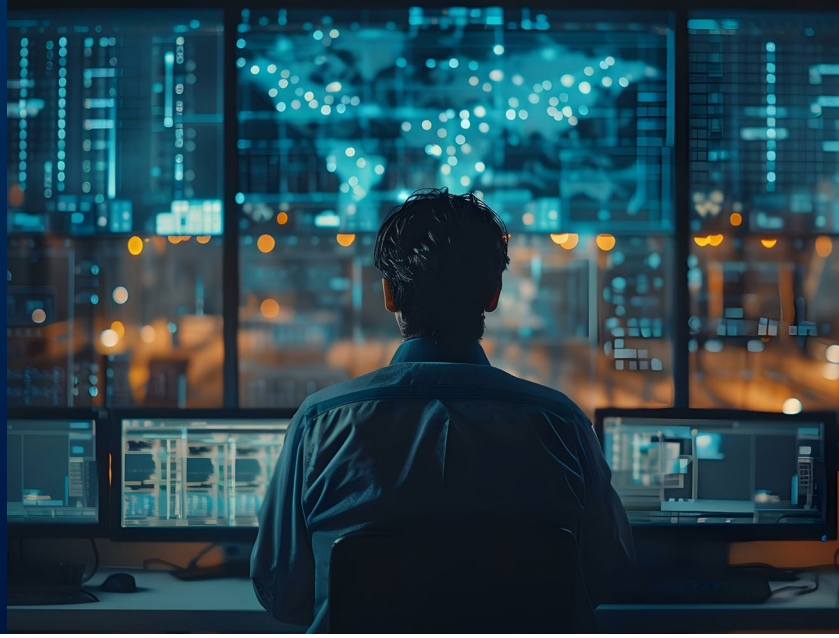
Brown & Brown

PROPERTY & CASUALTY

# Crowdstrike

## Insurance Considerations



Early reporting has estimated the CrowdStrike update failure to have cost businesses more than $5B, with assessments being made that 10% to 20% could be insured. It will be challenging to determine the credibility of this reporting, as notifications and the insurability of these claims are in the very initial stages of being assessed. As of this publication's date, which will likely evolve, market feedback indicates that the CrowdStrike outage is not anticipated to have a material impact on loss ratios. In fact, several cyber underwriting executives have commented that CrowdStrike is exactly the type of widespread event they have expected and price their risks with this eventuality in mind. Nevertheless, there is much to consider when considering possible insurance recoveries for claims. We unpack some of these policy complexities for you here.

## Systems Failure

The culprit in last Friday's event was a defect in CrowdStrike's Falcon update that ultimately resulted in significant IT outages. If the network interruption was on the network of an insured CrowdStrike customer, it could be deemed a first-party "Systems Failure," an extension to cyber insurance coverage. Whether the insurance contract provides for the extension will likely be considered. Systems Failure coverage extension to IT cybersecurity and threat detection services as part of the definition of "your Computer System" or "Network" may also be evaluated when making a Claim. This also may vary depending on the insurer's contract language.

## Contingent Business Interruption

Systems Failure as applied to Contingent Business Interruption will be a focus in assessing coverage where an insured's vendors were brought down, but this coverage extension varies by insurer. For example, some underwriters intend to cover dependencies such as cloud providers, operational technology, or payment processors. In that case, if a business relies on a cloud service provider to run operations and that cloud provider goes down, Contingent Business Interruption will likely respond. If CrowdStrike did not go down, but clients of CrowdStrike had business impacts due to a software failure, then Contingent Business Interruption will likely not come into play. Determining how Contingent Business Interruption is worded in a policy in terms of dependency and whether cyber security such as EDR (Endpoint Detection and Response) and threat intelligence are included as a covered vendor should be evaluated.

## Time Element Deductible or Waiting Period

The Time Element Deductible or Waiting Period and the Period of Restoration provisions will be another area of focus when evaluating a Claim. Information supporting how

long a system was down will be required. For a Claim to be triggered under most Business Interruption insurance clauses, the insured's systems or business must be down for a period of time, typically between eight to twelve hours for SME (Small to Medium-sized Enterprise) and Middle-Market businesses and up to twenty-four hours or more for large accounts, before coverage attaches. Cyber insurers want evidence and attestation that a network and operations were suspended to satisfy the waiting period. Components of your business may have been remediated earlier than others, and revenue streams may have returned partially as your business continued to work toward complete restoration. Quantifying Business Interruption can become complex when considering the totality of your network, what elements were impacted, the associated revenues, whether the waiting period was satisfied and how the Period of Restoration is defined.

## Customer Attrition

Another consideration is Customer Attrition as a direct result of the CrowdStrike event. Customer Attrition allows a company to recover losses after restoring the computer systems. For example, the airline industry faced cascading disruptions due to the scale of the IT failure. Some airline impacts included crew scheduling and logistics systems, which prolonged recovery. Whether customers of an airline determine they would rather fly with an alternative carrier and the widespread loss of customers can be evaluated.

Some cyber insurance policies will limit coverage for loss of income from the time your network went down to the time it was restored. In contrast, others will extend coverage for Customer Attrition to include the residual impact to determine the total financial loss. The extent of this coverage and the amount of time granted to determine the full impact of Customer Attrition may vary. Quantifying the impact by evidencing historic revenue trajectories and disruption as a direct result of the CrowdStrike incident will likely be challenging. It may require forensic accounting services and negotiations with your insurance carrier.

## Supply Chain Coverage

Another element of coverage that could be tested is whether Contingent Business Interruption includes non-IT dependencies such as companies in the product supply chain. For example, hospitals reliant on medications and manufacturers dependent on raw materials may experience disruption to their supply chain, causing delays in their ability to provide products and services. Contingent Business Interruption due to non-malicious acts impacting an insured's third-party dependencies outside their IT network and vendors is another area of the cyber insurance contract to evaluate.

## Extra Expense

Extra Expense is also another coverage consideration. Questions will be: did the incident require employees to work overtime, are those employees salaried or paid hourly, and were third parties employed to assess, test or assist in the recovery? The level to which employee costs can be covered under cyber policies can differ and will be a part of the calculations when the claim comes to be adjusted.

## Financial Deductible

Besides fulfilling the time element deductible or waiting period, insureds might also be responsible for the financial deductible. Whether you incurred a loss of income, even after satisfying the waiting period, will be considered. As an example, consider an insured that has a waiting period of twelve hours and a financial deductible of $500,000., If it is determined it took twenty-four hours for the insured to fully recover, satisfying the waiting period, but the loss of income was only $250,000, coverage will not apply. Some policies only require the waiting period to be eroded for coverage to apply.

The CrowdStrike update presents a unique set of circumstances and the early reporting of its impact on the insurance industry gives us insight as to how widespread and costly it might be. However, insurers must assess numerous elements before a final determination can be made of whether coverage is afforded for each insured. Time will tell as insurers determine how many of their insureds utilize CrowdStrike, whether those insureds will be making a claim and the intricacies of coverage language as to how much it may cost the insurance industry. The ability of companies to recover quickly and efficiently seems to reduce worst-case scenarios envisaged by some. Brown & Brown will continue to provide updates as the event's size and impact are evaluated.

# How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

**Find Your Solution at BBrown.com**