LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

You Haven't Got Mail: Coverage Claims For Microsoft Outage

By **Carlton Wilde III and George Buckley** (November 16, 2026, 5:22 PM EST)


Carlton Wilde


George Buckley

Shortly before 1 p.m. Eastern time on Thursday, Nov. 12, email stopped.

Exchange Online, the engine behind Microsoft Outlook for hundreds of millions of business users, began refusing connections, and within hours Teams, SharePoint, Copilot and Defender XDR were degraded or unavailable across 74 countries. The disruption ran through the Asian and European business days and into Friday in the U.S., with Microsoft reporting only marginal success with repairs for much of that period.

Microsoft did not declare service restored to all remaining customers and regions until early Sat., Nov. 14, roughly 36 hours after the first reports.

Microsoft has said the event was not a cyberattack.

In a preliminary post-incident statement posted by a Microsoft executive on X on Nov. 16, Microsoft attributed the outage to three factors that combined to take down the networking gateway that fronts Exchange Online and other Microsoft 365 services, including a latent software defect introduced in July that had run globally for more than three months without incident, a surge in gateway load after Teams failed over onto the same gateway roughly 15 hours earlier as part of normal operations, and the temporary loss of nearly 14% of gateway server capacity to an unrelated issue the day before.

Under that load, the defect caused servers to stop responding, traffic was automatically redirected to the remaining servers and the failure cascaded until more than 80% of the fleet was unresponsive. Microsoft also acknowledged that the partitions designed to contain such a failure did not hold, that Exchange Online, unlike Teams and SharePoint, could not fail out of the affected gateway, and that its normal rollback tools could not revert a defect that had been in place for months.

Microsoft's characterization of the incident matters enormously to policyholders, because a nonmalicious, nonphysical outage at a third-party provider is the exact scenario in which commercial insurance programs tend to be least coherent. Cyber policies were built around hackers. Property policies were built around fire and wind. Liability policies were built around someone else getting hurt.

Last week's loss fits none of those templates neatly, and that is why the claim process will turn on specific wording rather than on the size of the headline.

For corporate policyholders, particularly in the energy, industrial, healthcare, real estate and private equity sectors, the first week after an event like this is when recoveries are won or lost. Below are the coverage questions we expect to dominate the next several months, and the steps that should be taken now.

Cyber Policies: Trigger, Dependency and the Clock

Most cyber policies written today include some form of business interruption coverage, but three features of the form will decide whether last week's loss is covered at all.

The Trigger

Older and narrower forms respond only to a "security failure," meaning an actual or suspected unauthorized access, malware event or denial of service. Microsoft's own statements that no malicious activity was involved will be the first thing an adjuster reads.

Policyholders need a "system failure" or "unplanned outage" trigger, which covers an unintentional and unplanned interruption of computer systems regardless of cause. Microsoft's description of a dormant code defect exposed by a surge in load is the textbook unintentional and unplanned outage that "system failure" wording was written to cover, and precisely the kind of event a "security failure only" form will not reach.

Many policies added system failure coverage after the CrowdStrike event in July 2024, often by endorsement and sometimes with a reduced sublimit. Check whether the endorsement extends to dependent systems or only to the insured's own network.

The Dependency

Even with a system failure trigger, first-party business interruption in most cyber forms covers only the insured's own computer systems. An Exchange Online outage is a failure of Microsoft's systems, not yours. Recovery therefore depends on contingent or dependent business interruption coverage, and on how the policy defines the dependent provider.

Some forms cover any "outsourced service provider" or "cloud provider" under written contract. Others require the provider to be scheduled by name, or cave out "infrastructure" such as internet, telecommunications and utility providers.

Insurers may argue that a platform as pervasive as Microsoft 365 is infrastructure rather than a vendor. The policy language, and the way the insured's Microsoft agreements are papered, will answer that question.

Some carriers also introduced "widespread event" or systemic-risk sublimits and exclusions after CrowdStrike that specifically target a single provider failure affecting many insureds; those provisions have not been tested in court and should be read closely before accepting an insurer's reading.

The Clock

Cyber business interruption coverage is almost always subject to a waiting period, typically eight to 12 hours, and sometimes 24 hours or more for dependent coverage. The waiting period runs from the start

of the interruption, not from the time the insured noticed it or gave notice.

Last week's event exceeded eight hours for essentially everyone and exceeded 24 hours for many, so the waiting period should not bar most claims outright. But policies differ on what happens once it is satisfied. Under some forms, coverage runs retroactively from the first minute of the outage. Under others, only the loss after the waiting period expires is recoverable. For an outage that began midday in the U.S., that difference may be the bulk of the claim.

Insurers may also point out that much of the deadline duration fell outside U.S. working hours. Microsoft's own report undercuts that argument as it states that the failure occurred during the peak traffic window in the U.S. and that the cascading collapse took the fleet down in less than two hours.

Policyholders with overseas operations, overnight trading desks, 24-hour control rooms or healthcare facilities should be prepared to show that the hours lost were real.

Microsoft's account also supports measuring the period of interruption through actual restoration rather than through the first signs of recovery. Microsoft has acknowledged that recovering servers were immediately overwhelmed by waiting traffic and failed again, that its automated recovery processes were not designed for a failure of this breadth, and that it was warning customers of intermittent access and delayed delivery well into Friday.

A degraded or partial service is still an interruption under most cyber forms, and the claim period should run until the policyholder's own operations were functioning normally, not until Microsoft's status page turned green.

Two further points deserve attention. First, many cyber forms cover extra expense and mitigation costs separately from income loss, and often without a waiting period. Overtime, temporary communication tools, third-party IT support and manual workarounds should be tracked from the first hour.

Second, the period of restoration in cyber policies is frequently short, sometimes limited to 30, 60 or 90 days, and includes an extended tail only if negotiated. Catch-up costs and lingering disruption need to be captured within that window.

A third point arises directly from Microsoft's report. Microsoft states that Teams, SharePoint, OneDrive and the Office apps were able to fail out of the affected gateway and were restored earlier, with Teams chat and meetings functioning for most of the outage, while Exchange Online could not.

Expect insurers to argue that the interruption was partial and that workable alternatives existed. Policyholders should document, service by service and location by location, what was actually available to their users. A chat tool that functioned while email, calendaring, and the approval, scheduling, and notification workflows built on them did not cannot substitute for the dependent service the policy covers, and the loss calculation should reflect that.

Property and Business Interruption: The Physical Damage Problem

Traditional commercial property programs, including the all-risk and manuscript forms used by large energy and industrial companies, are built on "direct physical loss or damage." The postpandemic case law tends to apply that requirement strictly to losses with no physical alteration of property.

An email outage caused by a server configuration change at a Microsoft data center is a difficult fit, and we expect property insurers to deny most outage claims on that basis. Microsoft has made the argument easier by describing the root cause as a "latent defect" in its gateway software.

Latent defects, faulty design and faulty workmanship exclusions appear in nearly every all-risk form, and adjusters will quote Microsoft's words back to policyholders. The response is in the ensuing-loss exception found in most of those exclusions. Even where the defect itself is excluded, resulting loss from a cause that is not excluded may remain covered. That analysis is policy-specific and should be done before a denial arrives, not after.

That does not end the inquiry, however. Larger programs often contain endorsements that may respond regardless of physical damage at the insured's own premises:

- Service interruption or off-premises utility coverage is historically limited to power, water, gas and telecommunications. Many manuscript forms now define covered services to include "communication" or "data" services, and some expressly include cloud and hosting providers. Whether Exchange Online qualifies, and whether that endorsement still requires physical damage at the utility's facility, are wording questions that vary from program to program.

- Some electronic data and computer systems coverage forms treat corruption or loss of functionality of electric data as covered damage. Microsoft's own description, servers failing health checks after a settings change, may support an argument that the data or software was damaged in the sense those provisions contemplate.

- Contingent business interruption for "dependent properties" generally requires physical damage of a type insured at the supplier's location. That requirement is the central obstacle here, but the definition of "damage" and any data-related exclusions should be reviewed rather than assumed.

Our experience with Winter Storm Uri and various other pipeline and refinery contingent business interruption claims for energy companies is that dependent-property analysis is intensely fact-specific. The same is true here. The claim should be built on the actual service chain, which specific Microsoft services the business depended on, what the policy says about each and what the loss looked like hour by hour.

Liability Lines: When Your Outage Becomes Your Customer's Claim

The outage did not stop at corporate email. Companies that deliver services through Microsoft-dependent platforms, including software vendors, managed service providers, logistics and scheduling businesses, and healthcare and financial services firms, will face claims from their own customers for missed deadlines, failed deliveries and breached service-level agreements.

Technology errors and omissions and professional liability policies are the primary response. Watch for exclusions for contractual liability, for failure to perform a contract and third-party technology failures, and for insurer arguments that service-level agreement, or SLA, credits are a contractual obligation rather than damages. Early notice is essential because most of these policies are claims-made, and a customer complaint or demand letter may itself qualify as a claim.

Directors and officers coverage is less obvious but should not be overlooked. Public companies that

suffered material disruption may face securities claims if disclosures about operational resilience or vendor concentration are later alleged to have been misleading. Boards that have not addressed single-provider dependency as an enterprise risk may face derivative claims.

The CrowdStrike event generated exactly this type of litigation. D&O policies typically carry no waiting period and no physical damage requirements, and they may provide defense cost coverage that first-party policies will not.

General liability is unlikely to respond. Electronic data exclusions and the absence of bodily injury or property damage will defeat most claims, though companies that suffered downstream physical consequences, for example a healthcare provider whose patient care was affected or an industrial operator whose safety communications failed, should analyze their facts carefully.

Supply Chain and Contract Issues

Microsoft's commercial agreements generally limit remedies for service outages to service credits under published SLAs, and typically make those credits the customer's sole remedy. Credits should be claimed, but policyholders should not expect them to approach actual losses.

More importantly, check whether the insurance policy requires those credits to be deducted from recoverable loss, or treats them as "other insurance" or salvage.

Insurers will also be evaluating subrogation against Microsoft and may ask the insured to preserve contractual rights. This cuts both ways and should be managed deliberately.

Microsoft's preliminary report should also be read as a preview of its liability position. It emphasizes that the defect passed safe deployment and ran for more than three months without issue, that the Teams failover was part of normal operations, and that the service had sufficient headroom for the lost server capacity to be harmless on its own.

At the same time, Microsoft acknowledges that its load testing did not detect the defect because its test labs used weaker hardware than the production fleet, and that the bulkheads designed to contain a cascading failure did not work. Those admissions will be the focus of any subrogation or direct claim, but policyholders should assume Microsoft will defend the SLA credit as the exclusive remedy and plan their insurance recovery accordingly.

Companies that themselves have force majeure indemnity of SLA obligations to counterparties should review those provisions in parallel with the insurance analysis. A force majeure clause that excuses performance may reduce liability exposure, but a strong contractual defense can also be used by a liability insurer to argue that no covered loss exists.

Coordination between the commercial and insurance workstreams prevents one from undermining the other.

Industry Notes

Energy and Industrial

Operational technology and control systems were largely unaffected, but scheduling, nominations,

trading confirmations, regulatory filings and safety communications run on email and Teams.

Document the commercial consequences of missed nominations or delayed confirmations because these are often the measurable loss. Energy trading operations that run overnight should be able to demonstrate loss during hours insurers will assume were idle.

Healthcare

Patient communications, scheduling and referrals were disrupted. Where staff turned to personal email or unsecured messaging to keep working, that creates privacy issues and exposure under the Health Insurance Portability and Accountability Act that may itself become a cyber claim. Preserve a record of workarounds now.

Real Estate and Private Equity

Closing, wire instructions and diligence timelines were affected. The days following a major outage historically bring a surge in phishing and wire-fraud attempts as attackers exploit confusion about which emails are legitimate. Social engineering and funds transfer fraud sublimits in the cyber policy should be confirmed and employees reminded to verify instructions by phone.

Conclusion

Microsoft's outage may very well be described as a near miss for the insurance industry, as CrowdStrike and AWS were, because the aggregate insured loss may be a fraction of the aggregate economic loss. That gap is not an accident. Microsoft's own account makes the point that this was a defect no once could see, triggered by routine operations, at a provider no customer can audit.

This is the loss most insurance programs cannot handle well. It is the product of waiting periods, sublimits, physical damage requirements and trigger definitions that were drafted for a different kind of loss.

Policyholders who treat the next few weeks as a documentation and wording exercise, rather than a wait-and-see exercise, will be the ones whose claims close the gap.

Carlton Wilde III is a partner and leader of the insurance recovery group at Bracewell LLP.

George Buckley is an associate at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.