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

Data Center Insurance Boom May Obscure Claims' Difficulty

By **Carlton Wilde** (May 13, 2026, 4:22 PM EDT)


Carlton Wilde

An S&P Global Ratings report published on April 13 projects that insurance premiums tied to data center construction and operations could reach $10 billion in 2026, with annual data center investment expected to surpass $300 billion by 2030. For insurers, this represents what S&P calls a "meaningful growth opportunity." For the technology companies, developers and operators actually purchasing this coverage, the picture is more complicated.

The insurance industry's enthusiasm for this emerging market is understandable. Individual data center projects may eventually carry insurable values as high as $30 billion, which would dwarf most traditional infrastructure projects. But the rush of carrier capital into the data center space should not obscure the reality that policyholders face a distinct and evolving set of risks that existing insurance products were not designed to address.

As this market matures, policyholders must be proactive in understanding those risks and securing coverage that actually responds when losses occur.

Business Interruption: The Central Challenge

Of all the coverage issues that data center owners and operators will confront, business interruption may be the most consequential and the most likely to produce disputes. Traditional business interruption policies were built around stand-alone manufacturing or commercial facilities, where the insured's revenue stream is tied to a single physical location.

Data centers do not operate that way. A modern hyperscale campus is part of an interconnected network, and an outage at one facility can cascade across clients, services and geographies within seconds.

This interconnectedness creates several problems under conventional business interruption policy language. First, the concept of a "period of restoration" — the time frame during which business interruption coverage applies — may not map cleanly onto data center operations. Restoration in a traditional sense means returning a damaged facility to its preloss condition.

But for a data center operator whose clients have migrated workloads to other facilities during an outage, the economic harm may persist long after physical repairs are complete. Client attrition, service-

level agreement penalties and reputational damage can extend the financial impact well beyond the restoration window that a standard policy contemplates.

Second, dependent property and contingent business interruption coverage, which is designed to address losses caused by disruptions at third-party locations, will be critical for data center operators but is frequently sublimited or subject to restrictive triggering conditions.

A data center's dependence on third-party power providers, cooling infrastructure and network connectivity means that a loss originating entirely off premises can shut down operations just as effectively as an onsite fire. Policyholders should scrutinize whether their contingent business interruption coverage is broad enough to respond to these scenarios and whether sublimits are adequate relative to the potential exposure.

Third, valuation of business interruption losses at data centers presents its own challenges. The revenue generated per square foot at a hyperscale facility bears no resemblance to a conventional commercial building. A single rack of servers may support millions of dollars in client revenue. Policyholders need to ensure that their business interruption limits and valuation methodologies reflect the actual economic output of these facilities, not assumptions borrowed from other asset classes.

Property and Construction Risks

The sheer scale of data center projects introduces property risks that differ meaningfully from traditional commercial construction. The specialized equipment housed in these facilities — servers, networking hardware, uninterruptible power supplies and precision cooling systems — represents a concentration of high-value, difficult-to-replace assets.

Lead times for critical components can stretch to months, and in some cases, custom-fabricated equipment may have no readily available substitute. A property loss that might be resolved in weeks at a conventional facility could sideline a data center for far longer.

Builder's risk coverage during the construction phase warrants particular attention. Data center construction timelines are aggressive, and developers face enormous pressure to bring capacity online quickly.

Delay in start-up coverage, sometimes called advance loss of profits, is essential but often negotiated as an afterthought. Given that a completed data center may begin generating revenue immediately upon commissioning, even a modest construction delay can translate into significant financial losses that a policyholder will expect its builder's risk program to cover.

Environmental and regulatory risks also deserve scrutiny. Data centers consume enormous quantities of water for cooling and draw significant electrical power, often in jurisdictions where both resources are increasingly constrained. Regulatory changes affecting water usage, emissions or power consumption could force operational modifications that trigger coverage questions under property and business interruption policies.

Policyholders should consider whether their programs address regulatory-driven losses or treat them as excluded.

Cyber and Equipment Breakdown Risks

It may seem obvious that facilities dedicated to computing infrastructure face cyber risk, but the insurance implications are nuanced. Many property policies contain broad cyber exclusions, and stand-alone cyber policies may not adequately address the physical damage that a cyberattack can cause to data center equipment.

The gap between property and cyber coverage — sometimes called the silent cyber problem — is particularly acute for data centers, where a single intrusion could simultaneously cause physical equipment damage, data loss and prolonged business interruption.

Equipment breakdown coverage is another area requiring careful attention. Data centers depend on an array of mechanical and electrical systems operating in concert, e.g., generators, transformers, switchgear, cooling units and the servers themselves. A failure in any one of these systems can cascade through the facility.

Equipment breakdown policies can fill gaps left by standard property coverage, but policyholders must confirm that coverage extends to the full range of equipment in a modern data center and that the interplay between equipment breakdown and property policies does not create unintended gaps.

The Claims Complexity of Layered Programs

S&P's report acknowledges that no single insurer can absorb the risk associated with a $30 billion data center project. The industry's response of pooling risk across multiple insurance and reinsurance partners is a practical necessity, but it introduces significant claims complexity for policyholders.

A layered insurance program with multiple participating carriers means that a major loss will trigger coverage across several policies, potentially with different wordings, different claims-handling protocols and different coverage positions.

Policyholders in this environment need to think carefully about program architecture at the placement stage. Consistency of policy language across layers, clear allocation mechanisms for losses and preagreed claims protocols can make the difference between a manageable claim and protracted multiparty litigation.

The time to negotiate these terms is before the loss, not after.

Looking Ahead

The $10 billion data center insurance market is good news for policyholders in one respect: Carrier competition and capacity should, in theory, give buyers leverage to negotiate broader coverage terms. But premium volume alone does not guarantee that coverage will perform as expected when a loss occurs. As insurers compete for market share, some may offer coverage they do not fully understand, leading to disputes when novel loss scenarios arise.

Data center owners, developers and operators should approach this market with clear eyes. The risks are real, the coverage gaps are identifiable, and the time to address both is now while carriers are eager for the business and the negotiating leverage favors buyers.

Waiting until after a loss to discover that a policy's business interruption language does not account for interconnected operations, or that a cyber exclusion eliminates coverage for a physically destructive attack, is a mistake that the scale of these projects makes unaffordable.

Carlton D. Wilde III is a partner at Bracewell LLP.