Key Insurance Coverage Considerations For AI Data Centers

By **Sergio Oehninger and Garrett Nemeroff** (September 5, 2025, 3:39 PM EDT)

The burgeoning artificial intelligence industry has sparked a surge in data center projects across the U.S., a trend likely to be further accelerated by measures announced in July by the White House as part of its AI Action Plan. But these complex facilities come with equally complex risks, raising several key insurance coverage considerations for policyholders in the data center industry.

Surge in Data Center Projects

Sergio Oehninger

Data centers are the physical infrastructure supporting today's AI platforms. While thousands of data centers already exist across the U.S., a Gartner report estimates that $475 billion will be spent on data centers in 2025 alone, with McKinsey expecting total spending to exceed $5 trillion by 2030.[1] McKinsey forecasts roughly $7 trillion in global spending on data centers over the next five years.[2]

As part of its AI Action Plan, the U.S. presidential administration announced measures aimed at accelerating the development of these projects in the U.S. On July 23, the White House issued an executive order to provide federal funding for data center projects, streamline the permitting process for key infrastructure and expedite environmental reviews.[3]

Garrett Nemeroff

On July 24, the U.S. Department of Energy also announced plans to develop AI infrastructure projects on federal lands, soliciting bids from the private sector to build data centers in South Carolina, Tennessee, Kentucky and Idaho.[4]

These public sector initiatives are the latest development in the ongoing data center boom, driven by the enormous data processing power needed to support today's AI platforms. As AI platforms continue to become more prevalent across a variety of industries, data centers also become critically important to develop, maintain and insure.

Key Insurance Coverage Considerations

Given the sheer scale and complexity of AI data centers — featuring massive multibuilding properties housing thousands of computer servers, critical equipment and important technology — data centers involve several significant and complex risks. In light of these risks, policyholders should consider several important insurance coverage issues in the data center context.

Builders Risk Coverage

One critical type of insurance coverage for any construction project, and especially modern data centers, is builders risk insurance.

Builders risk insurance generally protects against physical loss or damage to property during the construction process: not only the buildings or structures, but also the materials, equipment and machinery used in the construction process.

Depending on the policy language, coverage might exist for loss or damage while these components are on-site, stored off-site or in transit. Builders risk policies may also cover lost income and additional costs, including soft costs such as design and engineering fees, resulting from delays in the construction process.

Data center projects involve the design, manufacture, and installation of complex equipment and expensive computer hardware, including racks of powerful data processors known as GPUs, cutting-edge computer chips, and critical cooling equipment needed to keep systems running. To protect against loss or damage during the data center construction process, policyholders must have adequate builders risk coverage and limits.

Property and Business Interruption Insurance Coverage

Commercial property insurance policies generally protect against physical loss or damage to the insured property after construction is complete, in addition to attendant business income losses. Property policies can contain standard industry forms, manuscript forms with customized language negotiated between the broker and insurer, or a combination of the two. In the data center context, there are several key property insurance issues to consider.

Covered Property

First, policyholders that own or operate data centers should ensure that their property policies cover the entirety of the data center operation, encompassing all structures, infrastructure, equipment, computer systems, technology and business personal property.

What constitutes "covered property" depends on the specific definitions, exclusions and schedules in the policy. And while most property policies define "covered property" to include the buildings, structures and equipment at the insured's location, some policies might exclude or impose "sublimits" for certain properties or components. Moreover, property policies often exclude coverage for loss of electronic data — a critical issue for data centers.

Data centers continue to grow in scale, cost and complexity, increasingly featuring sprawling campuses comprising multiple buildings, complex infrastructure and expensive computer equipment. Ensuring sufficient coverage for the entirety of the data center property is step one.

Covered and Excluded Risks

Policyholders in the data center industry should carefully review and familiarize themselves with the

covered causes of loss under their property policies, again paying close attention to any exclusions or sublimits.

Property policies can provide crucial protection for loss or damage caused by fires, storms, earthquakes, water damage, high or freezing temperatures, and explosions. Property insurance policies might also provide specific "equipment breakdown" coverage, adding an important layer of protection for mechanical or electrical breakdowns.

At the same time, property policies can include a wide range of exclusions; for example, property policies often exclude coverage for certain types of water intrusion, flood damage, faulty construction and design, and deterioration and erosion.

AI data centers involve complex mechanical and electrical equipment that could be susceptible to fires and breakdowns, liquid-based cooling systems that may be susceptible to leaks and condensation, and expensive computer hardware that could be incredibly costly to replace.

As such, any fire or water intrusion incident could be disastrous for data center operators. Policyholders should closely review and negotiate their property policies to maximize coverage for the risks of physical loss or damage to data center properties.

Business Interruption Coverage

In addition to the significant property damage risks, because AI data centers operate 24/7, continuously processing massive amounts of data, another key risk facing data centers is the possibility of power failures and other system interruptions.

Commercial property policies often include business interruption coverage, which generally applies when a policyholder is forced to suspend operations at the insured property — often resulting in lost revenue and increased operating expenses. Property policies generally limit business interruption coverage to situations where some physical loss or damage to the property precipitated the closure, but the scope of coverage depends on the policy language.

In some cases, policyholders can obtain contingent business interruption coverage, a broader business interruption coverage triggered by physical loss or damage to an entirely separate property. Contingent business interruption coverage is another key feature for policyholders to consider as data centers increasingly span multiple properties and rely on suppliers and manufacturers that operate from entirely different properties and locations across the global supply chain.

Among other exclusions, property policies might exclude losses caused by certain types of power failures, including utility services exclusions that might bar coverage for losses due to the failure of communication or power supply services. Because the data center boom is reportedly beginning to strain existing U.S. power grids, policyholders in the data center industry should also carefully review any exclusions related to power failure interruptions.[5]

Cyber Coverage

By their nature, AI data centers also raise significant cyber risks, spanning data breaches, ransomware attacks, computer system failures or violations, data privacy liability, and potential third-party liability to clients, customers and shareholders.

At the same time, as with other insurance policies, cyber policies typically contain several exclusions. For example, cyber policies often exclude coverage for cyber incidents caused by the policyholder's failure to follow cybersecurity measures, war or terrorism risks, and social engineering, unless such coverages are "bought back" by endorsements or otherwise. And given the new and evolving risks associated with generative AI, insurers might begin to adopt AI exclusions.

Cyber coverage is essential in the data center context. Policyholders should closely review, understand and negotiate the terms of their cyber policies, including at the time of renewal, to ensure that they obtain appropriate coverages and policy limits.

Liability Coverages

Data center construction projects have also led to disputes with surrounding residents and communities. Many data centers are located near residential areas and have reportedly led to construction vibrations and excessive noise in nearby homes.[6] Recently, a proposed $30 billion data center campus in Mooresville, North Carolina, drew sharp objections from the surrounding community over its prospective impact on natural resources and wildlife. These disputes highlight the potential liability risks and exposure surrounding data center projects.[7]

A wide range of liability policies can protect against claims and lawsuits involving data centers, including commercial general liability and errors and omissions policies.

CGL policies generally provide coverage for claims or lawsuits alleging bodily injury, property damage, or personal or advertising injury arising from the policyholder's business operations. As such, CGL policies might apply to potential lawsuits alleging bodily injury or property damage due to construction hazards, vibrations or sounds emanating from data center projects.

Further, E&O policies can provide coverage for claims arising from professional services, such as engineering and design services. To the extent data center developers or operators engage engineering consultants and design professionals, it is important to ensure that adequate E&O coverage is in place and review and negotiate additional insured provisions to minimize any gaps in coverage.

Conclusion

Modern data centers raise a broad range of important insurance coverage issues. Given the increasingly complex risks associated with data center projects — including massive development, construction, management, and operational costs and related exposures — policyholders in the AI industry should carefully review and negotiate their insurance policies to ensure that coverage aligns with those risks.

Sergio Oehninger is a partner and leader of the global insurance recovery practice at Morgan Lewis & Bockius LLP.

Garrett Nemeroff is of counsel at the firm.

[1] See https://ig.ft.com/ai-data-centres/.

[2] See https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers.

[3] See https://www.whitehouse.gov/presidential-actions/2025/07/accelerating-federal-permitting-of-data-center-infrastructure/.

[4] See https://www.energy.gov/articles/doe-announces-site-selection-ai-data-center-and-energy-infrastructure-development-federal.

[5] See https://www.reuters.com/sustainability/boards-policy-regulation/americas-largest-power-grid-is-struggling-meet-demand-ai-2025-07-09/.

[6] See https://www.bloomberg.com/news/features/2025-07-29/loudon-county-data-center-growth-strains-residents-seeking-ai-regulation.

[7] See https://www.nbcnews.com/news/us-news/dale-earnhardt-widow-son-battle-data-center-mooresville-north-carolina-rcna223895.