Gallagher

DATA CENTER CONSTRUCTION

Managing Risk for Contractors in a $100 Billion Market

Executive Summary

Overview

Data center construction exemplifies the need for precision under pressure. These are facilities in which performance expectations are absolute, timelines are unforgiving and the margin for error is minimal. Yet, the financial reward is considerable for contractors who are educated in the various unique exposures and leverage the insurance solutions crafted to help protect their investment.

Market Characteristics

- Data center construction is currently experiencing a full-scale infrastructure boom, fueled by the growth of AI, hyperscale cloud computing and enterprise digital transformation.
- The average data center project's value has grown to $633 million, a 70% year-over-year (YoY) increase.
- Construction costs now exceed $1,000 per square foot, nearly double the levels seen just two years ago.

Contractor Opportunity

- In January 2026, US data center construction starts reached a historic high of $25.2 billion.[2]
- With more than $100 billion earmarked for new builds in 2026, data centers represent the largest revenue source in the construction sector.
- In a market defined by speed, scale and precision, contractors must carefully manage multiple exposures while seizing the financial opportunity.

Unique Job Site Exposures

- Data center contractors face a spectrum of nonstandard construction risks that can incur severe penalties from the owner/operator.
- Fire, water, completion delays and natural catastrophes can be extremely costly.
- Coverage gaps must be carefully managed in builder's risk, general liability and professional liability policies.

An Immense Opportunity

The accelerated expansion of data center infrastructure presents one of the most consequential and capital-intensive construction opportunities in the US today. This specialized subset of commercial construction has evolved into a full-scale infrastructure boom, fueled by the explosive growth of artificial intelligence, hyperscale cloud computing and enterprise digital transformation.

For contractors, this shift represents a massive surge in demand, characterized by unprecedented project volume, aggressive timelines and increasingly complex execution requirements.

The numbers underscore the magnitude of this moment: 19 projects broke ground in December 2025, representing $12.5 billion in new construction.[1] Over the preceding 12 months, total data center construction starts climbed to $103.7 billion, with an average monthly spend of $8.6 billion.[2]

In January 2026, US data center construction starts reached a historic $25.2 billion, including megaprojects with individual valuations as high as $10 billion.[2]

The demand for new data centers is not expected to abate anytime soon. It is forecasted that as much as $3 trillion will be invested globally in AI-driven data center infrastructure by the end of 2028, with roughly half of that total allocated to construction.[3]

Why Managing Risk Is Critical for Contractors

For contractors, the opportunity is as compelling as it's demanding. The average data center project has grown dramatically in both size and cost, with 2025 figures indicating an average project value of $633 million (up approximately 70% year-over-year) and construction costs now exceeding $1,000 per square foot, nearly double the levels seen just two years ago.

At the same time, hyperscale clients (such as major cloud and social media platforms) continue to compress delivery timelines, often expecting facilities spanning 100,000 square feet and housing tens of thousands of servers to be completed in as little as 12 to 14 months, roughly the same time it takes to build a residential home. This combination of scale, cost intensity and speed-to-market expectations places intense pressure on contractors to execute with precision across the planning, procurement and construction phases.

"As the data center boom continues to reshape the construction landscape, contractors who recognize both the magnitude of the opportunity and the importance of strategic risk management will be best positioned to lead in this next phase of infrastructure development," says Brian Cooper, Gallagher's Senior Managing Director for US Construction.

The strategic importance of data center development continues to elevate the role of contractors within the wider technology ecosystem. These projects are no longer simply buildings; they are mission-critical assets that underpin global digital infrastructure. Expectations around reliability, resilience and performance have never been higher, and the margin for error has never been smaller.

For contractors who can successfully navigate this environment, the rewards are substantial: sustained project pipelines, larger contract values and deeper relationships with some of the world's most well-capitalized clients. However, capturing this opportunity requires far more than technical capability. The unique risk profile of data center construction — from high-value equipment exposures and tight commissioning schedules to evolving energy strategies and regulatory scrutiny — demands a mindful, sophisticated approach to risk management and insurance.

Experienced, trusted counsel is required for projects of this scale and complexity. Contractors must align with partners who understand the nuances of data center construction and can deliver tailored coverage, proactive risk engineering and access to specialized underwriting capacity.

In a market defined by speed, scale and precision, the ability to effectively manage risk is not just a protective measure. It's a competitive differentiator.

POWER AND WATER

The Defining Factors in Data Center Development

If the current wave of data center construction is defined by speed, scale and capital intensity, it's ultimately governed by a far more fundamental set of constraints: access to power and water.

As demand for AI-driven computing and cloud infrastructure accelerates, these two resources have emerged as the key determinants of where projects can be built, how they are designed and whether they are both economically and operationally viable over the long term.

Power

At its core, a data center is an energy-intensive asset. The rapid evolution of computing workloads, particularly the shift toward AI training and inference, has dramatically increased the power density of modern facilities. Just five years ago, typical rack densities ranged from 5 to 8 kilowatts; today, many new facilities are being designed to support between 15 and 50 kilowatts per rack, fundamentally altering both infrastructure requirements and site selection criteria.

This increase in density translates directly into higher overall power demand, with even midsized facilities requiring several megawatts of capacity and hyperscale developments demanding as much as 100 megawatts or more.

As a result, access to reliable, scalable electrical infrastructure has become a critical factor in determining project feasibility. In many traditional data center hubs, power availability is no longer keeping pace with demand.

This dynamic is forcing developers to expand beyond established markets such as Northern Virginia and into "frontier markets," including West Texas, Tennessee, Wisconsin and Ohio, locations where grid capacity is more readily available. In Texas alone, more than 6.5 gigawatts of data center capacity is currently under construction, underscoring both the scale of demand and the geographic shift underway.

Yet access to power is not simply a matter of proximity to the grid. Developers must also account for reliability, redundancy and long-term scalability. Data centers are facilities in which even brief outages can result in significant financial consequences.

"To be in data center construction in many cases means you are in power generation construction — the data centers of 2026 and beyond are going to be two construction projects in one: power generation and data halls," says Ted Way, Area Executive Vice President, Gallagher Construction Services.

Data centers are designed with multiple layers of power continuity, including uninterruptible power supply (UPS) systems to manage short-term disruptions and on-site backup generation (most commonly diesel generators) to ensure continued operation during extended outages. Increasingly, some operators are also exploring on-site or dedicated power-generation solutions to mitigate grid constraints.

Water

Parallel to the challenge of power availability is the equally critical issue of cooling. The immense heat generated by densely packed servers must be continuously managed to maintain performance and prevent equipment failure.

Historically, air-based cooling systems have been the standard approach, supported by large-scale HVAC infrastructure. However, as rack densities increase and thermal loads intensify, liquid cooling technologies — many of which rely on water or specialized fluids — are gaining traction due to their efficiency in high-density environments. This shift has elevated water from a secondary consideration to a central factor in site selection and design.

Large-scale data centers, particularly those utilizing evaporative cooling systems, can consume millions of liters of water annually. While these systems can offer significant energy efficiency benefits compared to air-only cooling, they also introduce new challenges related to water sourcing, sustainability and community impact. In water-constrained regions, such demand can place additional strain on already limited resources, creating potential conflicts with residential, agricultural and industrial users.

As a result, water stewardship has become a vital component of data center development. Developers are placing greater emphasis on strategies such as the use of recycled or non-potable water, closed-loop cooling systems and site selection in water-abundant regions.

Transparency around water usage has also grown in importance, as regulatory scrutiny and stakeholder expectations continue to evolve. The environmental implications of drawing from municipal supplies, groundwater aquifers or surface water sources must be carefully evaluated, as each carries distinct ecological and operational risks.

Expert Guidance Pays Off at Every Step

It's therefore not surprising that the remote locations in which data centers must be built present their share of challenges, both for logistical reasons and potential exposure to natural catastrophes.

"The sites that work best for data centers tend to be very challenging from a geographic risk standpoint," says Way. "There are multiple factors that must be taken into account."

The potential exposure to wildfire, earthquake, flood, severe convective wind, named wind and storm surge must be determined, he says, when sites are being considered. Once those risks are ascertained, Gallagher's detailed catastrophe modeling report details the probable maximum loss from those perils. Recommendations can be made for site alterations to mitigate potentially expensive losses.

Way recalls one client who previously had not yet brought Gallagher's team into the site selection process and soon learned expensive lessons in securing windstorm coverage while construction was underway. Now, they leverage the guidance of Gallagher's Construction team from the start of every project.

Since 2023, Ted Way and Gallagher Construction Services Area Executive Vice President Nils Sorenson have together insured 36 US-based projects representing $21 billion in contracted volume.

"There's no one-size-fits-all solution for any construction project, particularly with data centers," Way adds. "It's about having a process in place and relationships in the market, so that when we ask for the proper amount of capacity, the markets listen. Developers move very quickly, and we move quickly with them."

Once the site's location is locked in, construction often begins within three to four weeks, at which point the exposures for contractors are brought sharply into focus.

SPEED, SCALE AND PRECISION

How Data Centers Are Built

If power and water determine where data centers can be built, the construction process itself defines how quickly and successfully those facilities can be brought online.

For contractors, data center construction is about executing highly coordinated, industrialized delivery at scale. The combination of compressed timelines, complex engineering systems and substantial performance requirements makes these projects some of the most demanding undertakings in modern construction.

At a structural level, data centers are designed for durability, scalability and load-bearing performance. Most facilities are built using reinforced concrete, with steel serving as the structural framework to support and shape the overall build.

Foundations are typically poured in place, while walls and floors are often constructed using prefabricated concrete panels, some spanning more than 20 meters in length. Floor systems are heavily reinforced, frequently utilizing T-shaped designs similar to steel girders to support the immense weight of equipment and infrastructure. In hyperscale projects, a single facility can incorporate hundreds of these panels.

Increasingly, developers are adopting a "powered shell" approach to accelerate time to market. Rather than delivering fully turnkey facilities, contractors may construct a completed exterior structure equipped with core power and connectivity infrastructure, while leaving the interior spaces unfinished. This allows tenants to customize the interior buildout to their specific operational requirements, including server installations, cooling systems and specialized equipment.

While this approach shortens initial delivery timelines, it also introduces additional coordination complexity, as multiple contractors and stakeholders may be engaged simultaneously across different phases of the project.

Phases of Construction

Data center construction typically proceeds across three primary phases, each with its own technical challenges and risk considerations.

The **foundation phase** begins with site preparation, including clearing, grading and excavation. Given the scale of many data center campuses, this alone can represent a substantial undertaking. Contractors must install deep foundations, utility corridors and electrical grounding systems designed to protect sensitive equipment from power irregularities. Precision at this stage is critical, as errors in foundational work can lead to costly complications later in the build.

The **structural phase** involves the erection of the building shell (framework, walls, floors and roofing systems), creating the physical footprint of the facility. While this phase may resemble traditional commercial construction on the surface, it's distinguished by the need to accommodate highly specialized infrastructure, including large mechanical and electrical systems that must be integrated seamlessly into the building design.

The **interior fit-out phase** is where data center construction differs most significantly from other projects. This stage is both technically complex and schedule-critical, involving the installation of extensive electrical distribution systems, network cabling, cooling infrastructure, backup power systems and security controls. Cooling systems, in particular, play a central role in maintaining operational integrity, requiring precise installation and redundancy to ensure continuous performance.

The Pressure Mounts for Contractors

Complicating matters further, data centers are rarely delivered as single, discrete projects. Instead, they are often constructed in multiple phases, with overlapping tranches of development progressing concurrently.

Different sections of a facility may be at entirely different stages of completion at any given time, with some areas nearing operational readiness while others remain under active construction. This phased delivery model enables faster capacity deployment but introduces significant coordination challenges, particularly when multiple contractors are working in close proximity.

From a risk perspective, phased construction also creates unique exposure scenarios: it's not uncommon for portions of a data center to become operational while construction continues elsewhere on-site. In these cases, contractors may remain actively engaged on a project even as third-party operators begin using adjacent facilities, introducing potential third-party liability risks.

In a similar way, the interplay between construction completion timelines and operational readiness can create costly delays in startup and complicate the transition between construction and operational insurance programs.

Adding another layer of complexity is the growing reliance on modular and prefabricated delivery methods. Critical components such as electrical systems, cooling units and structural elements are often manufactured off-site and delivered for assembly, allowing for faster build times but requiring meticulous coordination across a distributed supply chain.

Contractors must manage multiple fabrication partners, track production schedules and align on-site installation with manufacturing progress off-site. In this model, schedule performance is driven as much by factory output as by on-site labor productivity.

This places increased pressure on early-stage decision-making. Long-lead equipment such as generators, transformers and switchgear can carry lead times of 12 to 18 months, meaning that missed procurement windows or manufacturing delays can have cascading impacts on project timelines. Successful delivery depends on disciplined planning, rigorous change management and real-time visibility into both cost and schedules across the entire project.

When delays occur in data center construction, they can cost the developer as much as $2 million per day in lost revenue. "That's something for contractors to pay particular attention to," says Brian Cooper, who notes that such setbacks need to be attached to the client's builder's risk coverage.

Surety Challenges

Securing surety bonds for data center projects can be challenging due to the size, complexity and risk profile of these builds. Many projects involve very large contract values, tight timelines and highly technical scopes, which can push contractors up against their bonding capacity limits. Even well-established contractors may need to carefully manage their backlog and financial strength to qualify for additional bonding.

Underwriters must consider the potential for cost overruns, delays and performance issues, especially given factors like specialized labor shortages, supply chain pressures and evolving technologies such as advanced cooling systems or power infrastructure. If a contractor lacks a strong track record with similar large-scale projects or if the contract terms are particularly demanding, the resulting bonds may contain stricter conditions or require additional collateral.

Exposures for Data Center Contractors

There are a variety of unique risks associated with data center construction. As the risk profile of these sites is continually evolving, contractors must ensure they are fully insured against these exposures. Customized insurance solutions, developed with a trusted advisor, are key to this endeavor.

1 Fire and Water Risks

The backbone exposure for data center contractors is impairing the project while it's being built. These facilities often involve high-value materials such as switchgear, generators and cooling systems, so any damage caused by fire or water can be catastrophic.

Inside data centers, an enormous amount of electrical equipment is packed into a confined space. For this reason, fire is a constant concern. Fires can be sparked by overheating equipment or electrical faults and high-capacity lithium-ion batteries used in UPS backup systems can overheat or even combust if they fail.

While fire suppression (either sprinkler or gas-based) systems are utilized, a serious fire can still destroy essential equipment. Additionally, electrical units can be damaged if those sprinkler systems malfunction.

As data centers utilize water-based cooling systems, such as cooling towers and chilled water loops, any water intrusions — for example, those caused by flooding or a roof leak — can damage servers.

"The need for cooling water in data centers is not always considered by the contractor and it presents a specific set of exposures," says Cooper. "Partnering with advisors who understand the characteristics of water use and the risks they present in these projects is paramount."

2 Builder's Risk Coverage Gaps

Contractors working on data centers need to be made aware of the exposures introduced by the subtleties in coverage around these types of projects.

Ambiguity Around Project Completion and Coverage Termination

One of the most significant exposures for contractors arises from uncertainty around when their builder's risk coverage ends. Policies typically terminate upon "completion" of the project, but that term is often subject to interpretation. Insurers may argue that a project is "substantially complete" earlier than contractors expect.

This issue often arises in data center construction, where projects are frequently delivered in phases, such as powered shells that become operational before full buildout. If a tenant occupies part of the facility while construction continues elsewhere, coverage for the entire project may be challenged or curtailed.

Contractors face the risk that a loss occurring after partial occupancy but before full completion could fall into a gray area, potentially leaving them without coverage unless policy language or endorsements clearly extend protection through phased completion.

Damage to Existing or Operational Structures

Data centers are often built in stages, which means contractors may be working next to areas that are already finished and in use. Standard builder's risk policies usually don't cover damage to these existing or operational parts of the facility if the damage is caused by ongoing construction.

This creates a critical exposure for contractors working on phased or expansion projects. For instance, construction work in a new data hall could inadvertently damage adjacent operational infrastructure such as live electrical systems or cooling equipment. Without appropriate endorsements or separate coverage, the contractor may be responsible for costly repairs to high-value assets.

Exclusion of Contractor Tools and Temporary Equipment

Many contractors assume that builder's risk insurance covers everything on the job site, but that is not the case. Typically, the policy covers the building and its permanent systems (such as electrical equipment, HVAC and structural components), but it doesn't cover the contractor's tools or temporary equipment.

In data center construction, this can represent a significant exposure for contractors. Specialized tools, temporary cooling systems and installation equipment can be expensive. If these items are damaged, stolen or destroyed, the contractor may bear the full cost unless separate equipment policies are in place.

3 Delays in Completion

Contractors face intense pressure to deliver data centers on tight timelines, making speed to market essential. Delays of any kind can be extremely costly to the owner/operator, who can pass those financial losses on to the contractor.

The construction of data centers is highly dependent on the timely delivery of materials and equipment and the construction sector is known for being one of the hardest hit industries when it comes to supply chain issues. Experts maintain that nine out of ten data center construction projects are delayed and the average overrun is 34%. These are wholly unacceptable margins when it comes to projects of this size and scope.

Whether due to geopolitical risks, rising material costs or trade disputes, disruption in supply chains can lead to project delays, higher costs and damage to the contractor's reputation.

Many components — such as semiconductors, switchgear and cooling units — have long lead times and limited suppliers. If a critical component becomes unavailable or is delayed, the contractor may face penalties or need to source alternatives at a premium. In some cases, redesign may be required, compounding costs and risks.

Materials and equipment (e.g., generators, cooling units and electrical gear) can also be damaged while in transit or awaiting installation. Their protection is critical, given the high-value components involved. For example, custom electrical gear shipped from overseas could be delayed, damaged en route or even stolen from a staging area.

Data center construction also requires highly specialized labor, particularly for installing electrical systems and cooling infrastructure. The pool of workers with this expertise is relatively limited and demand has surged alongside the rapid growth in data center development.

For contractors, this creates several challenges. Skilled tradespeople can be difficult to source and retain, which can increase both labor costs and the risk of project delays. At the same time, relying on less-experienced labor or stretching experienced crews too thin can increase the likelihood of installation errors, safety incidents and rework, particularly given the precision required in data center environments.

"Given the very short time frames in place for these projects, the demand for labor in these trades can be a challenge," says Cooper, who has seen cases in which one construction project draws talent from other sites in the area due to the need for specialized expertise.

4 Professional Liability Risks

Data center construction often involves design-build delivery, delegated design responsibilities and highly specialized systems integration, all of which can shift professional risk onto contractors.

Professional liability exposure, sometimes called "errors and omissions" risk, arises when a contractor's design, advice or technical decisions lead to a financial loss. While this has traditionally been associated with architects and engineers, it's increasingly relevant for contractors working on data center projects.

Design-Build and "Delegated Design" Exposures

Many data center projects are delivered on a design-build basis or include elements of "delegated design," in which contractors are responsible for designing specific components of the project. This might include electrical systems, cooling infrastructure or structural supports for server equipment.

When contractors take on these responsibilities, they are no longer just building to someone else's plans; they are making design decisions themselves. If those decisions turn out to be flawed, the contractor can be held responsible for the resulting costs.

Complexity of Mission-Critical Systems

Data centers are highly sensitive environments in which even the smallest design or coordination error can lead to outsized consequences. Electrical distribution, backup power, cooling and network infrastructure must all work together seamlessly.

Even something as simple as incorrect load calculations or poor integration between systems can lead to system failures or inefficiencies. In a data center, that can mean downtime, lost revenue for the owner and potential contractual penalties. Contractors involved in system design or coordination may be drawn into these claims, even if the issue stems from a seemingly minor oversight.

Performance Expectations and Uptime Guarantees

Data centers are often built with strict performance requirements, including uptime targets such as "five nines" availability (meaning that the facility is operating 99.999% of the time). While these guarantees are typically the responsibility of the owner or operator, contractors may still face exposure if their work contributes to a failure to meet those standards.

For instance, if a design or installation issue causes a failure in backup power or cooling systems, the contractor could be blamed for downtime even if the problem only occurs under certain conditions.

Coordination and Integration Risk

Data center construction involves multiple specialized trades (electrical, mechanical, IT infrastructure and others) all working in close coordination. Contractors are often responsible for making sure these different systems are properly integrated.

If there's a breakdown in coordination, such as mismatched specifications between electrical and cooling systems, it can lead to operational issues that are expensive to solve. These are not always "physical damage" claims. Instead, they may involve rework, system inefficiencies or failure to meet performance standards.

5 General Liability (Third-Party Injury or Property Damage) Risks

Commercial General Liability (CGL) insurance is designed to protect contractors from claims involving bodily injury, property damage and certain third-party losses arising out of their work. While these risks exist on any construction project, data center builds bring a set of exposures that can increase both the likelihood and the severity of claims.

Bodily Injury on a High-Intensity Job Site

Data center construction sites are often fast-paced and highly coordinated, with multiple trades working simultaneously in tight spaces. This increases the risk of accidents involving workers, subcontractors or even third-party visitors.

Injuries could result from electrical work, heavy equipment operation, elevated installations or confined working areas. While workers' compensation typically covers employee injuries, contractors can still face liability if a third party, such as a subcontractor's employee or site visitor, is injured and alleges unsafe conditions or negligence.

Damage to Third-Party Property

CGL policies also respond to claims for damage to property that doesn't belong to the contractor. In data center construction, this exposure can be significant, especially when projects take place near existing infrastructure or in active facilities.

For example, construction activities could damage adjacent buildings, underground utilities or nearby equipment. In urban or campus-style data center environments, even a relatively small mistake like striking a utility line can have ripple effects, leading to costly repairs and potential claims from multiple parties.

Work in (and Around) Live Environments

Many data center projects involve expansions or upgrades to facilities that are already operational. This means contractors may be working near live electrical systems, active servers and critical cooling infrastructure.

If construction activities accidentally disrupt these systems, causing power outages, overheating or equipment shutdowns, the contractor could be held responsible. While some policies limit coverage for purely financial losses (like lost data or business interruption), there may still be covered property damage components, such as physical damage to equipment.

Products and Completed Operations Exposure

General liability doesn't just apply during construction. It also covers certain risks after the work is finished. This is known as "completed operations" coverage.

In the context of data centers, a defect in construction such as improperly installed electrical systems or faulty connections may not cause a problem immediately. However, if it later leads to a fire, system failure or other damage, the contractor could face a claim months or even years after the project is complete. Given the complexity and continuous operation of data centers, these delayed-loss scenarios are a meaningful exposure.

6 Equipment Breakdown

Data centers undergo rigorous testing before going live, including load testing generators and cooling systems. If a generator fails catastrophically during testing due to improper installation, it could cause both physical damage and project delays. These systems are expensive and highly specialized, amplifying the financial impact.

7 Subcontractor Default/Performance Risk

Data center construction relies heavily on specialized mechanical, electrical and IT infrastructure subcontractors. The scale of individual mechanical and electrical packages can reach as much as of $500 million for a single campus.

If a key subcontractor goes bankrupt mid-project or fails to perform, the general contractor may need to step in, hire replacements at a higher cost and absorb delays. This can lead to broader financial and contractual issues with the project's owner.
As a result, prequalification standards and risk mitigation strategies are extremely critical.

8 Natural Catastrophe Risks

Contractors are put at particular risk by natural catastrophes because they're exposed in the middle of the build, when the project is at its most fragile and least protected.

Unlike a completed data center, which is engineered for resilience, a job site is a moving target: Structures are incomplete, systems aren't fully commissioned and protective features like flood barriers or permanent roofing may not yet be in place. That means a single severe weather event can undo months of progress, leaving the contractor responsible not just for rebuilding, but for managing the financial and contractual fallout that follows.

Wind events — including hurricanes, coastal storms or even severe thunderstorms — are among the most immediate threats. A partially enclosed structure can be highly susceptible to uplift and internal pressurization, especially if exterior walls or roofing systems haven't been fully installed. High winds can topple cranes, scatter unsecured materials or damage sensitive equipment staged on-site, such as generators or switchgear awaiting installation.

For contractors, this can result in costly repairs, extended project timelines and potential disputes over responsibility for damaged materials or improperly secured work.

Flooding introduces a different but equally disruptive set of challenges. Even in areas not traditionally considered high-risk, intense rainfall events can overwhelm temporary drainage systems and inundate the site. Water intrusion can damage electrical infrastructure, saturate building materials and compromise underground systems like conduit runs or foundations.

In seismically active regions, earthquakes present a more unpredictable but potentially catastrophic exposure. During construction, structural elements may not yet be fully tied together and seismic bracing for equipment and systems is often installed later in the build. Even a moderate seismic event can shift or weaken partially completed structures, forcing contractors to halt work, reassess structural integrity and in some cases rebuild affected sections.

Extreme temperatures and weather variability also play a quieter but meaningful role in contractor risk. Heat waves can warp materials, degrade temporary installations and increase the likelihood of worker fatigue-related incidents, slowing productivity. Conversely, cold snaps can freeze and rupture partially installed piping systems or make certain construction activities unsafe or impossible. These conditions can steadily erode schedules and budgets, particularly on fast-tracked data center builds in which timing is critical.

Natural catastrophes can also create impacts beyond the job site. A regional storm or wildfire can disrupt supply chains, delay the delivery of critical components or limit the availability of skilled labor. Even if the site is not directly impacted, contractors may still face significant delays and cost overruns, along with potential penalties tied to missed milestones.

In this way, catastrophe risk becomes not just a question of physical damage, but a broader operational and financial challenge that contractors must actively manage throughout the project's life cycle.

9 BESS-Related Risks

Battery Energy Storage Systems (BESS) are increasingly used in data centers to support backup power, load balancing and energy efficiency. While they offer clear operational benefits, they also introduce safety, technical and liability risks during construction and installation.

Fire and Thermal Runaway Risk

The most significant exposure associated with BESS is the risk of fire, particularly from "thermal runaway" events in lithium-ion batteries. This occurs when a battery cell overheats and triggers a chain reaction, potentially leading to fires that are difficult to control and extinguish.

For contractors, the risk is highest during installation, commissioning and testing. Improper handling, damage during transport or installation or errors in system setup can all increase the likelihood of a fire. Even a small incident can escalate quickly, leading to major property damage and potential third-party liability claims.

Fires involving battery systems behave differently from typical construction fires. They can reignite, produce toxic gases and require specialized suppression methods. If a fire occurs on-site, standard fire protection measures may not be sufficient. Contractors could face increased liability if it's determined that proper precautions — such as spacing, monitoring systems or coordination with local fire departments — weren't in place. This also raises the stakes for job site planning and safety protocols.

10 Environmental Liability

Construction activities can create pollution exposures, particularly with fuel storage, refrigerants and hazardous materials. A diesel spill from on-site generators could contaminate soil or groundwater, triggering cleanup costs and regulatory scrutiny. Similarly, improper handling of cooling chemicals could create environmental hazards.

Battery systems contain hazardous materials that can be released during a fire or failure event. This can include toxic gases, contaminated runoff from firefighting efforts or disposal issues for damaged battery units.

Standard general liability policies often contain limited coverage for pollution-related claims. Contractors could face cleanup costs, regulatory penalties or third-party claims if a BESS-related incident leads to environmental contamination.

11 Cyber Risk

Even during construction, data centers are increasingly "live" environments in which networked systems are being tested. A contractor's systems could be compromised during installation of network infrastructure, leading to unauthorized access or malware introduction. A breach in a data center's systems could lead to data theft or severe service disruptions.

Why Expertise Matters

Partnering with a broker possessing a proven track record of data center builds can provide invaluable specialist knowledge for data center contractors seeking to mitigate these various, potentially costly exposures.

"Our experience, the depth of our team and our relationships with the insurance and surety markets make us well positioned to respond so that when something does happen, we can assist in resolving it quickly and get the project back on schedule," says Cooper.

Consistency

Data center risks require a wide range of insurance coverage endorsements, and contractors must ensure that their contractual obligations are aligned with their insurance protections.

Through its end-to-end Data Center Solutions practice group, Gallagher supports clients through the full life cycle of data center development and operations, from site selection and construction to operational risk, power strategy and business interruption exposures. We help clients plan for supply chain disruptions for long-lead equipment, establish comprehensive safety protocols, ensure multiple power sources and address potential delays from permitting and compliance issues.

Risk management consultation at the earliest stage of each data center construction project empowers contractors to understand the multiple exposures they face and how responsibilities are allocated among the asset owner, contractors and subcontractors. Structuring bespoke insurance programs helps protect the asset's value and reduces the likelihood of uninsured or poorly understood losses arising from infrastructure failure and contractual performance obligations.

Sources section:

[1]Guckes, Michael. "February 2026 Data Center Report: After Record Growth, the Outlook for the Year Ahead," *Construct Connect,* 3 Feb. 2026

[2]Guckes, Michael. "March 2026 Data Center Report: Year Begins with Record Construction Starts," *Construct Connect,* 4 Mar. 2026.

[3]Sheets, Andrew. "Who Will Fund AI's $3 Trillion Ask?" *Morgan Stanley,* 25 Jul. 2025.