Find all our research in sigma explorer: http://sigma.swissre.com

Swiss Re Institute

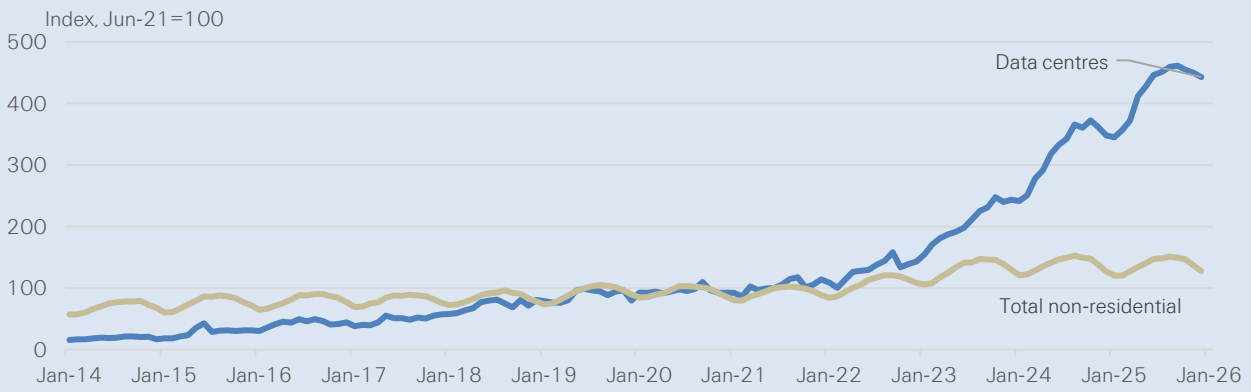
sigma insights March 2026

Insuring AI: data centre value accumulation risks

The data centres powering today's AI infrastructure are growing in scale and complexity, challenging the insurance industry's ability to provide the cover demanded by financing. Construction costs for a single location can reach USD 20bn and increase further once technology is installed. This accumulation of value heightens the impact of physical risks, including natural catastrophes. Our modelling finds that more than a quarter of the US data centre capacity may be in locations experiencing ≥3 large-hail days per year. Over 40% of capacity could also sit in significant-to-very-high tornado-day zones. Water damage from cooling failures, power continuity vulnerabilities, and new fire ignition sources are additional emerging contributors to data centre risk.

Data centres are critical AI infrastructure, housing the physical technology behind the sector's rapid growth. Capital spending for the "big five" cloud service providers, also known as hyperscalers,[1] is now widely forecast to exceed USD 600 billion in 2026, a 36% annual increase. Roughly 75%, or USD 450 billion, of that spend is directly tied to physical AI infrastructure housed in large data centres, such as servers or graphics processing units (GPUs).[2] The data centre sector worldwide is forecast to expand at a 14% CAGR through 2030, with the US growing the fastest, according to JLL.[3] US construction spending on data centres has far outpaced growth in total non-residential construction (see Figure 1).[4]

Figure 1: US construction spending, monthly, 2014-2025



Source: U.S. Census Bureau[5]

Data centre construction is creating growing insurance demand

Demand for data centre insurance has grown accordingly. Global insurance premiums tied to data centres are expected to rise to USD 24.2 billion by 2030, up from USD 10.6 billion.[6] Re/insuring data centres at this scale is complex, both during construction but especially during the operational phase, as we explore in this report. While construction risk is primarily about *creating* the asset (challenges include physical perils, subcontractor interdependencies, and delay), operational risk is about keeping a high-value, multi-tenant critical system *continuously available*. Once GPUs, tenants, and services are in place, both the value and operational complexity increase, making business interruption (BI), loss of rent, and service interruption critical. We also see emerging exposure drivers in rising insured value on catastrophe-exposed locations.

Data centre construction: USD 20 billion projects present scale and complexity challenges for re/insurers

The data centres being built to support AI workloads today are larger both in size and in engineering complexity than the smaller traditional constructions of the past. Those were familiar risks for insurers, whereas the new data centres are built as campuses with dense systems and tight operational interdependencies that compound risks in single sites. These capital-intensive projects require advanced cooling systems, high-voltage power and back-up infrastructure, sophisticated hardware and robust security software.[7] The full cost of construction can exceed USD 20 billion,[8] which can double after GPUs and other technology is installed.

The need for insurance cover for these large projects is driven by the multi-billion financing need. This creates demand for very high insured limits for a single data centre location. Financing institutions demand limits to cover the full cost of construction, even as maximum probable loss scenarios are much lower.[9] The re/insurance industry can only support a fraction of this limit at competitive rates for traditional construction risk policies.

Surety bonds on major builds,[10, 11] and subcontractor default insurance, are becoming increasingly important with this uptick in engineering complexity. Each site relies on numerous specialised subcontractors and defaults can cause delays and broader project disruptions.

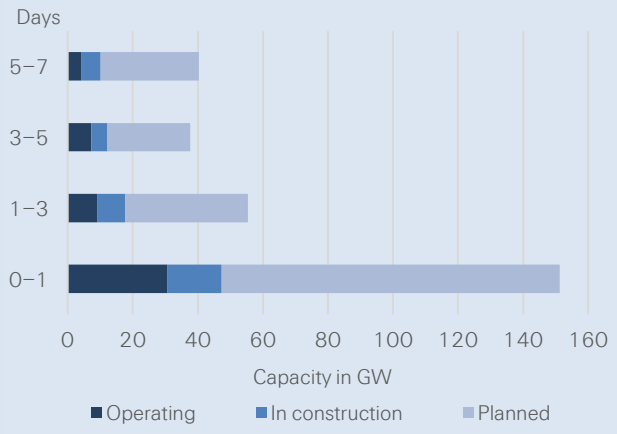
Building boom in high natural hazard locations

In the US, the extensive land and renewable energy requirements of new data centres are increasingly driving their development in more natural catastrophe-exposed locations. This is an increasing risk, given *sigma* data shows insured losses from natural catastrophes are rising by 5-7% annually on average in real terms over the long term.[12] These include areas at risk of severe convective storm (SCS),[13] which particularly impact the US and Europe and caused global losses of USD 51 billion in 2025.

The issue is compounded when developers build large clusters of data centres together, as is occurring in locations such as Abilene, Texas, and in Virginia. Placing multiple sites within a ~20-mile radius means a regional natural catastrophe event can affect a high density of insured value at once.

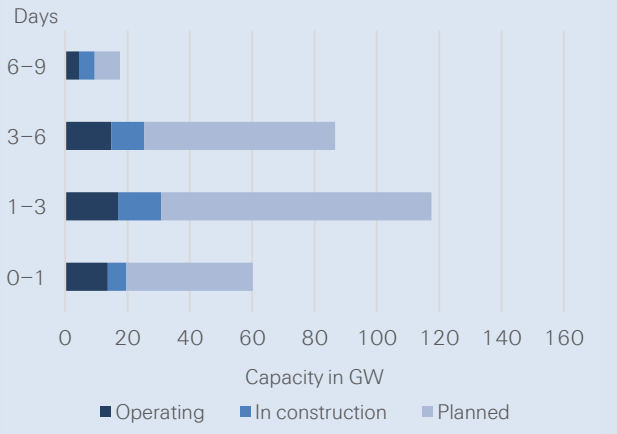
A substantial portion of US data centre capacity may also be located in places with elevated severe hail potential. Using Swiss Re's CatNet® tool for assessing catastrophic risks, we analysed data on planned and existing data centre capacity (available from the US Department of Energy, by county) to find that over a quarter of US data centre capacity could be in locations experiencing ≥3 large-hail days per year, averaged over a historical 64-year period.[14] The concentration is similar when modelled under current climatic conditions. This is particularly important, as data centre construction makes them susceptible to water damage. Key factors include large footprints, low-sloped roofs, numerous surface penetrations for building services infrastructure, and the high sensitivity of equipment to humidity. The campuses also include critical outdoor equipment, which can be directly exposed to hail and debris impacts.

Figure 2: US data centre capacity (GW) by large-hail days per year



Note: Historical 64-year (1959-2022) average large hail (diameter >2.5cm) days per year related to an area of 25km x 25km; a hail day has hail probability of ≥50%. The hazard footprint is extrapolated using county centroids, with GW aggregated to the county total, not mapped to individual data centre coordinates.
Source: *US Department of Energy, Swiss Re CatNet®,* Swiss Re Institute[15]

Figure 3: US data centre capacity (GW) by ≥EF1 tornado days per year



Note: 30 years (1994-2024) mean annual number of days with tornadoes ≥ (E)F1 (Enhanced Fujita scale), with wind speeds 86–110 mph (3-second gust), within a grid cell of 25km x 25km. The hazard footprint is extrapolated using county centroids, with GW aggregated to the county total, not mapped to individual data centre coordinates.
Source: *US Department of Energy, Swiss Re CatNet®,* Swiss Re Institute[16]

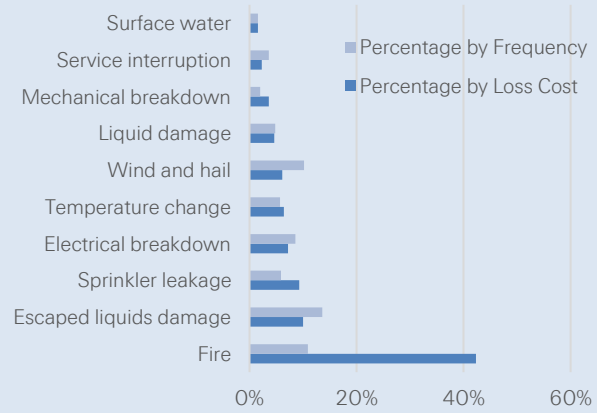
In the case of tornadoes, we estimate that ~40% of data centre capacity in the US could sit in significant-to-very-high tornado-day zones (≥ 3 days in a year with tornadoes ≥ (E)F1, or Enhanced Fujita 1), meaning the occurrence of an EF1+ is not improbable during a policy term.

A tornado's swath and debris field can readily traverse separated structures in the same campus, damaging multiple buildings simultaneously. A single event can lead to a loss higher than would be expected under a man-made single-location maximum probable loss assumption, where typically only one building or part of it is damaged. In a worst-case track scenario, a tropical cyclone passing through a dense market such as Texas could drive loss accumulation, with wind and flooding affecting many campuses and shared infrastructure at the same time.

Lithium batteries create new fire risks

Fire has been a primary driver of loss severity in traditional data centres. While it accounted for only 10.9% of loss events, it was responsible for 42.3% of loss costs, according to FM's 15-year study (see Figure 4). In new builds, we see a key operational change in the integration of lithium-ion battery backup units (BBUs) into server racks. These BBUs create an ignition source "that did not previously exist" within data processing equipment rooms, which can raise the intensity and frequency of fire losses.[17]

Figure 4: Data centre losses by engineering peril, last 15 years



Source: FM Global, DS 5-32 Data Sheet, January 2026[18]

This changing trend can be seen in FM's loss prevention evolving guidance, which now recommends increased fire and equipment protection for new data centres (see Table 1). The 2026 full revision increased the recommended fire-resistance rating for walls from one hour to two hours to limit conflagration, as well as introduced more stringent sprinkler expectations. Beyond downtime, uncontrolled thermal events risk employee safety and structural damage. Recent examples include a government-wide shutdown in Korea and a Singapore incident involving an explosion.[19]

Table 1: Evolution in features of data centres and accompanying safety requirements (selected)

Features of data centres	2018 full revision of guidance	2022 full revision of guidance	2026 full revision of guidance
Li-ion battery backup	No mention	Comprehensive (new)	Enhanced guidance
Liquid cooling	Brief mention	Brief mention	Comprehensive section
Compartmentation	1-hour walls	1-hour walls	2-hour walls (multiple rooms)
Sprinkler density	0.1 gpm /ft² over 1,500 ft²	0.1 gpm/ft² (no BBU); 0.2 gpm/ft² (BBU)	0.2 gpm/ft² over 2,500 ft² (all rooms)
Sprinkler temperature	165°F (74°C)	165°F (74°C)	135°F (55°C) wet; 165°F dry pipe

Note: gpm= gallons per minute, Source: *FM Global Property loss prevention data sheet 5-32: Data centers and related facilities*

Liquid cooling creates new "escaped liquids" exposure

The 2026 loss prevention guidance now also includes a comprehensive liquid-cooling section. Liquid-related losses represented nearly 24% of total data centre loss costs, according to a 15-year FM review[20]. Fire-related sprinkler leakage accounted for 9.3% of loss costs, while another 10% came from escaped liquid damage introduced by new cooling systems. Modern high-performance GPUs generate significantly more heat than traditional servers due to their high power consumption. As a response, more effective direct-to-chip liquid cooling replaced traditional air cooling.

The increased scale and complexity of cooling networks create risks of water damage from improper installation or maintenance, if contractors lack specialised data-centre experience with large-diameter pipes and networks.

Water stress and local water-related policy actions can also directly limit operations. If municipalities reduce water supply due to droughts or capacity issues, the site may have to shift cooling modes or temporarily shut down to prevent equipment damage.

Power sourcing as risk: on-site generation, battery storage and grid complexity

The largest driver of BI risk for data centres is power supply, accounting for 45% of outages, according to the Uptime Institute Global Data Center Survey.[21] Power-hungry GPUs and high-efficiency cooling significantly increase power requirements.

Traditional servers needed 5-15 kilowatts per rack, but AI servers can require more than 100 kilowatts per rack.[22] There are even discussions of restarting decommissioned conventional nuclear plants to meet data-centre power demand. [23, 24] Where grid connection cannot be secured fast enough, developers are now building power stations on site, which presents new hazards.[25] Reports suggest that roughly 30% of planned data centre capacity in the US could have power generation on-site.[26] Some hyperscalers now deploy dedicated behind-the-meter plants to avoid grid congestion. Battery energy storage systems (BESS) are also being integrated into data centres, but bring significant fire, explosion, and toxic gas hazards. Key considerations include the operation of on-site power generation and storage, and whether a credible third party is involved, given that power generation has not been a core activity for data centre developers.

Cyber risk: growing internet connectivity of operational technologies could increase vulnerability

Cyber risk in data centres varies by operating model. Facilities hosting customer information are attractive targets and can present high exposure to cyber-attacks. This was demonstrated by recent incidents that caused service disruption.[27] While hyperscalers are often perceived as lower risk due to their complete control over infrastructure, growing internet connectivity of operational technologies such as power, cooling, security, and monitoring systems is creating new cyber vulnerabilities across modern data centres.[28]

Concentration risk from correlated losses across multiple insureds and lines

Accumulation transparency is key, as insured portfolios can unintentionally build concentration. Large data centres are sometimes presented to risk carriers in separate insurance programs (eg, separately for building, equipment, power plants), making capacity accumulation difficult to track for insurers. This could allow a single loss event to impact several insurance programs. Large data centres also concentrate many tenants and insured interests within a single physical footprint, often behind common critical systems such as power, cooling and fire protection. This increases the likelihood of multiple concurrent claims arising from one occurrence.

Implications for underwriting and risk management

The data centre industry is evolving from a relatively low-hazard electronic equipment occupancy to complex, high-energy-density facilities requiring sophisticated, multi-layered protection strategies.[29] In some cases, new infrastructure is rolled out before researchers have had the chance to fully assess associated hazards, and before prescriptive regulations are available to mitigate them.[30]

Insurers have deep experience with traditional data centres, but only a few large, next-generation facilities are fully operational yet, making empirical loss experience limited. In this environment, underwriting success depends not only on capacity, but on specialised technical assessment and disciplined accumulation management.

Authors
Jonathan Anchen, Head Market Intelligence, Swiss Re Institute
James Finucane, P&C Research Lead, Swiss Re Institute

Editor
Barbara Zmuskova, Research Editor

Managing Editor
Dr Thomas Holzheu, Chief Economist Americas and Deputy Managing Editor, Swiss Re Institute

References

[1] Amazon Web Services, Microsoft Azure, Google Cloud Platform, Meta, and Apple.
[2] *Hyperscalers' Capex Above $600 Bn in 2026*, MUFG Americas, December 2025.
[3] *2026 Global Data Center Outlook*, JLL, 5 January 2026.
[4] *Value of Construction Put in Place at a Glance*, U.S. Census Bureau, accessed on 16 March 2026.
[5] Ibid.
[6] *Reinsurance Market Dynamics: January 2026 Renewal*, AON, 2026.
[7] *The role of surety in the development and operation of data centers*, Marsh, 11 May 2025
[8] *Data centers construction risk trends*, Allianz Commercial, November 2025.
[9] Ibid.
[10] N. Hemmer, G. Gionis, *Surety Bonds for Data Center Development*, WTW, 9 June 2025.
[11] *The role of surety in the development and operation of data centers*, Marsh, 11 May 2025.
[12] *sigma* 1/2026: Natural catastrophes in 2025: the persistent rise of wildfire and storm risk, Swiss Re, March 2026.
[13] Zurich's McBride and Penwright warn data center cat exposure rising as project scale accelerates | The Insurer Tv
[14] Ibid.
[15] *Speed to power data viewer*, National Laboratory of the Rockies, U.S. Department of Energy, accessed 12 March 2026. Data Center Demand Capacity (by county, operational, in construction, and planned)/ Developed by the National Laboratory of the Rockies (NLR) on behalf of the U.S. Department of Energy. The website noted a high degree of uncertainty in completion rate of planned projects.
[16] Ibid.
[17] *Data Centres and Related Facilities: FM Property Loss Prevention Data Sheets 5-32*, FM Global, January 2026.
[18] Ibid.
[19] South Korea (Sept 2025): A BBU failed during maintenance at the National Information Resources Service (NIRS) data centre, causing an explosion and fire that crippled 647 government services, including emergency responses and tax systems. Singapore (Sept 2024): A Li-ion battery thermal runaway at a Digital Realty facility burned for over 36 hours, heavily impacting Alibaba Cloud services. France (2021/2023): Multiple incidents, including the 2021 OVHcloud fire, highlighted the vulnerability of data centres to battery-initiated blazes.
[20] FM Global, Property loss prevention data sheet 5-32: January 2026.
[21] *Uptime Institute Global Data Center Survey 2025*, Uptime Institute, July 2025.
[22] *Copper in the Age of AI: Challenges of Electrification*, S&P Global Energy & Market Intelligence, January 2026.
[23] *Christopher M. Crane Clean Energy Center*, United States Nuclear Regulatory Commission, accessed 20 March 2026.
[24] *Duane Arnold Energy Center*, United States Nuclear Regulatory Commission, accessed 20 March 2026.
[25] *Bypassing the Grid: How Data Centers Are Building Their Own Power Plants*, Cleanview, 2026. A study by Cleanview found that data centres with a combined capacity of 56 GW have announced plans to build their own power generation.
[26] *Data Center Demand Capacity by County: 2025 June 16, Power demand*, NLR, US Department of Energy, accessed on 12 March 2026.
[27] For example, *Tietoevry: systematic restoration work continues after the ransomware attack – first customer systems back up and running*, Tietoevry Corporation, 25 January 2024.
[28] *Key Risks in Design, Development and Construction of Data Centers*, Aon, 9 May 2025.
[29] Swiss Re, Data Centers Factsheet, 2025.
[30] J. Roman, *A World of Demand*, NFPA, 12 November 2025.