12 October 2026

AI data centre risks investors should watch

Beyond power: AI and data centre sustainability

Sustainability
Global

- Several emerging sustainability risks for data centres deserve more attention: land, resources, and cybersecurity
- Community resistance to environmental, social, and cost-of-living impacts can materially affect business operations
- Regulatory framework for managing environmental and social effects lags sector growth, spurring approval moratoriums



Nneka Chike-Obi
Head of Sustainability Research
The Hongkong and Shanghai Banking Corporation Limited
nneka.chike-obi@hsbc.com.hk
+852 2284 1241

Yaryna Kobel
Corporate Governance Analyst
HSBC Bank plc
yaryna.kobel@hsbc.com
+44 20 3359 6152

Power demand is only part of the sustainability story for AI and data centres

The rapid expansion of AI is intensifying investor focus on data centres, most notably through rising electricity demand and implications for grid infrastructure. We think the data centre sustainability debate needs to go further. Beyond power consumption, the sector is beginning to face a broader set of environmental, social, and governance considerations that could become increasingly material over time, including stranded asset risk, land use intensity, community opposition, and the wider societal effects of large-scale AI infrastructure buildout.

Sustainability risk transmission may mirror resource and infrastructure sectors

We argue that the sector is starting to exhibit some of the same sustainability risk transmission channels seen in other infrastructure-heavy industries, where policy change, technology shifts, litigation, and social licence to operate can all affect valuations. As AI deployment accelerates, investors should pay closer attention to how data centres interact with communities, natural resources, and evolving governance expectations.

Cybersecurity gaps could disrupt physical infrastructure

Cybersecurity vulnerabilities in data centre management systems can now extend beyond data loss to disrupt power distribution, cooling, access controls and other critical operations. With 64% of organisations globally reporting that their cyber resilience meets only minimum standards, and nearly one in five data centre assets reportedly one step away from systems making outbound connections, investors should view cyber-physical resilience and recovery planning as increasingly material governance considerations.

This is our latest report on the Disruptive Technology theme. If you want to subscribe to any of our nine big themes, *click here*.

Disclosures & Disclaimer
This report must be read with the disclosures and the analyst certifications in the Disclosure appendix, and with the Disclaimer, which forms part of it.

Issuer of report: The Hongkong and Shanghai Banking Corporation Limited

View HSBC Global Investment Research at:
https://www.research.hsbc.com

Digging deeper on data centres and sustainability

- Much has been said about the impact of AI and data centre power demand on grid infrastructure and energy costs
- Beyond power, we see some emerging environmental, social, and governance issues that could become material to the sector
- Risks to the social acceptance of AI expansion include land use management, cost of living effects, and privacy rights

Materiality matters for AI and data centres

Everyone is talking about the relationship between data centre growth, driven lately by the AI boom, and energy consumption. As sustainability analysts, we are particularly interested in understanding how the growth of the data centre sector, including but not limited to its growing power demand, could have broader economic and societal effects; and if these could become material risk factors with subsequent valuation impacts down the line.

In our previous note (*AI Regulations*, 4 Aug 2026), we answered seven questions on the AI regulatory environment including licensing, legislation, and consumer protection. Here, we present some emerging environmental, social, and governance topics that we think are worth paying attention to, and our case for why investors should take a second look at them when evaluating the sustainability performance of companies in this sector.

1. Land and resources: what's a stranded data centre?

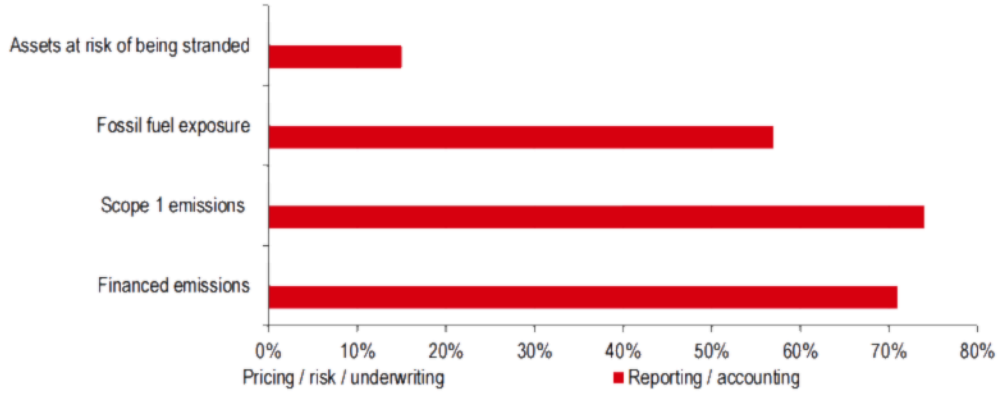
Stranded assets are units of physical infrastructure whose primary use is no longer needed, often before the end of the expected economic life, and are not able to be readily converted into alternative uses. For the fossil fuel industry, asset stranding is considered a material transition risk due to reduced demand ahead of an asset's planned closure date.

Assuming the transition trend continues, companies operating fossil fuel-related facilities could end up holding a fleet of obsolete assets, due to a combination of regulation and a continued trend towards low-carbon and renewable energy. Some academic research estimates that more than USD 1 trillion of energy assets globally are at risk of stranding.[1]

[1] "Stranded fossil-fuel assets translate to major losses for investors in advanced economies," Semieniuk, G., Holden, P.B., Mercure, JF. et al., *Nature Climate Change* 12, 532-538 (2002)

In a 2025 survey of global banks conducted by the UN Environment Programme Finance Initiative (UNEP FI), stranded asset risk ranked ninth among transition-related credit risks considered by large banks[2]. Broken down by how the banks use these criteria, we can see that stranded asset risk plays a much larger role in their overall risk appetite and underwriting criteria for companies in the sectors most exposed to stranding risk, such as natural resources.

Transition risk metrics used by banks by use case (% of survey respondents)



Source: UNEP FI, HSBC

When compared to factors like emissions and fossil fuel exposure, stranded asset risk seems to be equally material regarding lending decisions, but less important for regulatory or compliance-related climate risk reporting.

Producing power instead of plugging in: behind-the-meter data centres

Looking at the rapid growth of data centres, the question arises of whether the sector could face its own version of stranding risk. The specific driver here is not a data centre's power needs per se, but rather how it is meeting that need in the context of the wider power and commercial real estate market.

Average US interconnection queue is >5 years

In the US, grid connectivity for planned data centre projects is a significant bottleneck. Analysis by the Lawrence Berkeley National Laboratory indicates that the queue of grid interconnection requests in 2025 was about 50% higher than the country's total installed power capacity, and the time from request to completion is growing – from 36 months in 2015 to 61 months in 2025.[3]

The bottleneck in on-grid, or front-of-the-meter (FTM), power capacity is driving data centre projects to pursue behind-the-meter (BTM) power solutions – electricity generated on site that is not connected to the grid. Forecast US data centre power demand is expected to exceed on-grid, or front-of-the-meter (FTM), supply by more than 2:1 by 2030[4].

The RAND Corporation estimates that 60% of US-wide power sector capacity additions by 2030 will be behind-the-meter, driven by a combination of planned retirements of older facilities, energy and load availability, and historical project completion rates[5]. This aligns with the views

---

[2] "Bridging Climate and Credit Risk: Current Approaches and Emerging Trends for Climate-Related Credit Risk Assessment Methodologies—insights from a global survey," United Nations Environment Programme Finance Initiative, July 2025

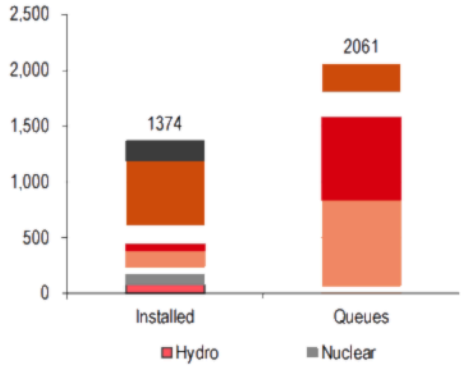
[3] "Queued Up: 2026 Edition – Characteristics of Power Plants Seeking Transmission Interconnection As of the End of 2025," J. Rand, A. Cheyette, et. al., Lawrence Berkeley National Laboratory and Interconnection.fyi, June 2026

[4] "How Much More Power Can the U.S. Grid Provide for AI? Projections and Policy Implications for 2030," A, Rueda, Ismael E., H. van Soest, H.M. Park, A. Smidt, D. Gill, R. Wang, K. Klima, and A, Najera, RAND Corporation, 2026

[5] "How Much More Power Can the U.S. Grid Provide for AI? Projections and Policy Implications for 2030," A, Rueda, Ismael E., H. van Soest, H.M. Park, A. Smidt, D. Gill, R. Wang, K. Klima, and A, Najera, RAND Corporation, 2026

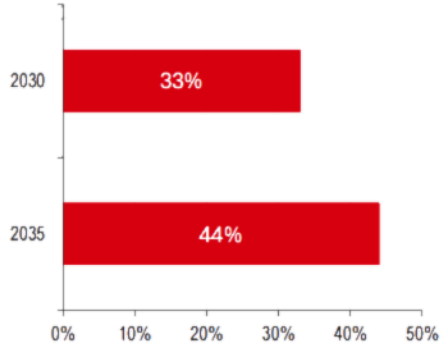
of the data centre industry itself; a November 2025 survey of data centre developers indicates that industry participants expect 33% of data centres to be operating with 100% on-site power generation by 2030, rising to 44% by 2035.[6]

Figure 1: US active interconnection requests compared to installed capacity, 2025 (GW)



Source: Lawrence Berkeley National Laboratory, HSBC

Figure 2: Developers' expectation of the share of data centres with 100% on-site power generation



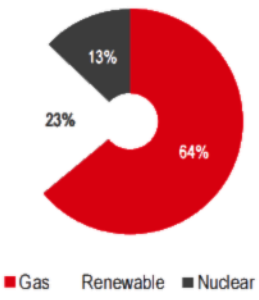
Source: Bloom Energy, HSBC

Producing power instead of plugging in – going behind-the-meter

The growing role of BTM energy to bypass the grid interconnection queue places means that the building's owner or operator is also in charge of generating its power. With nearly two-thirds of new data centre BTM capacity expected to come from natural gas (Figure 3), the responsibility extends to the sourcing and procuring fuel as well. This makes BTM data centres more like industrial facilities with captive fossil fuel power plants than traditional commercial real estate.

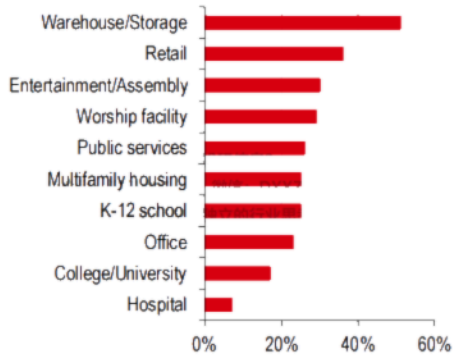
Other types of commercial buildings are increasingly adopting rooftop solar and battery energy storage systems for on-site power, which for many US building types can generate 25% or more of their total electricity needs (Figure 4). Why would a warehouse or retail facility operator take on the additional complexity of fuel management with a property running on BTM natural gas given the alternative - a combination of FTM electricity and on-site renewables?

Figure 3: Expectations of US on-site data centre generation by fuel type, 2030



Source: US Energy Information Administration, McKinsey, HSBC

Figure 4: Average % of US commercial electricity needs met with on-site renewable generation, 2019



Source: US Environmental Protection Agency, HSBC

[6] "2026 Data Center Power Report," Bloom Energy, January 2026

No man's land? Data centre footprints are large and getting larger

At the same time, data centre technology is quickly evolving, meaning that ongoing investment, renovation, and refurbishments will be needed to avoid obsolescence. When considering the lifespan of a data centre, Oracle estimates 10 years or more for buildings, HVAC, power, and physical security assets but just 3-5 years for computation equipment.[7]

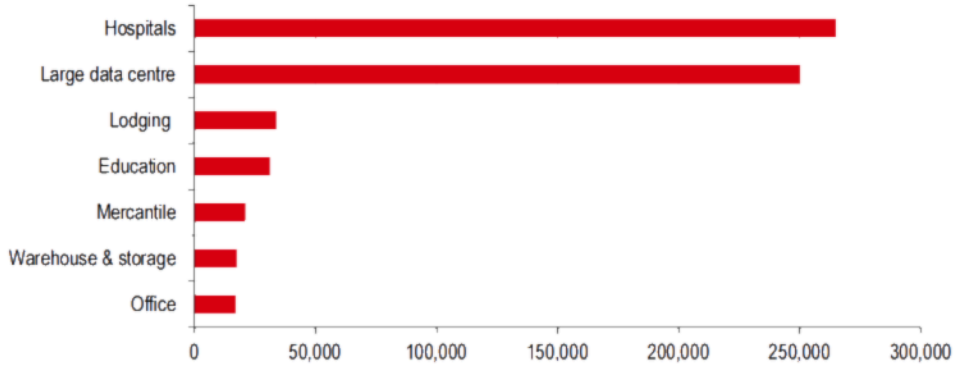
The average size of a large data centre in the US is 250,000 square feet (23,225 square metres), which far exceeds the average size of most other types of commercial buildings in the US, other than hospitals. Data centres also tend to be single-storey because of equipment weight and heat management, making their land use much larger than similar commercial buildings with the same floor area that occupy multiple storeys.

As a point of comparison, the largest hospital in the US based on number of patient beds, AdventHealth Orlando, has a 172-acre campus. Real estate broker Cushman & Wakefield estimates the size of the average US data centre land transaction in 2024 to be 224 acres – 30% larger than one of the largest medical facilities in the country.[8]

Current data centres may have limited alternative uses

These factors seem to limit the potential for turning end-of-life or prematurely retired data centres into alternative facilities like schools, health clinics, or warehouses, and therefore raise the risk of stranded data centre assets in the case of market changes or technological advancements that reduce demand for older facilities. The concept of adaptive reuse – converting a building for a different purpose than it was originally designed for – in this sector currently focuses on how existing buildings can be converted into data centres, and not on what the potential future uses are of retired modern data centres.

Figure 5: Average size of US commercial buildings (square feet)



Source: US Energy Information Administration, McKinsey, HSBC

End-of-life data centre regulation has not caught up with industry growth

There is currently a gap in the legal framework at both local and state levels addressing data centre decommissioning and repurposing, compared to other sectors like power and oil and gas where regulations already exist, according to analysis from the Sabin Center for Climate Change Law.[9]

We expect to see investors increasingly applying a similar transition risk approach to data centres as they do to the fossil fuel sector. The modes of risk transmission overlap: a shifting policy and regulatory environment, technology and market changes, and, particularly in the US, litigation. Nineteen stranded asset-related cases have been filed in the US since 2020 against

[7] "Exiting the Data Center: Planning Your Exit," Oracle, 9 March 2023
[8] "Data Center Development Cost Guide 2025, Cushman & Wakefield
[9] "Decommissioning Data Centers: Avoiding Stranded Assets," A. Murthy, 6 August 2026

oil companies, power utilities and government agencies[10], on the basis of a failure to manage or disclose the impacts of transition risk on an entity's operations and investment plans.[11]

For data centres, claims could relate to the impact of land use changes on local communities, lack of transparency on how obsolescence risk could affect a particular project, or whether the potential environmental effects of unabated on-site fossil fuel generation were incorporated into the project approval process.

2. Community resistance: how much for a social licence to operate?

Social licence to operate under pressure in the US

According to real estate management firm JLL, "community acceptance has become the [data centre] industry's greatest challenge[12]." Community support is a critical element of a sector's social licence to operate – the continued approval or acceptance of local stakeholders that enables a business to function. The impacts of a loss of social licence to operate can range from low-level resistance (e.g. protests) to the withdrawal of regulatory or legal permissions.

Political resistance against data centres is growing in the US; New York and Texas have instituted state-wide moratoriums on new data centre developments, citing resource use (i.e. electricity, water), grid stability concerns, and community impacts like land use change, noise and light pollution, and air quality. There are many smaller-scale pauses and moratoriums at local levels across the country.

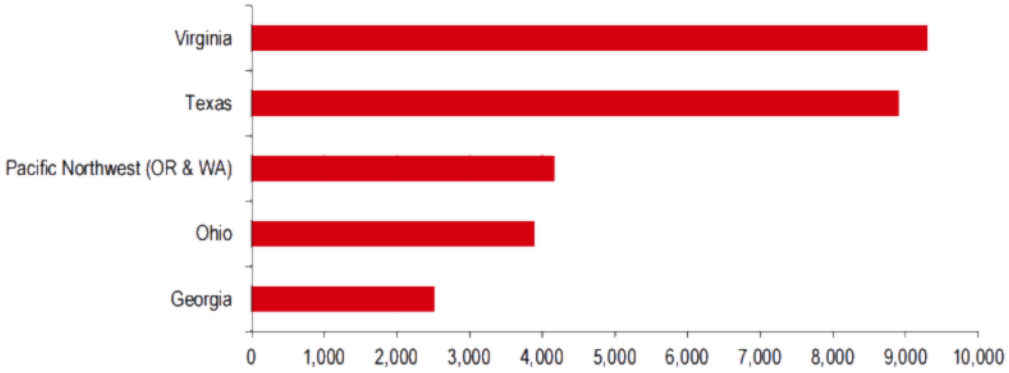
In a previous report (see *Global Commodities: 'Super-squeeze' continues*, 9 Sep 2026), we noted that the share of electricity being used by data centres in the US (6.5% in 2025) is much higher than in China (1.9%), Europe (2.6%), and the global average (2.4%), and that this may be a driver of community-related issues. We maintain that view – the resistance in the US seems not to be particularly ideological or populist. Instead, communities are blaming data centres for a combination of rising living costs and declining quality of life factors and increasingly taking a "not in my back yard" (NIMBY) approach with local elected officials.

We have taken a more granular look at the specific regions of the US with the most current and expected new data centre capacity, to see whether there is a relationship between energy prices and the community response. In terms of current data centre capacity, the top states/regions are Virginia, Texas, the Pacific Northwest (Oregon and Washington), Ohio, and Georgia, with a combined total of 28 GW, around 45% of the national total.

[10] Sabin Center for Climate Change Law. Platform operated by Climate Policy Radar
[11] "Stranded Assets, Climate Litigation, and the Role of U.S. Federal Agencies," K.A. *Public Policy Journal*, 2 March 2025
[12] "North America Data Center Report: Midyear 2026," Jones Lange Lasalle



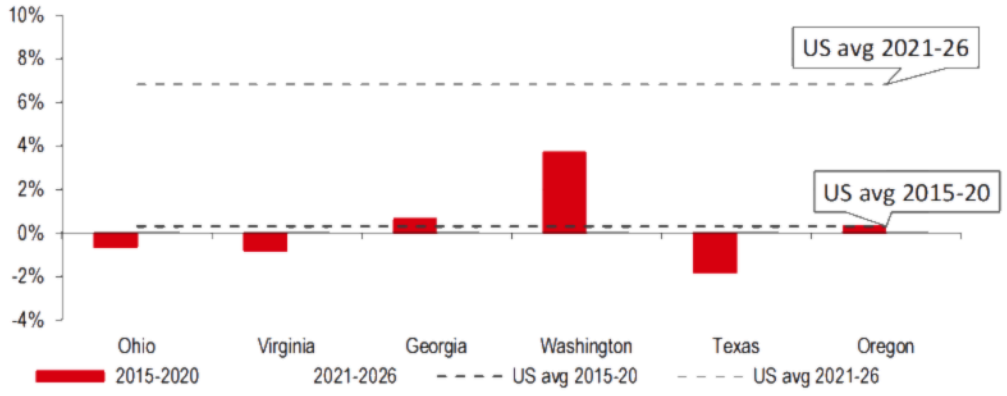
Figure 6: North America data centre capacity – top five states/regions as of mid-2026 (MW)



Source: JLL Research, HSBC

From 2015 to 2020, average US electricity prices rose about 0.3% per year. From 2021 to July 2026, the annual rate of growth jumped to 6.8%. In three of the six states with the most data centre capacity already installed, the annual increase in electricity prices between 2021 and 2026 exceeds the national average – Ohio (9.2%), Virginia (7.7%), and Georgia (6.9%). Although Texas has the lowest electricity prices of these states on an absolute basis (around USD 11.80/kWh), the change has been notable, moving from negative price growth prior to 2021 to more than 5% per annum since then.

Figure 6: Average electricity price CAGR in states with the most data centre capacity

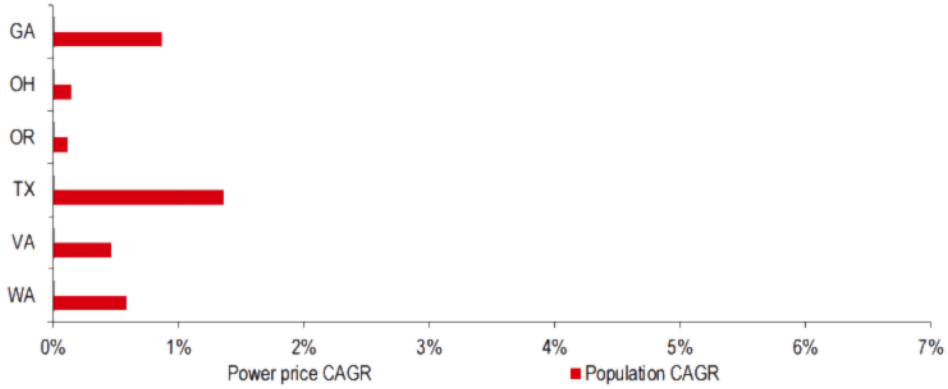


Source: US Energy Information Administration, Bloomberg, HSBC

Power to the people?
Population and energy mix

Are there other factors that could explain the rise in prices? Population growth does not seem to be a contributor. According to US Census data, both Ohio and Oregon experienced population growth of 0.9% from 2020-2025, yet Ohio's electricity prices grew at nearly twice the annual rate as Oregon's did. Texas's population rose 8.8%, and it still has both slower annual power price rises and a lower absolute average electricity price than Oregon.

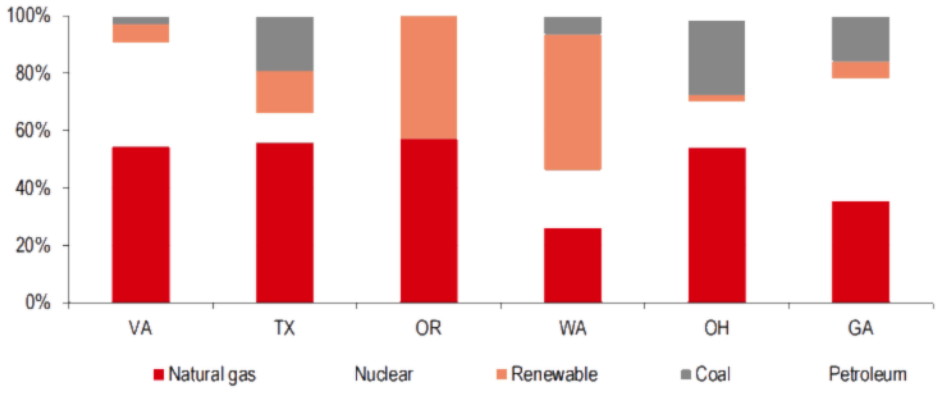
Figure 7: Population and electricity price CAGR in US states with the most data centre capacity, 2020-2025



Source: US Census Bureau, US EIA, Bloomberg, HSBC

On a CAGR basis, it doesn't seem to be related to the electricity fuel mix either. Ohio and Texas have similar shares of fossil fuel-generated power, but Ohio's electricity prices have risen nearly twice as much per annum as Texas's since 2020. There may be a slight benefit from fuel source diversity; the states with the largest price increases are more reliant on one fuel type, such as Ohio (natural gas) and Washington (hydropower). Georgia has the most diversified power mix of these states, split evenly between fossil fuel (52%) and low-carbon sources like renewables and nuclear (48%).

Figure 8: Electric power consumption by source, 2024



Source: US EIA, HSBC

So – can we say that data centre demand is the reason for rising prices in these states? With no clear signal in the data from population or fuel mix, we are willing to make an educated guess in this direction. Power prices are just one of the more measurable signals of the data centre industry's impact on communities. Lifestyle impacts like noise, light, and changes in natural capital are harder to quantify but can serve as additional anecdotal fuel for the general "vibe" that data centres are bad for local neighbourhoods beyond energy bills.

Are the kids alright?

One area that seems to be energising data centre opposition more recently is the impact on schools. The National Education Association, the US's largest labour union, amended its AI policy in July 2026 to address the impact of data centre construction on educator and student health, such as exposure to low-frequency noise. In the same month, the local government of

Palm Beach County, Florida, voted against a 600 MW AI data centre project that was within 1,200 feet (365 metres) of an elementary school[13].

Looking forward, policy responses to community opposition could be strongest in states where data centre capacity under construction exceeds existing inventory, and where the absolute rise in electricity prices from 2020-2025 was below 30%; policymakers are likely to face pressure to minimise further increases, given data showing more than 40%+ increases in states with large data centre industries like Ohio and Washington (Figure 9).

More broadly, similar dynamics are starting to emerge in other data centre hubs around the world. So far this year there have been local government proposals to allow communities to reject new projects in South Korea, a lawsuit against a proposed data centre project in Japan, and protests in Malaysia.[14]

Traditionally, community resistance has been identified as a material social sustainability factor for the natural resource industry, with cases around the world of local resistance to mines or extractive facilities causing project delays or suspensions[15]. Investors may need to consider the materiality of community resistance to data centres using a similar approach as they would for mining or energy projects.

Figure 9: US data centre capacity by state (states with the largest current or planned capacity)

Market	Under construction (GW)	Existing inventory (GW)	Total (GW)	Data centre policy	Population growth 2020-2025	Electricity price increase 2020-2025
Virginia	3.9	9.1	13	Statewide oversight law; local moratoriums incl. largest city (Virginia Beach)	2.9%	28%
Texas	17.2	8.8	26	Statewide moratorium	8.8%	24%
Pacific Northwest (OR & WA)	0.3	4.7	5			
Oregon				Statewide tax incentive pause; statewide moratorium proposed; local moratoriums	0.9%	26%
Washington				Local moratoriums incl. largest city (Seattle)	3.8%	40%
Ohio	3.2	3.8	7	Local moratoriums	0.9%	46%
Georgia	3.6	2.4	6	Local moratoriums	5.1%	28%
Louisiana	6.6	0	6.6	Local moratoriums	-0.9%	37%
Carolinas (NC & SC)	3.6	1.4	5			
North Carolina				Local moratoriums incl. largest city (Charlotte)	7.2%	25%
South Carolina				Local moratoriums	8.8%	35%
Arizona	1.9	2.1	4	Statewide pause on tax breaks; local moratoriums	6.5%	27%
Indiana	2.9	1.1	4	Local moratoriums	2.8%	38%
Wyoming	4	0	4	Statewide oversight law; local moratoriums	2.1%	22%

Source: Bloomberg, JLL, US Census Bureau, US EIA, HSBC

[13] "Why Are Data Centers Being Built So Close to Public Schools?" *NEA Today*, 14 Sep 2026, National Education Association

[14] "Data center boom fuels calls for tighter regulation in Korea," *The Korea Herald*, 13 Aug 2026; "Opposition to data centres grows in cramped urban Japan," *AFP*, 17 Jul 2026; "Malaysia draws first data centre protest over pollution and water," *The Straits Times*, 9 Feb 2026

[15] "Community matters: Mining, local engagement and the race for critical energy transition materials," S&P Global, 15 Sep 2024

3. Governance: cyber risk is becoming physical

Most companies only meet minimum cybersecurity standards

Cyber risks are a significant global concern. The WEF Global Risks Report 2026, based on responses from academia, business and government, identifies **cyber insecurity** as the sixth most severe short-term risk over the next two years. Meanwhile, the WEF Global Cybersecurity Outlook 2026 reports that 17% of organisations consider their cyber resilience unsustainable, while 64% believe it meets only minimum standards.

Ransomware is one of the key growing cyber threats facing companies; ransomware is now involved in 44% of all breaches, a sharp increase from the previous figure of 32%.[16] A recent survey suggests that 49% of companies that had their data encrypted in a ransomware attack paid a ransom to recover it. For organisations with more than 3,000 employees, the average cost of recovering from a ransomware attack - including downtime, staff time, device and network costs, and lost opportunities, but excluding ransom payments - reached USD 1.5 million in 2025.[17]

Data centre operations are subject to cyber risk

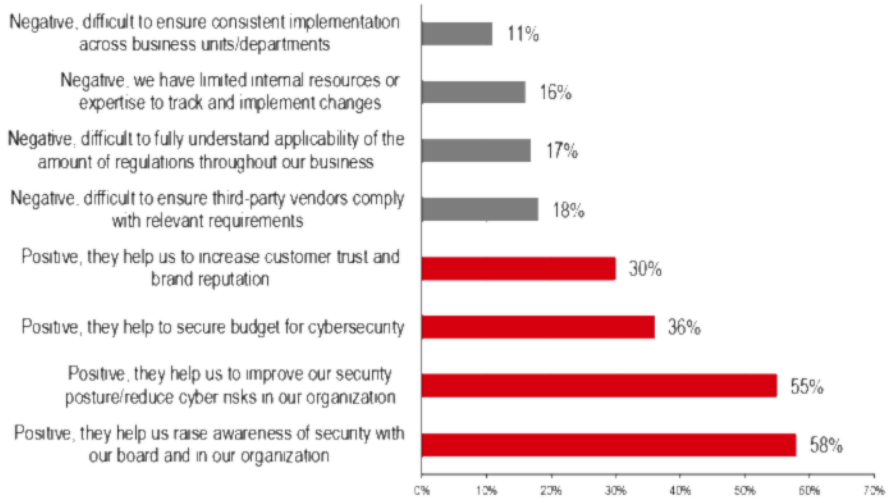
The risks extend beyond data loss. **Cyber-physical failures** are becoming more likely[18] as attackers exploit weaknesses in data centre management systems. Indeed, modern facilities depend on integrated information technology and operational technology systems - including energy management, building management and industrial control systems - to regulate power distribution, temperature and physical access. These systems support operational efficiency and physical safety, but they also create additional attack surfaces.

Recent research has identified widespread security gaps in data centre cyber-physical systems, with power distribution units and building management systems being the most exposed through insecure legacy protocols, outdated firmware, and internet-facing connections. Nearly one in five assets is one step away from systems making outbound connections that could provide attackers with a pathway to exposed data centre assets.[19]

In our view, advanced, **data centre-specific regulatory frameworks** and greater alignment across markets could help strengthen the cybersecurity ecosystem. Indeed, a recent survey found that 74% of respondents hold a positive view of the effectiveness of cyber-related regulations (figure 10); however, the fragmentation and variation in these approaches have added a new layer of complexity to the organisations trying to navigate a patchwork of regulations.[20]

16 Verizon, Data Breach Investigations Report2025
17 Sophos, The State Of Ransomware, 2025
18 WEF, Global Risks Report, 2026
19 K Hill, Claroty finds 1 in 5 data centre assets one hop from risky internet exposure, Datacentre Solutions, 28 July 2026
20 WEF, Global Cybersecurity Outlook 2026

Figure 10: Sentiment towards cybersecurity regulations



Source: WEF 2026

Regulation is starting to emerge

Some markets are now moving towards **greater regulatory clarity and oversight**. For example, in the *UK*, under the *Cyber Security and Resilience (Network and Information Systems) Bill*, data centres with a rated IT load of ≥1 megawatt operated by or for the Crown, are considered essential services and required to have appropriate and proportionate measures in place to prevent and minimise the impact of incidents. This includes notifying the regulator and customers about any incident that has a significant impact on the continuity of the service provided by data centres.[21]

In the *US*, in April 2026, experts at a hearing of the *House Homeland Security Committee's Subcommittee on Cybersecurity* called for a dedicated coordinating structure and clearer federal oversight of data centre protection.[22] We think clear regulatory oversight and support will help promote robust defences and recovery plans, ensuring resilience, transparency, and accountability across the sector.

More from Global Investment Research

Data Centres: Comparing mainland China, Hong Kong and SEA, 11 September 2026

ASEAN Perspectives: The data centre race, 31 August 2026

India Data Centres: A tussle between supply and demand, 20 July 2026

21 UK Government, Data centres: Policy paper, 30 June 2026
22 The U.S. House Committee on Homeland Security, Media Advisory: Subcommittee Chairman Ogles Announces Hearing on Combating Cyber Threats to Telecom Networks, Data Centers, Satellites, 23 April 2026