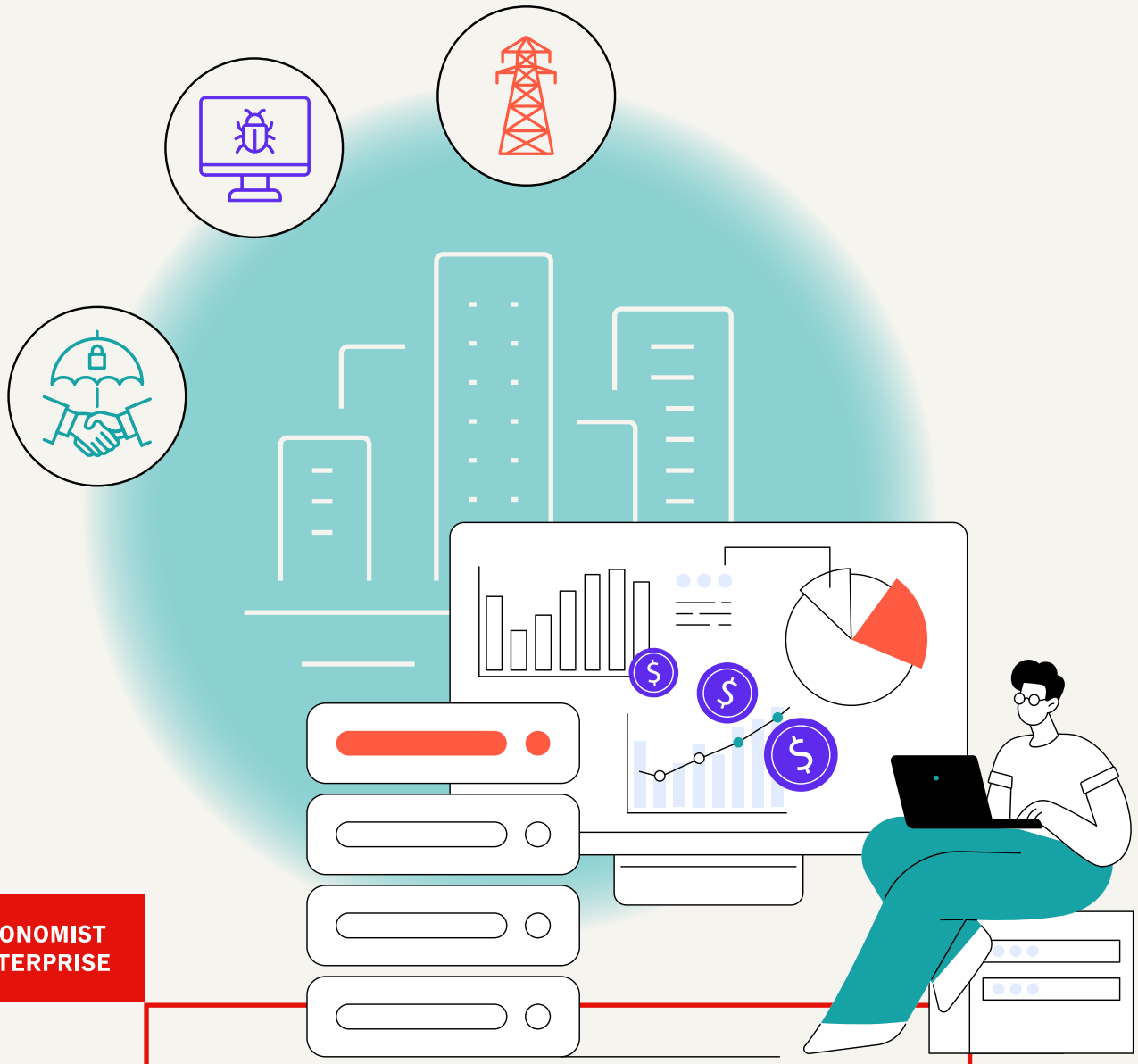


ECONOMIST ENTERPRISE

Built for what's next: evaluating digital infrastructure resilience

The investor guide

Sponsored by

Sponsor foreword

Digital infrastructure is becoming as fundamental to economic growth as transportation, energy and communications networks. As AI adoption accelerates and investment in digital infrastructure continues to expand, resilience is becoming an increasingly important determinant of long-term asset performance and value.

The Economist Enterprise research presented in this guide suggests that investors increasingly recognise resilience as a strategic investment consideration. Yet the findings also point to a broader resilience gap. While resilience is receiving greater attention, the interconnected risks shaping the future of digital infrastructure are often more complex than traditional evaluation frameworks were designed to assess.

Climate, energy, cyber, supply chain and technology risks do not operate independently. The most significant disruptions frequently emerge when vulnerabilities across multiple systems interact and compound one another. Understanding those interdependencies is becoming increasingly important for investors seeking to protect portfolio performance and long-term value.

FM's engineering research and decades of loss prevention experience indicate that severe failures often occur not because of a single event, but because interconnected systems are unable to adapt and recover when placed under stress. As digital infrastructure evolves, investors must evaluate not only current resilience, but also how assets may respond to emerging technologies, changing power requirements and future sources of disruption.

This requires a broader perspective on resilience. Alongside financial, operational and technical due diligence, investors increasingly need resilience intelligence that provides a clearer view of vulnerabilities, interdependencies and future risks across the digital infrastructure ecosystem.

This guide offers a practical framework to support better-informed investment decisions. The next phase of digital infrastructure growth will not be defined solely by the expansion of capacity. It will be defined by the ability of assets to perform reliably, adapt to change and retain value in an increasingly interconnected world.

About this research

Built for what's next is an Economist Enterprise research programme, sponsored by global commercial property insurer FM. It examines how risks across energy, people and technology often come together to disrupt digital infrastructure, and how organisations can best prepare to meet those shocks.

The research is based on:

- A global survey of 1,800 data centre stakeholders across the digital infrastructure value chain from 21 countries
- Interviews with global industry experts
- An expert panel discussion

Why the data centre boom is changing how investors assess risk, resilience and long-term value

Data centres used to be the dullest buildings an investor could own: windowless warehouses with credit-worthy tenants and a lease measured in decades. The AI boom has changed all that. Its gargantuan demand for compute is projected to lead to a near tripling of global data centre capacity by 2030, to around 220 GW, at a cost of some US$6.7trn, of which about US$5.2trn will be for AI workloads alone, according to consultancy McKinsey.[1] Four US technology giants plan around US$700bn of capital spending on AI infrastructure this year.[2] This is among the largest infrastructure booms in modern history. It is being built at a sprint.

The boom has also transformed who pays for it. A decade ago, listed real-estate trusts comfortably financed data centres drawing less than 100 MW. Today, the data centres where AI is born and lives are measured in gigawatts (each gigawatt of capacity costing up to US$50bn). This puts them far above the borrowing capacity of the data centre owners of the past. Their place has been taken by private-credit funds, sovereign-wealth funds, pension money and big banks. One peak was reached in October 2025, when Meta and funds managed by Blue Owl Capital closed a colossal US$27bn debt package—the largest private-credit and project-finance deal on record—for a single data centre campus in Louisiana.[3] As investors provide more of the capital behind the digital-infrastructure boom, the risk of the build-out has migrated from equity to debt.

One under-appreciated aspect of data centres as an investment asset is that they depend on things capital cannot conjure: land and permits to build, electricity to run, chips to fill, water to cool and, increasingly, the consent of neighbours. In the first quarter of 2026 alone, local opposition blocked or delayed at least 75 US projects, worth roughly US$130bn (as much as in the whole of 2025), according to advocacy group Data Center Watch.[4] A recent survey found that around seven in ten Americans would prefer not to live near a data centre.[5]

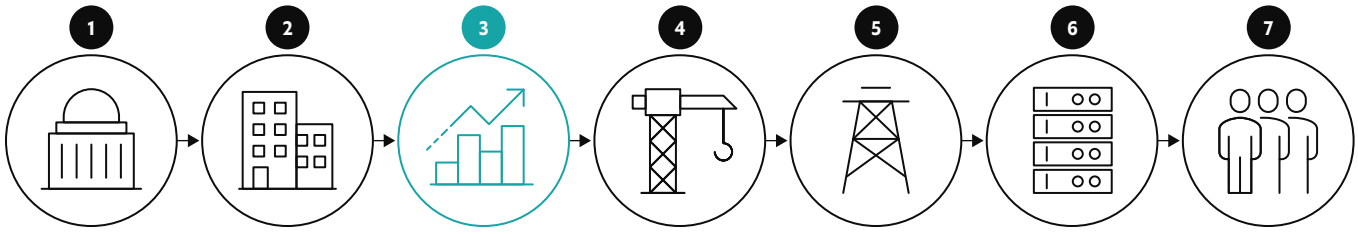
The demand for compute is projected to lead to a near tripling of global data centre capacity by 2030, to around 220 GW.

Scale compounds the problem. As projects grow to a gigawatt or more, each concentrates more value in a single point of failure, whether that is one grid connection, a single aquifer or dependence on chips of a generation that ages fast. Investment bank Morgan Stanley estimates that four big technology firms could record depreciation worth US$680bn over four years owing to tech that falls short of its intended purposes.[6]

How data centre risk arises, how it travels and who ends up carrying it is the subject of *Built for what's next*, an Economist Enterprise research programme, sponsored by FM. It draws on a survey of more than 1,800 senior leaders across the data centre value chain in 21 countries, including around 250 private-equity and institutional investors and representatives of more than 360 organisations that invest in or lend to digital-infrastructure assets.

One central lesson from our survey is that risk in digital infrastructure is largely generated at the level of the system, but it is most often priced at the level of the deal. Because investors hold the residual claim on other stakeholders—including the developer's siting, the utility's queue and the regulatory approval timelines—they are first to feel the effects. This guide sets out what investors worry about, how their strategies are changing and where practice still falls short of what resilient capital requires.

Figure 1: Investors' role in the digital infrastructure value chain

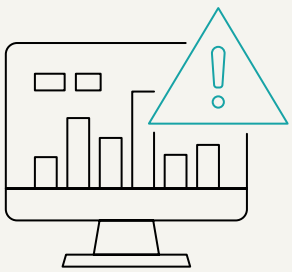


Source: Economist Enterprise

Key takeaway

Long-term climate exposure, technological obsolescence, asset concentration and compound shocks remain underweighted, based on our survey.

Investors should reflect these risks in financial models and stress test portfolios against compound shocks.



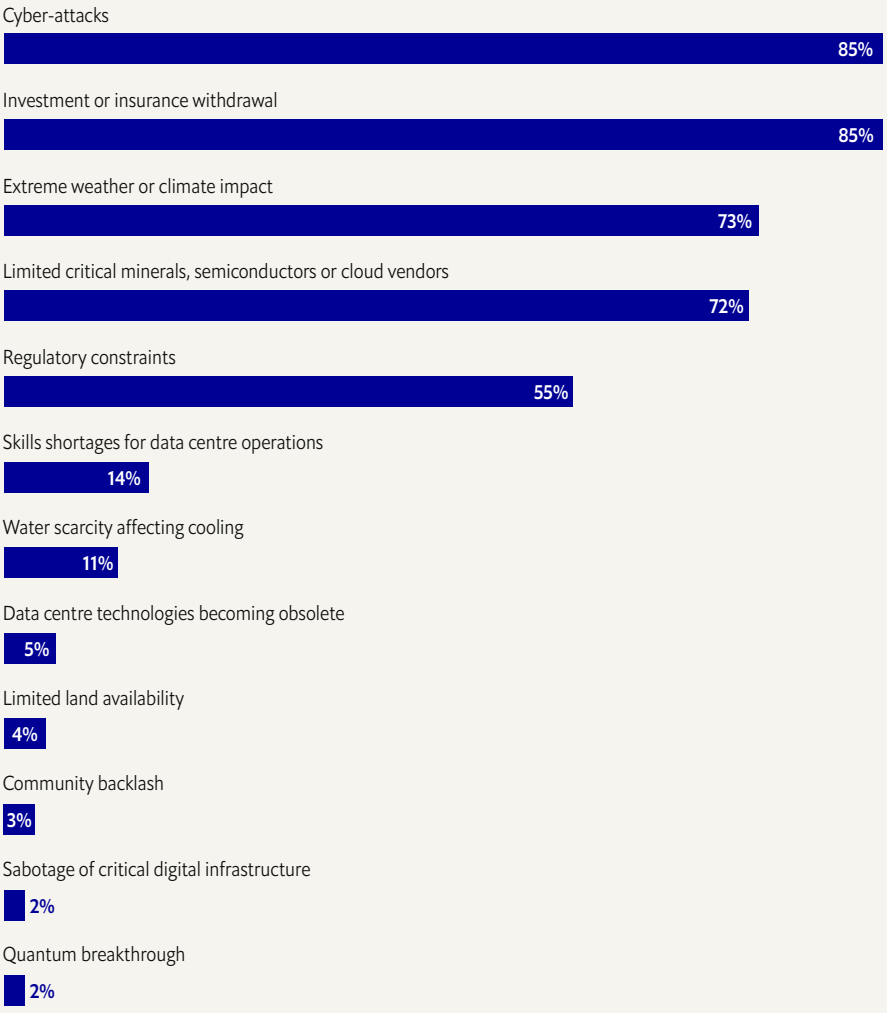
Where investors see risk—and where they do not

As AI capabilities surge, data centres are becoming undeniable engines of economic growth, attracting massive capital from investors eager to be part of the transformation AI will bring to economies worldwide. Yet behind that optimism lies a growing challenge. As these facilities scale to meet compute demand, they become far more complex and vulnerable to run. When operational reliability breaks down under grid strain, climate events or security threats, physical risk quickly turns into financial loss.

In our survey, we wanted to see which risks are on investors' radars, and whether they are tuned into the same threats as other players in the data centre value chain.

Figure 2: Risk exposure

Risks investors expect to have the greatest systemic impact on digital infrastructure over the next five years



Source: Economist Enterprise survey, February–April 2026

Cyber-risk is becoming a valuation risk

About nine in ten of the investors we surveyed identify cyber-risks as having the greatest systemic impact over the next five years. The threat of cyber-attacks extends beyond data breaches to encompass ransomware, distributed denial-of-service attacks, and malware targeting power and cooling control systems. Such attacks can spread across data centres, cloud platforms, energy systems and customer operations. A recent ransomware attack in Japan showed how quickly disruption can spread.

Attackers encrypted servers, disrupted customer orders and services, delayed financial reporting and contributed to a significant fall in the company's share price.[7] For investors, cyber incidents become a financial risk because they affect the drivers of value. Operational disruption can reduce revenues. Recovery and compliance increase costs. Reporting delays create uncertainty. Reputational damage may weaken future demand. As expectations about future cash flows deteriorate, valuations can come under pressure.

A risk of high concern specific to investors is the withdrawal of capital

The risk of cyber-attacks leads every stakeholder group's ranking, investors included. But the fear that most distinguishes investors from the rest of the value chain is the withdrawal of capital itself. Fully 85% of the private-equity and institutional investors we surveyed rank the withdrawal of investment or insurance among the risks most likely to materially disrupt digital infrastructure over the next five years, against 70% of respondents overall. The same share expects it to have systemic impact.

This fear makes sense because it is reflexive. In a boom financed increasingly by debt—including special-purpose vehicles, asset-backed securities and private credit—capital becomes the system's transmission mechanism. If lenders re-price, projects will stall, valuations fall and more lenders will follow suit.

For now, operational disruptions have not translated into widespread financial losses. Nearly three-quarters of surveyed investors report routine disruptions with little financial impact, while only 11% report severe losses. But this may reflect temporary financial insulation rather than resilience. Nearly seven in ten investors say short-term financial and growth targets are the biggest barrier to building resilience.

That insulation is beginning to fade. Until recently, strong demand helped absorb the cost of minor operational delays and power outages. Our survey suggests that is changing. More than half of institutional investors are applying higher risk premiums and discount rates, while two in five are repricing assets to reflect concentration risk. As these operational constraints intensify, investors are demanding higher returns to compensate for operational uncertainty.

Short-term targets crowd out long-term resilience

The single greatest barrier to strengthening resilience, say 70% of investors, is short-term financial and growth targets—ahead of legacy infrastructure and technical complexity. Their own behaviour confirms this. Eighty-three per cent at least somewhat prioritise short-term growth over long-term resilience investment, and 87% favour scaling up AI deployment over infrastructure readiness. Part of the reason lies in measurement. Some 37% of institutional investors say the return on resilience investment is unclear, well above the 26% of respondents overall. This is an odd complaint because, as the next section shows, investors' own valuation practices are already putting a price on resilience.

How resilience is reshaping investment strategy

As data centre projects become more complex, few investors will be able to manage these risks directly and many will have to bear their financial consequences. Investors' primary role is financing data centre growth. But increasingly they need to price in how risks spread across digital infrastructure and assess whether these AI factories can continue to generate returns while withstanding shocks.

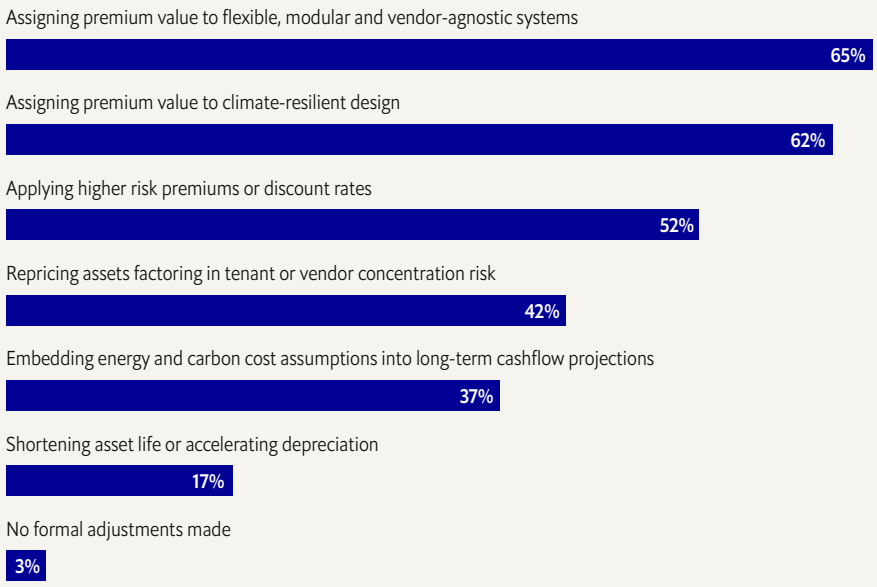
Valuation models are being rewritten

Only 3% of institutional investors say they make no formal adjustment to valuation models in response to emerging systemic shocks. Nearly two-thirds say they now assign premium value to flexible, modular and vendor-agnostic systems. About three in five assign a premium to climate-resilient design. Just over half apply higher risk premiums or discount rates. Two in five re-price assets for tenant or vendor concentration (see Figure 3). Some 17% are also shortening asset lives or accelerating depreciation—a sensible hedge against chips that improve relentlessly and cooling systems that date. These sentiments point to a resilience premium emerging in private markets. Investors seem to believe that assets that can be re-racked, re-cooled and re-let are worth more than the ones optimised for a single tenant and a single generation of hardware. That premium is the market's own answer to the "unclear return" on resilience.

Gonzague Boutry, head of digital infrastructure Europe at private equity firm Ardian, says resilience is reflected not through a single valuation adjustment, but through "assumptions on the asset's future resale value and the cost of significant upgrades". This leads prudent investors to engage closely with tenants and operators to anticipate changes in the technology data centres are filled with.

Figure 3: Resilience enters valuation

Investors' approaches to valuing digital infrastructure amid emerging systemic shocks



Source: Economist Enterprise survey, February–April 2026

Investors keep the exit door open, and that is itself a risk

Presented with sustained-shock scenarios, the investors we surveyed were two to three times likelier than the value chain overall to walk away. If a technology breakthrough rendered a large share of existing assets obsolete, 20% of investors would exit, against 7% of all respondents. Under emergency water restrictions, 14% would exit versus 6%. Under a prolonged chip-supply disruption, 7% would walk versus 3%. Exit is a portfolio manager's prerogative, and for any single fund it is prudent. But footloose capital at scale is precisely the "investment withdrawal" that investors themselves rank among the sector's most systemic threats. The behaviour investors fear most in aggregate is the behaviour they individually reserve the right to display. Notably, where investors feel constraints can be engineered around, they stay. Faced with indefinite grid delays and spiking power prices, 55% would maintain their positions and absorb the cost.

Investors watch the priced signals and miss the political ones

When asked to identify the five most important risk signals they monitor, investors' early-warning dashboards track what trades. About four in ten say they monitor electricity-price volatility, roughly two-thirds watch grid-connection delays and refusals, and 45% audit changes in insurance pricing, coverage limits or exclusions. But only 12% monitor media and political scrutiny of resource use, and just 5% track public opinion and protests—the cheapest and earliest warnings of the constraint that stalled US$130bn of projects in three months. Planning objections and council votes rarely appear on a Bloomberg terminal, which may be why the value chain's least tracked signal proved, in early 2026, its most binding.

Governance is half-built

The inputs of resilience are largely in place. About four in five investors report dedicated resilience capital allocation while 55% report structured engagement with insurers and investors, both above the survey average. However, the wiring between them is lacking. Only 11% of institutional investors report formal crisis co-ordination across all critical internal and external stakeholders—the lowest of any group—while 32% mainly co-ordinate internally, case by case. Just 12% engage communities and only a third rehearse their response to the cascading failures of compound shocks, despite our research showing how grid constraints can trigger operational failures, community opposition and regulatory intervention. It turns out that investors have bought the components of resilience but have not connected them.

Presented with sustained-shock scenarios, the investors we surveyed were two to three times likelier than the value chain overall to walk away.

Closing the gaps in resilient investment

Investors are increasingly factoring resilience into investment decisions. But protecting long-term value means looking beyond today's risks to tomorrow's vulnerabilities. Our research identifies four gaps where investors can strengthen resilience across investment decisions, asset management and portfolio strategy.

Investment decisions

Gap 1:

Climate risk remains underweighted in investment decisions

Investors are adjusting their models to reward climate resilience in digital infrastructure. Yet, when asked to report their three biggest risk considerations, only 14% of investors cite climate exposure and physical risk before considerations of cyber and energy security.

Climate risk is difficult to price, and frequently weighted less than immediate financial risks, because its impacts are long-term, location-specific and often lack consistent metrics.

Recommended actions:

Assess climate scenarios before choosing sites, not after capital has been committed

Investment decisions should account for how assets perform under future climate conditions, not just today's operating environment. "Data centre planning should not assume unlimited power, unlimited water or smooth supply chains," cautions Simon Allen, a data centre growth adviser.

Formal guidance from Britain's Task Force on Climate-related Financial Disclosure suggests that investors make climate-informed site selection part of due diligence and apply short-, medium- and long-term climate scenarios to test whether assets can continue operating and retain value as heat stress, water scarcity, grid constraints and insurance costs intensify.[8]

> **"Data centre planning should not assume unlimited power, unlimited water or smooth supply chains."**
>
> **Simon Allen, data centre growth adviser**

> **" Data centres need to be designed for today's chips and the next generation of hardware. Flexibility must be built in from the start because technology requirements can change faster than the asset life cycle."**
>
> **Gonzague Boutry,**
> **head of digital infrastructure Europe, Ardian**

Gap 2:

Technological obsolescence risk may not be fully priced

Graphics processing units, the chips that power most AI workloads, have a useful life of four to six years in high-density data centres, according to an estimate from financial analytics firm Moody's.[9] Over a 20-year financing horizon, the computing equipment housed within a facility could therefore pass through several replacement cycles.[10] A building need not become obsolete each time its servers do. But if new generations of hardware require materially different power distribution, cooling systems or rack densities—and the facility cannot be economically upgraded—its revenues and residual value could deteriorate.

The financial consequences of technological obsolescence may be substantial. In a modelled case study, international credit agency ARC Ratings found that a facility with high obsolescence risk was valued around 35% lower than a low-risk asset and generated approximately 24% less revenue.[11] Yet only around 5% of investors in our survey identify technological obsolescence as a top-three investment risk.

The findings suggest a potential asymmetry in how obsolescence risk is reflected in valuations. Investors cited premiums for adaptable assets, but relatively few report adjusting asset lives or depreciation schedules to reflect the exposure of less adaptable facilities.

Recommended actions:

Price adaptability into investment decisions

"Data centres need to be designed for today's chips and the next generation of hardware," says Mr Boutry. "Flexibility must be built in from the start because technology requirements can change faster than the asset life cycle."

Investors should therefore treat adaptability as a core component of technical and financial due diligence. Assessments should test whether facilities can accommodate future increases in power demand, compute density and advanced cooling. They should also estimate the cost and disruption involved and determine who bears those costs under lease and financing agreements. These findings should feed directly into assumptions about capital expenditure, lease renewal, depreciation and residual value.

Asset management

Gap 3:

Harder-to-measure risks are underweighted

Investors focus on risks they can measure, such as cyber-attacks, power disruption and supply-chain delays. This is because they can be incorporated into assumptions about downtime, capital expenditure, insurance costs and discount rates. Harder-to-measure risks, such as community opposition or cascading failures, are less consistently reflected in investment decisions despite their potential to affect long-term asset values. Only 2% of investors weigh community acceptance and only 5% monitor public opinion. No investor surveyed is confident community backlash can be managed.

Christopher Jelfs, data centres sector lead at construction company Laing O'Rourke, adds, "Some of the most significant risks facing large-scale data centre developments remain difficult to quantify during the early stages of project planning. Factors such as community acceptance, planning certainty, infrastructure readiness and latent site conditions can all have a material impact on delivery outcomes and long-term asset performance. Developing more consistent approaches to assessing these risks would help improve project certainty and support more informed investment decisions as demand for digital infrastructure continues to grow."

" Some of the most significant risks facing large-scale data centre developments remain difficult to quantify during the early stages of project planning. Factors such as community acceptance, planning certainty, infrastructure readiness and latent site conditions can all have a material impact on delivery outcomes and long-term asset performance. Developing more consistent approaches to assessing these risks would help improve project certainty and support more informed investment decisions as demand for digital infrastructure continues to grow."

Christopher Jelfs,
data centres sector lead, Laing O'Rourke

Recommended actions:

Stress test how operational shocks affect financial outcomes

Leonard Schliesser, senior researcher at the Centre for Security Studies at the ETH Zurich, a university, argues: "Some risks can be priced using historical data and return intervals, but scenario-based and cascading risks such as community backlash are harder to quantify because they lack clear probabilities."

Investors should model how events such as power disruption, cooling failure, cyber-attack or supply-chain delays could affect downtime, capital expenditure, insurance terms, refinancing risk, asset life and exit value.

Stress testing helps investors assess these "what if" risks even when they cannot be modelled precisely.

Portfolio strategy

Gap 4:

Hidden dependencies can undermine diversification

Shocks rarely stay contained. A heatwave can strain the power grid, forcing operators to cut cooling, increasing insurance costs and fuelling community opposition as services come under pressure. A cyber-incident can spread through shared vendors, platforms or tenants, leading to revenue loss. Yet, according to our survey, more than eight in ten investors prioritise concentrating assets to maximise return over geographic diversification to reduce systemic risk. And only a third of investors conduct compound-shock simulations or rehearsals, leaving them potentially exposed to risks that cascade across assets, geographies and portfolios.

Recommended actions:

Run portfolio-level stress tests to identify shared dependencies

Stress tests need to reflect reality and look beyond a single-facility outage to compound scenarios involving cyber-intrusion, physical disruption, loss of power or cooling, connectivity failure and operational recovery.

Some considerations that could better inform stress tests at a systemic level include:

- Recovery times, failover arrangements, redundancy levels and incident-response capabilities
- The impact of compound shocks, such as simultaneous power outages, cooling failures, cyber-attacks or cloud-region disruptions
- Concentration risks across operators, suppliers, regions, power grids and jurisdictions
- How disruptions could affect downtime, insurance coverage, refinancing conditions, asset life and exit value.

Stress tests need to reflect reality and look beyond a single-facility outage to compound scenarios involving cyber-intrusion, physical disruption, loss of power or cooling, connectivity failure and operational recovery.

Investing in assets built to endure

The data centre market is expanding, but growth alone will not protect the value of investments. Investors are already pricing data centre risk through premiums, discount rates and asset selection. But a greater challenge is knowing whether assets—and the systems that support them—can adapt, remain insurable and retain value when shocks combine.

That requires investors to ask tougher questions before they commit capital. Can the asset adapt to new chips, cooling systems and cyber-security demands? Will the site remain viable under heat stress, water scarcity, grid strain and insurance repricing? Are portfolio assets genuinely diversified, or do they share the same power, vendor, tenant, regulatory or climate exposure?

Answering these questions will require investors to understand how data centre risks move across interconnected systems and what role different stakeholders play in those systems.

Five actions for data centre investors:

1. **Integrate resilience into investment due diligence.**
2. **Price adaptability into asset valuations.**
3. **Translate operational disruption into financial exposure.**
4. **Map concentration risk across the portfolio.**
5. **Use compound scenarios to challenge investment decisions.**

References

1. The cost of compute: A $7 trillion race to scale data centers. McKinsey Quarterly, McKinsey & Company. April 28th 2025. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers
2. Tech AI spending may approach $700 billion this year, but the blow to cash raises red flags. CNBC. February 6th 2026. Available at: https://www.cnbc.com/2026/02/06/google-microsoft-meta-amazon-ai-cash.html
3. Meta partners with Blue Owl Capital on $27 billion AI data center project. CNBC. October 21st 2025. Available at: https://www.cnbc.com/2025/10/21/meta-blue-owl-capital-partner-on-27-billion-ai-data-center-project-.html
4. Q1 2026: Data Center Watch Report. Data Center Watch. Available at: https://www.datacenterwatch.org/q1-2026
5. Americans Oppose AI Data Centers in Their Area. Gallup. May 13th 2026. Available at: https://news.gallup.com/poll/709772/americans-oppose-data-centers-area.aspx
6. The Economist. (2026). The financialisation of AI is just beginning. 17 February. Available at: https://www.economist.com/finance-and-economics/2026/02/17/the-financialisation-of-ai-is-just-beginning
7. Investigation Results and Future Measures on Cyber Attack Data Exposure. Asahi Group Holdings. November 27th 2025. Available at: https://www.asahigroup-holdings.com/en/newsroom/detail/20251127-0204.html. See also: Asahi says 1.5 million customers' data potentially leaked in cyber-attack. BBC News. November 27th 2025. Available at: https://www.bbc.co.uk/news/articles/ce86n44178no
8. Task Force on Climate-related Financial Disclosure (TCFD)-Aligned disclosure application guidance. HM Treasure, Gov.UK. Updated July 17th 2025. Available at: https://www.gov.uk/government/publications/tcfd-aligned-disclosure-application-guidance/task-force-on-climate-related-financial-disclosure-tcfd-aligned-disclosure-application-guidance--2
9. The big deal about data centers: Part 2 - Modeling the data center boom. Moody's. June 29th 2026. Available at: https://www.moodys.com/web/en/us/insights/insurance/the-big-deal-about-data-centers-part-2.html
10. Ibid.
11. Data Centre cash flows: Obsolescence matters. ARC Ratings. September 12th 2025. Available at: https://arcratings.com/researches/data centre-cash-flows-obsolescence-matters

About FM

This research programme is sponsored by FM, one of the world's largest commercial property insurers, and is dedicated to helping organisations build resilience and protect long-term business value. Drawing on nearly two centuries of engineering expertise, scientific research and loss-prevention experience, FM helps clients better understand and manage the risks that affect critical operations and infrastructure.

FM Intellium brings together research, engineering insight and resilience intelligence to help organisations evaluate, strengthen and benchmark resilience across the digital infrastructure ecosystem. By providing a clearer view of resilience vulnerabilities, system interdependencies and emerging risks, FM Intellium supports better business, investment and policy decisions in an increasingly complex digital environment.