Executive Summary

Introduction

The vast commercial potential of AI and the growing demand for cloud computing have led to an explosion in demand for data centres. Global compute capacity is expected to nearly triple to about 220 GW by 2030, backed by some US$6.7trn worth of infrastructure spending, of which about US$5.2trn will be for AI workloads alone.[1,2]

These facilities are demanding, relying on land and permits to build, electricity to run, chips to fill them and water for cooling. As capacity expands, the digital economy is becoming increasingly dependent on an interconnected system of data centres, power grids, technology, supply chains and skilled people. However, the barriers are political, as well as physical. Local communities increasingly resist new facilities. In the US, local opposition halted or delayed projects worth tens of billions of dollars in the first three months of 2026 alone.[3]

As data centre projects grow larger and more ambitious, they concentrate more value. This often makes economic sense, but it also creates more dependence on single facilities and raises the cost of disruption. With projects at the scale of one or more gigawatts, a single failure could be felt across the system. Building resilience into this growth from the outset is therefore critical to ensure long-term operational reliability.

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.

Global compute capacity is expected to nearly triple by 2030 to about
220GW

backed by **infrastructure spending** of some
US$6.7 trillion

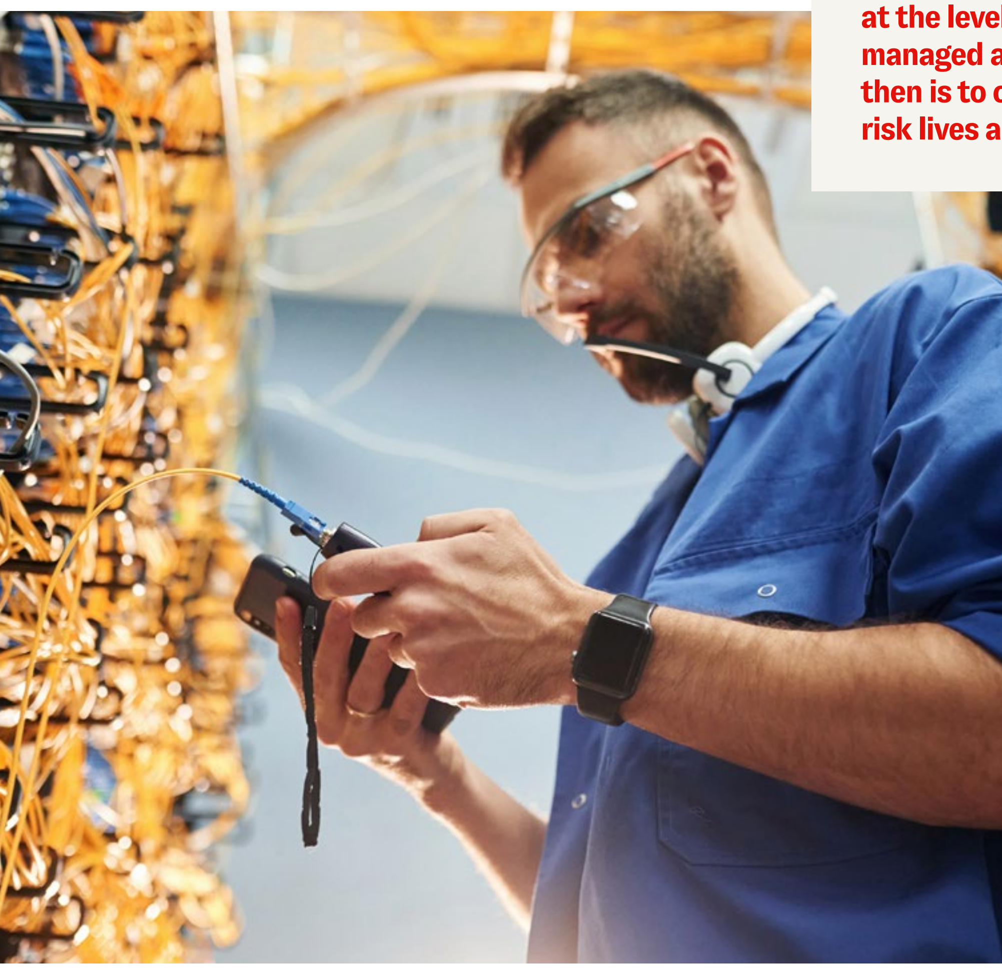
of which about
US$5.2 trillion
would be for **AI workloads** alone

It draws on a global survey of 1,800 leaders across the data centre value chain in 21 countries—including policymakers, data centre owners, developers and operators, as well as those who invest in, and rent out, these facilities. Also based around a scenario-mapping exercise, the research examines the signals, vulnerabilities and strategic decisions that shape the future of these critical systems. The findings and conclusions were informed and validated by an expert advisory board and in-depth interviews with data centre resilience specialists. These include experts in infrastructure investment, operations, cyber-security, urban systems, construction and technology policy.

Our research shows how risks linked to energy and environment, technology and supply chains, and people and organisational governance interact. This information can help decision-makers identify critical vulnerabilities and prepare for compound shocks.

Crucially, our findings suggest that while risk in digital infrastructure is largely generated at the level of the system, it is most often managed at the level of the firm. The aim then is to close the gap between where risk lives and where it is managed.

“ Our findings suggest that while risk in digital infrastructure is largely generated at the level of the system, it is most often managed at the level of the firm. The aim then is to close the gap between where risk lives and where it is managed.”



The data centre value chain

Data centres may look unremarkable from the outside, but they sit at the centre of a fast-growing network of capital, energy, technology and public policy. Investors, owners, operators, tenants and regulators all shape how data centres are built, financed, operated and used—and each holds a different piece of the risk.

Who are the data centre stakeholders?

To map systemic risk and resilience opportunities, across the digital infrastructure value chain, Economist Enterprise categorises the ecosystem into five core stakeholder groups:

Stakeholders	Role in the value chain
Regulators and policymakers	Set the legal, environmental and operational rules that govern digital infrastructure, balancing new data centre development against local limits on land, energy and other resources.
Owners and developers	Secure land, electricity and planning approval, then build the facilities that support the digital economy.
Investors and lenders	Provide capital for expansion while weighing long-term returns against growing regulatory, political and operational risks.
Operators	Keep facilities running by managing power, cooling, security and day-to-day operations. Performance depends on reliability, resilience and efficiency.
Tenants and cloud customers	Lease data centre or cloud capacity, and depend on infrastructure they neither own nor directly control. Reliability, flexibility and predictable costs are priorities.

No participant can secure the resilience of a data centre alone. Decisions made by each and every stakeholder converge in the same facilities. A single constraint, such as limited grid capacity or water scarcity, can affect every part of the ecosystem in different ways.

> **“A single constraint, such as limited grid capacity or water scarcity, can affect every part of the ecosystem in different ways...the risk is shared, and so resilience depends on co-ordinated action across the value chain.”**

For investors, community opposition or tighter regulation can delay or derail multi-billion-dollar projects, increasing financial risk.[4] Governments must balance demand for digital infrastructure against competing demands on energy and industrial capacity. Operators face volatile power demand, higher spending on back-up generation and difficult choices during periods of peak electricity use. For tenants, constrained grids and capped power allocations limit computing capacity, raise costs and increase operational risk—all because they depend on an electricity grid they neither own nor control.

Ultimately, however, the risk is shared, and so resilience depends on co-ordinated action across the value chain. One example from a data centre project in Frankfurt demonstrates how power constraints changed decisions across the value chain. Developers spread new capacity across more locations, operators improved energy efficiency and recovered waste heat, while planners aligned investment with long-term grid capacity. Such measures do not remove systemic risk entirely, but they reduce reliance on any one source of disruption.[5]

Testing resilience under systemic shocks

To understand how risks interact, our research grouped the threats facing digital infrastructure into four categories:

Energy risks

including grid capacity constraints, energy transition shortfalls and vulnerabilities in decentralised power systems.

Technology risks

including supply-chain concentration, core network fragility, advanced cyber-security threats and rapid technological obsolescence.

Organisational and human risks

including fragmented governance, critical skills shortages and failures to integrate climate risk into long-term planning.

Macro-environmental risks

including physical climate stress, regulatory interventions, tightening financing conditions and local community backlash.

In modern data centres, disruptions rarely occur in isolation. Two structural features explain why. The first of these is tight coupling, where facilities, grids and networks are so closely linked that stress in one quickly spreads to the others. Second is concentration, where a small number of power markets, cable routes and equipment suppliers account for a disproportionate share of global capacity.

To understand how disruptions spread through these structural vulnerabilities, we used cross-impact analysis to classify risks into two categories.

Primary triggers are acute shocks that initiate disruption, such as cyber-attacks, physical damage to facilities or critical equipment failures. **Amplifiers** are underlying friction points that escalate the shock and determine how far it spreads. They include climate stress, such as rising temperatures and water scarcity, organisational failures that hinder co-ordination, and growing community opposition that constrains expansion or recovery.

Data centre stakeholders cannot eliminate every potential trigger, but they can reduce both the likelihood and impact of many disruptive events. Because the factors that amplify them are the residue of past decisions about procurement, hiring, siting and governance.

Our research modelled three scenarios that illustrate how an initial trigger—whether physical, environmental or technological—ripples across the value chain, turning an isolated situation into a sustained regulatory, financial and operational disruption.

A selection of the scenarios we developed and tested

Scenario 1: The cooling constraint	Extreme heat and drought expose the vulnerability of cooling systems that depend on water. Local communities mobilise against perceived resource hoarding, leading to restrictions on how much water data centres can use. As operational facilities are forced to power down servers to stay within water caps, returns plummet. Investors are prompted to pull funding from any new projects in the region due to the escalating environmental, social and governance and regulatory risks.
Scenario 2: The stranded data centre	A rapid shift to ultra-high-density AI chips leaves many legacy data centres unable to support next-generation workloads. Facilities that lack the structural load capacity, electrical infrastructure or direct-to-chip liquid cooling needed for modern hardware quickly become obsolete. As tenants migrate to purpose-built sites, asset values fall sharply, while uncertain retrofit standards leave operators with stranded infrastructure.
Scenario 3: The chip choke-point	A disruption at a dominant chipmaker chokes the global supply of critical hardware. Customers are forced to use fewer platforms, increasing the risk of outage. Fearing such fragility, governments intervene with aggressive sovereign tech mandates, national chip-rationing and export controls to secure access to essential components for domestic industries.

Understanding how risks can spread is not an academic exercise. It is a requirement for sound executive decision-making and capital allocation across the digital economy.

As data centres face risks with increasingly systemic impacts, resilience planning should evolve beyond protection of individual facilities. It requires understanding how risks interact across the system, as well as balancing growth with long-term constraints such as energy, land and technology. The key findings below show how stakeholders across the data centre value chain can build resilience while protecting long-term value.

Key findings

1

Rapid data centre expansion is challenging resilience and forcing trade-offs

More than 90% of the stakeholders we surveyed report experiencing a material disruption to their digital infrastructure in the past five years. It's no surprise then that around two-thirds report board or governing-body oversight of digital infrastructure resilience. Three-quarters say their organisations are investing in resilience initiatives.

Yet investment does not necessarily translate into preparedness for every type of disruption. When forced to make trade-offs, more than 80% prioritise growth, efficiency and AI deployment over long-term resilience, while preparedness for interconnected and compound risks appears less mature. This matters because decisions made during expansion—including where facilities are built and how much structural capacity they have—can be costly to reverse and may shape how risks spread and amplify across interconnected systems.

Making data centres more resilient and expanding them need not be competing priorities. Decision-makers should seek to tie their risk-management plans to their business objectives to achieve both.

2

Pressure to meet short-term data centre growth targets can increase exposure to cascading "amplifier risks" when resilience is not built in earlywhen resilience is not built in early

Decision-makers recognise that amplifier risks—including supply-chain disruption, climate change and community opposition—can have system-wide effects. More than two-thirds rank supply-chain disruption among the top five systemic risks, yet only about half are confident in their ability to manage it. The challenge is not only to manage individual risks, but also to understand how they interact and amplify one another across interconnected systems. Climate risk shows a similar gap between concern and confidence.

Unlike primary triggers, amplifier risks often extend beyond individual facilities. They spread through supply chains, electricity grids, public infrastructure and markets, making them harder to anticipate and manage than traditional operational risks. This helps explain why respondents express less confidence in their ability to manage them.

At the same time, the pressure to expand sees no sign of easing. Seven in ten respondents identify short-term financial and growth targets as a barrier to strengthening digital infrastructure resilience. Organisations therefore tend to invest in resilience measures that deliver immediate operational benefits. Cyber-security is the most widely adopted measure (91%), followed by physical protection of control systems (88%), peak-demand optimisation (87%) and diversified energy supplies (85%).

Measures that address amplifier risks—including geographic diversification, climate-informed site selection and compound-shock simulations—remain less common. Although these measures often require greater upfront investment and longer planning horizons, the research suggests that decisions made early in development can strengthen resilience. As digital infrastructure expands, companies across the data centre value chain have an opportunity to consider these risks from the outset, strengthening long-term resilience against shocks that can spread and amplify across interconnected systems. The consequences of such disruption may extend beyond operations to financial performance, investor confidence and long-term enterprise value

Some underutilised resilience strategies are:

% share of respondents adopting each measure

Geographic diversification
12%

Climate-informed site selection
22%

Asset obsolescence stress testing
26%

Compound-shock simulation
30%

Data centre operators are right to fund defences that keep their facilities humming, including cyber-security, physical protection and energy resilience. Yet to stop isolated crises from snowballing, they should also invest to broaden supply chains, replace outdated kit and run rigorous stress tests.

3

Today's emerging risks could become tomorrow's constraints

Cyber-attacks, grid constraints and extreme weather dominate stakeholders' perceptions of systemic risks. More than 75% of each group selected all three among the five risks most likely to have system-wide effects. For the investors we surveyed, the withdrawal of investment or insurance coverage ranks as the second most important systemic risk after cyber-attacks.

By contrast, slower-moving emerging risks receive less attention despite their potential long-term potential to influence future investment, expansion and resilience outcomes across the ecosystem. Fewer than 5% of survey respondents rank community opposition among their top five systemic risks and barely a tenth cite technological obsolescence. This is despite the fact that public opinion is increasingly shape siting and expansion decisions, while technological change could affect investment choices and long-term resilience.

The evidence for this is growing. A Gallup poll from March this year found that seven in ten Americans oppose data centres in their area. Nearly half strongly oppose their construction, citing concerns about drains on resources and higher energy prices.[6] This scepticism is increasingly translating into organised action. According to Data Centre Watch, an advocacy group which tracks local opposition to data centre construction in the US, local resistance contributed to delays or cancellation affecting more than 75 data centre projects, worth around US$130bn, in early 2026 alone.[7]

Resilience planning should therefore consider not only immediate threats but also slower-moving risks and how they may interact and amplify disruption across interconnected systems.

To assess a facility's long-term worth, investors, developers and operators must look beyond traditional risks and factor in local public opinion, future regulations and the lifespan of the underlying technology.

4

Siloed planning could undermine resilience across the system

System-wide resilience depends on effective co-ordination between owners, operators, utilities, suppliers, regulators and other partners. However, planning and preparedness efforts often remain focused on individual parts of the data centre value chain.

Just 10% of those surveyed maintain structured crisis plans with all critical external partners. Almost two-thirds engage with only a select few, while a quarter stick to internal planning and reach out only when disaster strikes. This isolation could cripple readiness. A mere third possess cross-functional crisis teams, and only 30% run compound-shock simulations. Consequently, businesses across the data centre value chain may have limited visibility into how wider networks would respond to cascading disruptions.

The failure to work together extends beyond crisis response. About one in four developers cite complex multi-party co-ordination as one of the main obstacles to building new data centres.

As digital infrastructure becomes more interconnected, resilience depends increasingly on understanding how risks interact. Data centre stakeholders should strengthen their defences by mapping critical dependencies, identifying potential points of failure and testing how disruption might spread through the wider system.

5

Human capital is a resilience challenge across the data centre value chain

True resilience requires a skilled workforce capable of operating and repairing increasingly complex data centres. Yet investment in human capital is not keeping pace with rapid sector expansion, with fewer than half of respondents maintaining dedicated talent pipelines or training programmes.

Data centre operators, who run the facilities, grasp the challenge. Around 35% of operators—the highest share for any group—expect skills shortages to lead to failures in infrastructure resilience. By contrast, only around one in six investors identify workforce capability as a systemic risk, signaling a need for deeper integration and dialogue between asset owners and operators on human capital resilience.

The consequences are already becoming apparent. About 60% of data centre operators struggle to recruit qualified staff.[8] As specialist engineers become scarce, incidents take longer to be diagnosed and resolved, and new capacity takes longer to bring online. This spells service disruptions for tenants and eroded returns for investors.

The entire data centre industry must treat human capital as a strategic priority. When plotting new sites, investors and developers should weigh the supply of specialist talent as heavily as power, land and connectivity. Operators must look beyond hardware, pairing technical defences with rigorous training and disaster drills so staff can handle complex crises. Tenants, meanwhile, should vet their providers' staffing levels, fatigue management and emergency readiness.

As data centres face risks that can spread across organisations, supply chains, portfolios and even countries, resilience is no longer just about protecting individual facilities. It requires understanding how risks interact across the system and balancing growth with long-term constraints such as energy, land and technology.

Appendix

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

The report accompanies a survey, which captures the perspectives of four groups: governments, investors, owners and developers, and tenants. The analysis is based on a survey of 1,800 senior executives from these groups, across 21 countries: Australia, Belgium, Canada, Denmark, France, Germany, Hong Kong, India, Italy, Malaysia, the Netherlands, Saudi Arabia, Singapore, South Korea, Spain, Sweden, Switzerland, Thailand, the UAE, the UK and the US. The survey was conducted in March and April 2026.

Additional insights were obtained from in-depth interviews with the following experts:

- **Simon Allen**, data centre growth adviser
- **Aline Blankertz**, tech economy lead, Rebalance Now
- **Gonzague Boutry**, managing director of infrastructure, Ardian
- **Tom Gao**, chief technology and digital services officer, City of Sydney
- **Chris Jelfs**, data centres sector lead, Laing O'Rourke
- **Leonard Schliesser**, senior researcher at the Center for Security Studies, ETH Zurich
- **Piers Wilson**, cyber-security and data privacy manager, International Schools Partnership

Economist Enterprise would also like to thank FM colleagues, specifically **Adrian Oxley**, **Michael Perron** and **Sandor Becz**.

To explore the research findings further, and to learn what actions can be taken by different stakeholders in the data centre value chain to build resilience, please visit our executive insight guides for data centre investors and tenants. You can also explore our findings and recommendations at a country level across country profiles covering the Australia, Canada, France, Germany, India, Netherlands, Saudi Arabia, Southeast Asia, UAE, the UK and the US.

References

1. 2026 Global Data Center Outlook: Navigating AI demand, power constraints and global opportunities in 2026. JLL. January 5th 2026. Available at: https://www.jll.com/en-in/insights/market-outlook/data-center-outlook
2. 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
3. Q1 2026: Data Center Watch Report. Data Center Watch. Available at: https://www.datacenterwatch.org/q1-2026
4. $130 Billion in AI Data Centers Stalled: The Bottleneck Is Consent. Forbes. July 22nd 2026. Available at: https://www.forbes.com/sites/robertszczerba/2026/07/22/130-billion-in-ai-data-centers-stalled-the-bottleneck-is-consent/
5. Frankfurt Data Centers: FRAI Power Constraints and Pipeline Migration. Neospaces. May 19th 2026. Available at: https://neospaces.de/en/insights/frankfurt-data-center-fra1-power-2026-q2
6. 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
7. Q1 2026: Data Center Watch Report. Data Center Watch. Available at: https://www.datacenterwatch.org/q1-2026
8. World Economic Forum, "The Data Centre Boom Needs a Resilient Workforce – Here's How to Build One," September 24, 2025. Available at: https://www.weforum.org/stories/2025/09/data-centre-resilient-workforce/