ECONOMIST IMPACT

Foundations at risk:

assessing the resilience of data centres and digital infrastructure

Sponsored by

Contents

About this report

Foundations at risk is a report by Economist Impact, sponsored by FM, that examines the medium-to-long-term risk landscape affecting data centre operations. The report provides recommendations for data centre operators and businesses on how to increase the resilience of their digital infrastructure.

Economist Impact drew on desk research, expert consultations and proprietary risk analysis to identify and rank ongoing risks and emerging threats in the contextual and operating environment that have an impact on the running of data centres. We then developed a framework measuring the resilience of the digital infrastructure of 12 countries.

Economist Impact would like to extend our thanks to the following experts for their time and insights throughout this research programme:

- Mark Bjornsgaard, chief executive, Deep Green Technologies
- Laveena Iyer, technology and telecommunications analyst, EIU
- Isabelle Kemlin, business and innovation executive, RISE - Research Institutes of Sweden; vice-chair, Swedish Data Centre Industry Association
- Zahl Limbuwala, operating partner, DTCP
- Per Sieverts Nielsen, senior researcher, Department of Technology, DTU Management
- Herbert Radlinger, managing director, NDC-GARBE data centres Europe
- Leonard Schliesser, senior researcher, Risk and Resilience Team, Center for Security Studies (CSS), ETH Zürich
- Richard Taylor, emeritus professor, Penn State University
- Dexter Thillian, lead analyst, technology and telecoms, EIU
- Piers Wilson, head of product management, Huntsman Security

Executive summary: the nature of digital infrastructure risk

Modern businesses are critically dependent on data centres—they are the unseen yet crucial backbone of the global economy, ensuring the seamless operation of everything from our financial systems and internet connectivity to smart home technologies. Yet the complexity of global supply chains, accelerating data centre demand fuelled by the rapid growth of artificial intelligence (AI), rising sustainability pressures and rapidly evolving technology stack create a dense web of risks. Many of these threats are emerging and still not fully understood.

At the same time, businesses face strategic questions on where and how to expand digital infrastructure, including which markets or contingency measures might best protect them against outages, regulatory and geopolitical shifts, and climate-driven disruptions. Business leaders are under pressure to balance operational continuity, competitive advantage and environmental commitments in a context of overlapping uncertainties. Our research aims to address these gaps by mapping current and emerging risks and provides practical guidance on how business leaders can strengthen the resilience of their data centre investments and strategies.

The disruptive forces affecting data centres—from supply-chain breakdowns to climate events—involve deep uncertainties that defy precise forecasting. These risks are systemic, with interdependencies that span supply chains, geopolitics, human behaviour and environmental events that strain traditional risk assessment methods. Rather than attempting to predict specific outcomes, organisations must strengthen their capacity to manage uncertainty by exploring multiple plausible risk scenarios.

The interconnectedness of data centres and cloud infrastructure means that they represent systemic risk hubs—disruption in one major facility can trigger an unpredictable chain of failures potentially affecting entire economic sectors. For example, power constraints at one facility could cause cooling-system failures during extreme weather events, triggering wider outages that compromise both operational continuity and cybersecurity and drive knock-on effects far beyond the affected site. Serious failure at a dominant cloud provider, such as Amazon Web Services (AWS), could send shockwaves throughout our financial system by, for instance, incapacitating multiple banks or services simultaneously.[1] Understanding

[1] Duke Financial Economics Center (FinReg Blog). A New Source of Systemic Risk: Cloud Service Providers. August 8 2019. Available at: https://sites.duke.edu/thefinregblog/2019/08/08/a-new-source-of-systemic-risk-cloud-service-providers

these interdependencies is essential. Resilience planning must therefore consider both direct impacts and these ripple effects throughout interconnected systems.

To gain a comprehensive understanding of the risks facing data centres and digital infrastructure, Economist Impact undertook a rigorous, multi-phase research programme. The analysis presented in this report is grounded in the findings from a literature review, in-depth interviews and a Delphi survey with experts, horizon scanning and systemic risk analysis, and a benchmarking exercise across selected countries. Our key findings are:

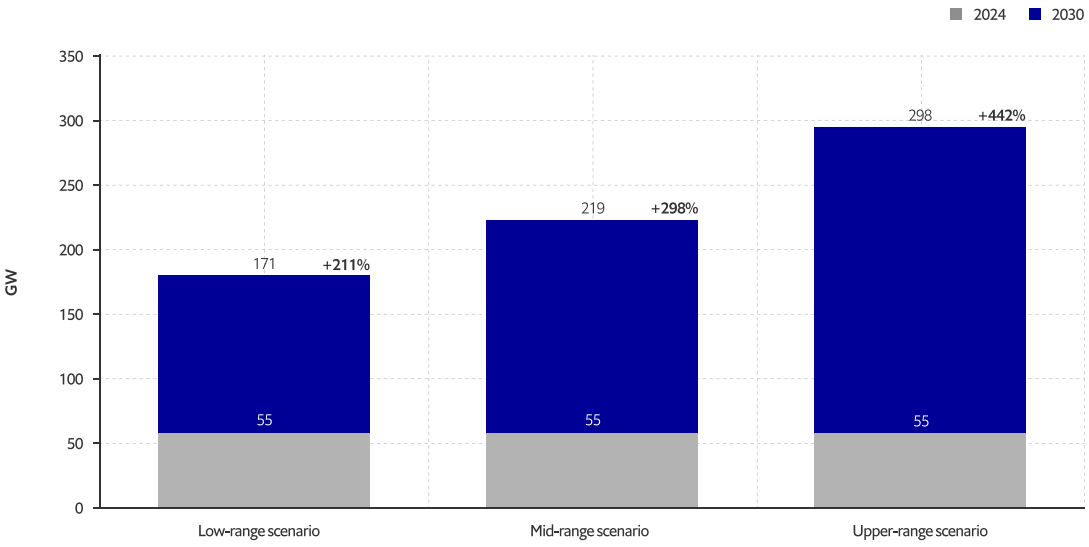
- **AI is driving an unprecedented surge in data centre capacity and energy demand.** Training large-scale models requires vast computer resources, prompting a wave of retrofits to accommodate new infrastructure. Conventional facilities with air-based cooling and limited power density are becoming obsolete, prompting a shift to liquid-cooling technologies and high-density racks that can support AI workloads. Operators are racing to construct new AI-dedicated data centres at the gigawatt scale, with forecasts suggesting annual demand could reach 219 GW by 2030.[2] This transformation is expected to more than double data centre electricity consumption to 945 TWh by 2030.[3] This raises pressing concerns about energy availability, sustainability and grid stability.
- **Systemic risks pose severe threats to data centre resilience.** Trade tensions, climate change, political instability and quantum computing are the most serious challenges. They have high impact and high uncertainty, and each has cascading effects that amplify vulnerabilities across global supply chains, digital services, and economies.
- **The range of suppliers and locations is too concentrated.** Heavy reliance on a small number of semiconductor suppliers, hyperscale cloud providers and overstretched locations like Dublin and northern Virginia has created structural fragility, raising the risk that a single point of failure could trigger widespread global disruption.
- **Environmental constraints are taking hold.** As AI causes data centre energy demand to grow, power grid strain, water scarcity and growing regulatory scrutiny over heat, water reuse and land use are reshaping data centre plans in key markets.
- **Data centres are becoming frontline geopolitical assets.** As hybrid warfare blurs the lines between digital and physical conflict, data centres face escalating risks, from cyber-attacks and forced service withdrawals to sabotage of physical infrastructure like undersea cables. Incidents linked to the Russia-Ukraine war and rising tensions in the Taiwan Strait highlight how political instability can disrupt digital services, threaten supply chains and undermine trust in critical infrastructure.
- **Quantum computing poses a looming threat to data centre architecture and cybersecurity.** Quantum breakthroughs could render widely used encryption methods obsolete, exposing sensitive data to decryption risks and undermining trust in digital infrastructure. Beyond security, quantum computing may introduce entirely new cooling, processing and integration demands, pushing operators to overhaul physical infrastructure once commercial-scale machines become viable.

[2] McKinsey & Company. AI power: Expanding data center capacity to meet growing demand. October 29 2024. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand

[3] International Energy Agency. Energy and AI—Executive summary. April 2025. Available at: https://www.iea.org/reports/energy-and-ai/executive-summary

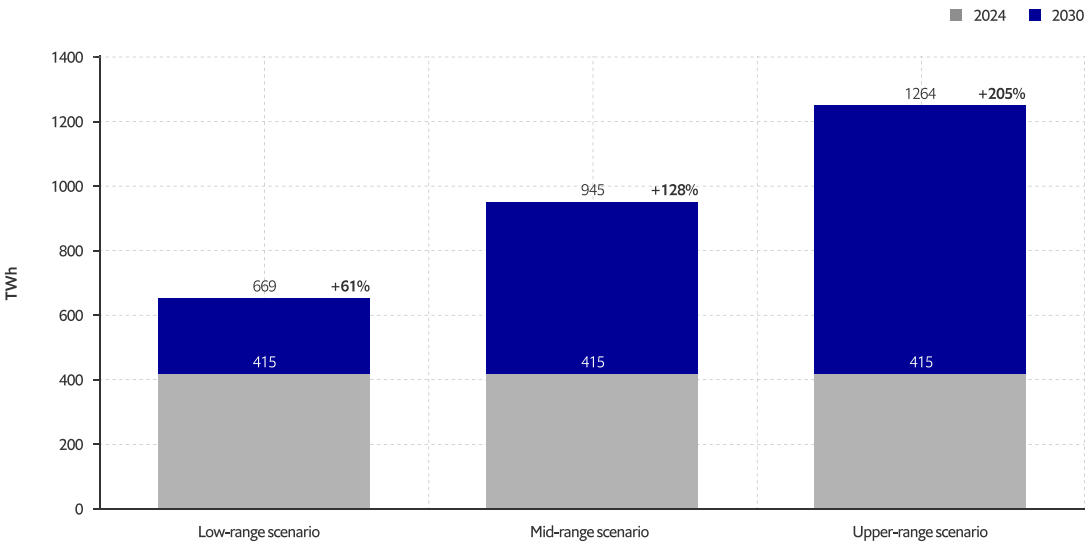
Global Data Capacity Forecast Scenarios

in gigawatts



Global Data Centre Electricity Consumption Forecast

in terawatt-hours



Source: McKinsey Data Centre Demand Model, International Energy Agency

Note: the mid-range scenario growth is based on existing forecast estimates.

To strengthen the resilience of digital infrastructure in an increasingly complex risk environment, stakeholders must take a proactive, multifaceted approach, including the following:

- **Data centre operators should prioritise geographic diversification to reduce exposure of physical assets to compound risks from climate events, cyber incidents and geopolitical volatility.** Outages in key regions like London and Virginia have demonstrated how regional clustering can amplify disruption. Distributing infrastructure across varied climate zones and jurisdictions can improve operational continuity and support national digital sovereignty.
- **All stakeholders with assets in digital infrastructure should integrate scenario planning and regulatory foresight into investment strategies to future-proof digital infrastructure.** For example, proactively anticipating changes in zoning regulations, sustainability requirements and data localisation policies helps to prevent stranded assets and ensures infrastructure remains aligned with evolving regulatory landscapes.
- **Policymakers should focus on strengthening national capacity in data centre infrastructure and key upstream components,** such as semiconductors, cooling systems and fibre networks. This will be essential in reducing reliance on volatile global supply chains. Emerging efforts in countries like Brazil and India to revive domestic production underscore the strategic importance of industrial policy in securing resilient and self-sufficient digital infrastructure.
- **As sustainability standards and regulatory requirements evolve, data centre operators need to boost efforts to embed circularity,** such as heat reuse, water recycling and component repurposing, into data centre design and operations. As jurisdictions like Germany and Singapore introduce mandates on resource reuse, circularity is becoming a key factor in regulatory compliance and long-term operational viability. Proactively integrating these practices will help to strengthen the resilience of infrastructure and guide responsible investment.

By embracing these strategic priorities—diversification, scenario planning, national capacity building and circularity—stakeholders can build a more resilient, sustainable and future-ready digital infrastructure. Coordinated action today will not only mitigate emerging risks but also ensure long-term value and operational continuity in a rapidly evolving global landscape.

Identifying systemic risks in the data centre ecosystem

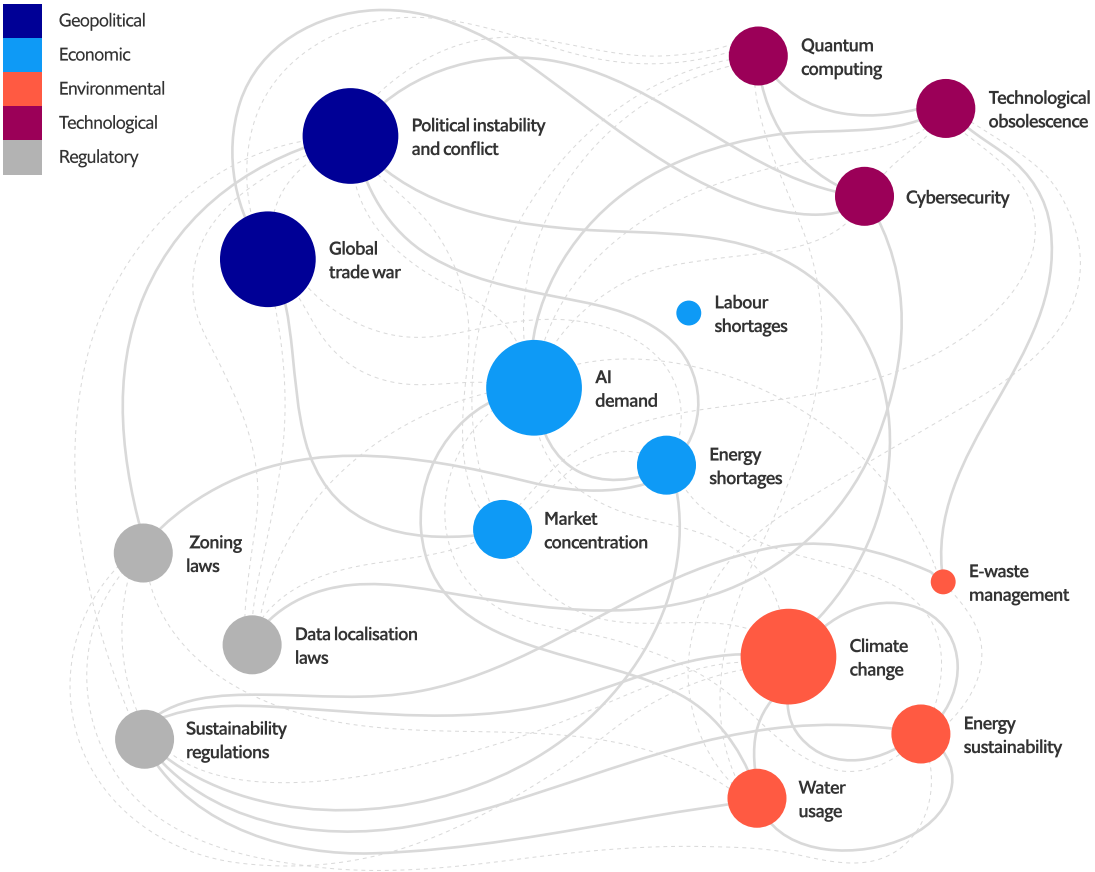
Data centres have become indispensable to the functioning of critical infrastructure, underpinning sectors such as healthcare, transportation, finance, government and emergency services. As digitisation accelerates, they serve as the foundational layer upon which these systems rely for continuous and reliable operation. However, this growing dependence also amplifies the vulnerabilities within this layer, highlighting the urgent need to identify and map the systemic risks facing data centres.

A cross-impact risk analysis exercise helped us to identify the most important risks faced by data centres. We identified the threat of a global trade war, climate change, quantum computing, and political instability and conflict as the most impactful and least certain risks in our analysis. These risks have cascading effects, meaning that their occurrence is highly likely to influence other contextual and transactional risks to the operating environment of data centres and digital infrastructure.

Our systems map (see figure 1) shows the interconnectedness of risks discussed in this report. The size of the bubble indicates the level of impact and uncertainty; the thickness of the linkages indicates the degree of interconnectedness. This reveals the systemic nature of certain geopolitical and technological risks identified in the literature and through engagement with experts.[4]

[4] Through a systematic literature review and series of expert interviews, Economist Impact identified risk factors in the contextual and operating environment that could disrupt data centre operations over a ten-year time horizon across economic, geopolitical, technological, environmental and regulatory risk pillars. We filtered and prioritised these risks based on assessments of their relative impact and perceived likelihood. We then conducted a cross-impact analysis of the risks to examine the strength and character of interconnections of risks in pairs, resulting in a score that reflects overall risk intensity. A higher number indicates a higher risk.

Figure 1: Global risks landscape, an interconnected map



Our analysis highlights four primary systemic risks that could undermine the entire digital infrastructure underpinning many of our everyday systems:

Trade tensions and national security	Climate change
Political instability and hybrid conflict	Quantum computing

The remainder of this section will provide an overview of each of these systemic risks and why they matter for businesses.

Trade tensions and national security

The outbreak of a global trade war goes beyond just protectionist policies on goods and services trade, posing systemic risks to data centre operations and businesses dependent on their services.

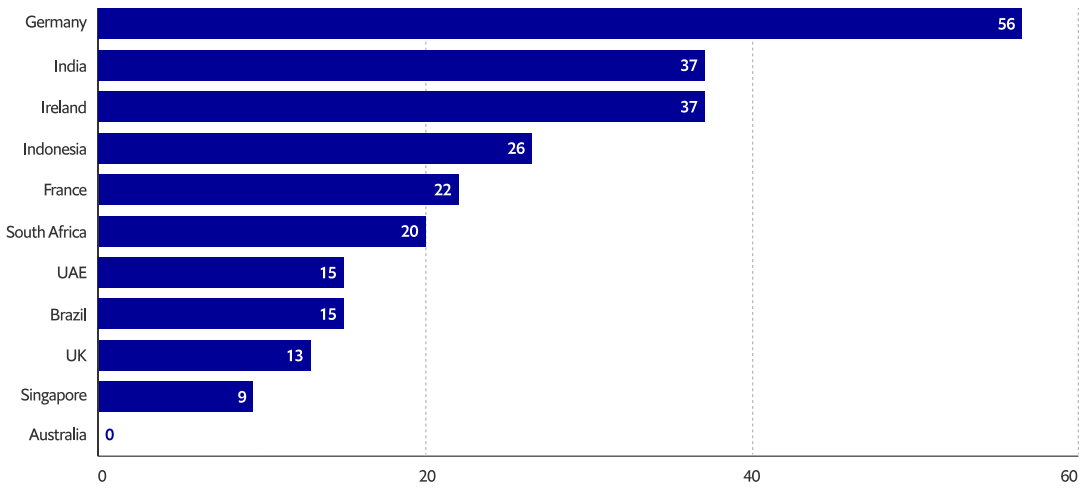
Geopolitical tensions, particularly between the US and China, are reshaping the global data centre landscape. As semiconductors and cloud infrastructure become strategic assets, they are increasingly subject to export controls, sanctions and retaliatory measures. A full-scale trade war would disrupt the global supply of critical components such as chips, rare-earth metals and server hardware, causing delays and cost surges for data centre operators and the businesses that rely on them. Recent controls by the US on advanced semiconductor exports to China, along with China's retaliatory restrictions on critical minerals essential for semiconductor production, could delay equipment deliveries, increase costs, and limit data centre capacity expansion amid strong demand.[5,6]

Businesses dependent on data centres are at risk of experiencing slower service delivery, higher operational costs and a reduction in access to new data centre capacity. The uncertainty surrounding future access to critical semiconductor components could force companies to reconsider their supply-chain sourcing, with some possibly looking to diversify their sources or even relocate their data centre operations to regions less affected by the trade war in semiconductors and critical inputs.[7]

Figure 2: Exposure to changes in trade policy

How exposed is the country to the impacts of a trade war with the US under the Trump administration?

(0=low risk, 100=high risk)



Source: Economist Intelligence Unit (2025)

[5] US Department of Commerce, Bureau of Industry and Security. Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications. December 2 2024 (press release). Available at: https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military

[6] Eversheds Sutherland. U.S. and China tighten respective export restrictions on advanced technology and critical minerals. January 10 2025. Available at: https://www.eversheds-sutherland.com/en/united-states/insights/us-and-china-tighten-respective-export-restrictions-on-advanced-technology-and-critical-minerals

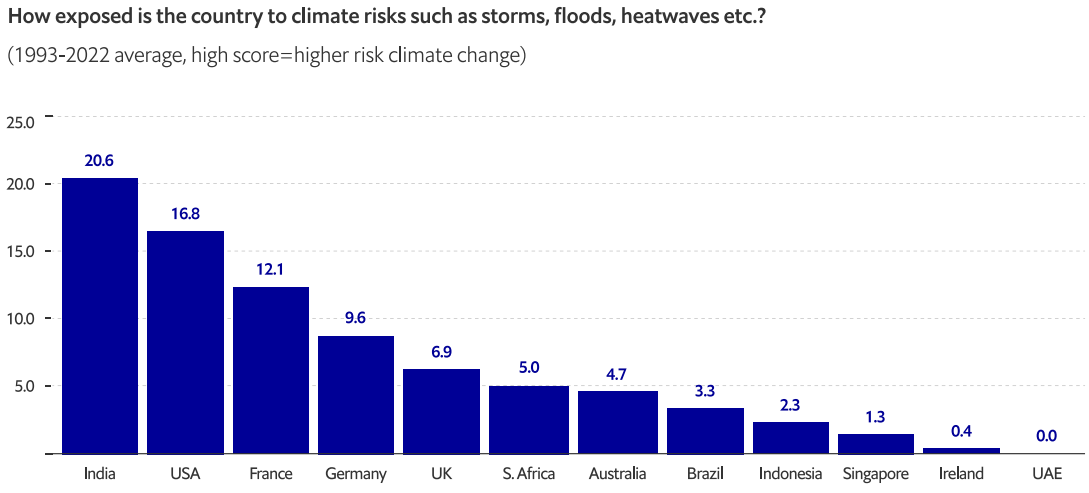
[7] Ibid.

Analysis by EIU shows that ten of eleven countries assessed are exposed to trade policy change enacted by the US administration of Donald Trump (see figure 2). Only Australia scores a zero in this measure, highlighting the high vulnerability of the majority of the countries in this assessment.[8] As data centres become entangled in strategic competition, businesses will need to proactively assess and adapt their supply chains, ensuring resilience against disruptions that could affect performance, growth and digital sovereignty.

Impacts of climate change

The rising frequency of extreme weather events poses a serious threat to economies and societies worldwide. According to the Climate Risk Index (CRI), which assesses the impact of climate-related extreme weather events on countries, measuring both human and economic losses, the average long-term climate risk level across the 12 countries assessed is only 6.9, suggesting lower climate risk compared with other countries included in the CRI.[9] For example, the country most affected by highly unusual climate events was Dominica, with a score of 56.7, while the least affected was the UAE with a score of 0.00.

Figure 3: Climate risk



Source: Germanwatch Climate Risk Index (2025)

Data centres are highly sensitive to environmental conditions—they depend on stable power and efficient cooling, which can be disrupted by extreme weather events. As the climate warms, record-breaking heat waves and other weather extremes are emerging as a serious threat to data

[8] Economist Intelligence Unit (EIU). Viewpoint — Article (subscription page). Available at: https://viewpoint.eiu.com/analysis/article/1372119137
[9] Germanwatch. Climate Risk Index 2025. February 2025. Available at: https://www.germanwatch.org/sites/default/files/2025-02/Climate%20Risk%20Index%202025.pdf

centre uptime. In the summer of 2022 an unprecedented heat wave in the UK caused cooling systems to fail at both Google's and Oracle's London data centres, disrupting operations.[10] The impacts of the outage were not isolated—it affected cloud customers in the US and Pacific region who relied on services from the London facilities. Similarly, in California a heat wave in September 2022 took down a Twitter data centre in Sacramento, causing a total shutdown of physical equipment at the site.[11] Research shows that 45% of US data centres have experienced an extreme weather event that threatened operations.[12] These incidents underscore the ever-increasing risk that extreme weather events associated with climate change pose to data centre infrastructure.

The nature of physical climate risks varies by region—heatwaves, wildfires, floods, hurricanes and severe storms each present unique challenges that demand different resilience measures. For example, intensified monsoons and cyclones in South Asia are predicted to increase flooding risks,[13] while prolonged droughts and an extended wildfire season threaten communities and key infrastructure on the US west coast.[14]

As climate risks intensify and diversify across geographies, data centre operators must move beyond reactive responses and embed climate resilience into long-term planning and infrastructure design. The growing threat of extreme weather events makes it clear: safeguarding digital infrastructure is not just a technical challenge but also a critical component of climate adaptation strategies worldwide.

Political instability and hybrid conflict

Escalating political instability and conflict can lead to hybrid warfare involving both conventional and unconventional instruments of power and tools of subversion. Cybersecurity risks escalate as large-scale cyber-attacks or malware campaigns between rival factions inflict economic damage, intensify geopolitical tensions and erode trust in digital infrastructure.

Data centres are physical assets subject to national jurisdictions. In politically unstable regions or active conflict zones, they become vulnerable to direct sabotage or forced shutdowns. The Russia-Ukraine conflict saw cloud providers like Oracle and SAP abruptly withdraw services from Russia, showing how political events can cause business-critical infrastructure loss.[15] Hybrid warfare further raises the spectre of sabotage—particularly of undersea cables and data centres—to disrupt communications and digital services. Countries near conflict zones or adversarial regimes face elevated risks.

Although the likelihood of another major conflict breaking out remains low, EIU identifies a direct military conflict between the US and China in the Taiwan Strait and South China Sea as a remote yet highly impactful risk for the global economic system and regional supply chains.[16]

[10] BBC. Heatwave forced Google and Oracle to shut down computers. 2022. Available at: https://www.bbc.com/news/technology-62202125
[11] Data Center Knowledge. Google, Oracle Data Centers Knocked Offline by London Heat. July 28 2022. Available at: https://www.datacenterknowledge.com/cooling/google-oracle-data-centers-knocked-offline-by-london-heat
[12] Uptime Institute. Extreme weather affects nearly half of data centers. 2021. Available at: https://journal.uptimeinstitute.com/extreme-weather-affects-nearly-half-of-data-centers/
[13] Frontiers. Regional climate change impacts—Explainer. October 2024. Available at: https://www.frontiersin.org/journals/science/article-hubs/regional-climate-change-impacts/explainer
[14] NASA. Effects of Climate Change.Available at: https://science.nasa.gov/climate-change/effects/
[15] Smolaks M. Data Center Knowledge. SAP is Shutting Down Russian Data Centers, Leaving the Country. April 20 2022. Available at: https://www.datacenterknowledge.com/cloud/sap-is-shutting-down-russian-data-centers-leaving-the-country
[16] Economist Intelligence Unit (EIU). Viewpoint — One-click report (subscription page). Available at: https://viewpoint.eiu.com/analysis/article/1962158996

A military conflict in the Taiwan Strait poses severe risks for high-tech industries, given the global reliance on Taiwan's advanced semiconductor sector and the Strait's strategic position for regional and global shipping routes. A rise in hostilities between China and Taiwan, requiring US intervention, would severely disrupt the supply and production of the most advanced chips needed for data centre expansion.

Data centres are also vulnerable to physical sabotage driven by hybrid conflict between geopolitically rivalrous countries. The Nord Stream pipeline sabotage in the Baltic Sea in 2022 demonstrates how physical attacks on infrastructure can have an impact on critical networks. Similar attacks could target undersea telecommunications cables, potentially resulting in internet shutdowns, with implications for vital infrastructure. According to EIU, critical infrastructure sabotage and hybrid attacks are key risks facing some European countries, particularly those exposed to the Baltic Sea underwater cables and in close proximity to Russia.[17]

In an era of rising geopolitical volatility and hybrid threats, data centres are no longer insulated digital hubs—they are strategic assets exposed to the frontlines of political conflict. Ensuring their resilience will require not only technical safeguards but also coordinated geopolitical risk planning across both the public and private sectors.

The rising threat of quantum computing

Although widely considered a decade away, breakthroughs in quantum computing will necessitate a complete overhaul of existing data centre infrastructure to accommodate its unique processing requirements and security needs. This transition presents significant challenges, including the need for specialised hardware, software integration and advanced cooling systems. The potential for quantum computers to compromise existing cybersecurity measures could have cascading effects across multiple critical sectors, such as healthcare, energy, finance and agriculture, which are increasingly reliant on secure digital communications and data storage.

Quantum computing may also pose a systemic risk to critical data and digital infrastructure owing to its potential to break widely used encryption methods that secure sensitive information.[18] Traditional cryptographic systems, such as RSA and ECC, rely on the computational difficulty of factoring large numbers or solving discrete logarithmic problems—challenges that classical computers struggle with but quantum computers solve exponentially faster.[19] This capability threatens the security of financial transactions, government communications, healthcare records and other essential digital infrastructure. If geopolitical rivals or adversaries gain access to sufficiently powerful quantum computers, they could decrypt confidential data, undermine cybersecurity frameworks and disrupt global digital economies.

[17] Economist Intelligence Unit (EIU). Viewpoint — Denmark (country/region landing, subscription page). Available at: https://viewpoint.eiu.com/analysis/article/442139644
[18] Denning DE. American Scientist. Is Quantum Computing a Cybersecurity Threat?. 2019. Available at: https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat
[19] Quantum Zeitgeist. Quantum technologies in cybersecurity: potential and limitations. July 2023. Available at: https://quantumzeitgeist.com/quantum-technology-and-its-implications-for-cybersecurity

The uncertain evolution of AI demand

AI usage has supercharged the demand for data centres, a trend expected to continue for the foreseeable future. Even before 2023 and the release of AI platforms for public use, expectations for data center demand were high due to the trajectory of data growth (Figure 4). Several trends will push demand significantly higher in the coming years: a shift toward big data, more workloads in the public cloud and robust IT spending.[20] Recent forecasts suggest that global demand for data centre capacity could rise at an annual rate of 19-22% between 2023 and 2030.[21] Traditional business workloads—file storing and sharing, transaction processing cloud computing—will continue to constitute the majority of data centre demand growth. AI-related computing will be the fastest-growing segment driving growth in data centre power demand—it is projected to make up around 60% between 2023 and 2028.[22] In the light of this, the data centre sector will require larger amounts of energy. The IEA expects global electricity consumption to increase at the fastest pace in years in 2025-27, citing the rapid expansion of data centres worldwide, among other factors.[23]

Although the outlook for AI-driven data centre demand remains predominantly bullish, there are a series of critical uncertainties about AI that may affect demand for data centre capacity. Breakthrough innovations, efficiency gains and technological progress in the AI space may stifle demand for backbone computing power. Recent developments in AI have shown signs of breakthroughs that may challenge demand growth assumptions. China's DeepSeek was able to train a frontier model using less electricity than its main competitors; its rapid and surprising emergence precipitated a sell-off of major energy companies and data centre infrastructure providers.[24] Microsoft has recently scrapped leases for large data centres in the US, indicating oversupply.[25] This suggests relative uncertainty around the power demand of AI and whether, if further breakthroughs proliferate in the market, electricity demand or indeed computing power may be lower than previously predicted.

A further uncertainty for AI-driven data centre demand is around the balance between training

[20] Tsoneva T, Affleck J. CBRE Investment Management. Decoding Data Centers: Opportunities, risks and investment strategies. July 17 2024. Available at: https://www.cbreim.com/insights/articles/decoding-data-centers
[21] McKinsey & Company. AI power: Expanding data center capacity to meet growing demand. October 29 2024. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand
[22] Lee V, Seshadri P, O'Niell C, et al. Boston Consulting Group. Breaking Barriers to Data Center Growth. January 20 2025. Available at: https://www.bcg.com/publications/2025/breaking-barriers-data-center-growth
[23] International Energy Agency. Electricity 2025. February 2025. Available at: https://www.iea.org/reports/electricity-2025
[24] Financial Times. DeepSeek threat exposes guesswork on AI power demand, says IEA. February 2025. Available at: https://www.ft.com/content/0cc897c2-e12d-4143-81ff-e56c5381a5a1
[25] Soni A. Reuters. Microsoft data center leases slowing, analysts say, raising investor attention. February 24 2025. Available at: https://www.reuters.com/technology/microsoft-shelves-ai-data-center-deals-sign-potential-oversupply-analyst-says-2025-02-24/

and inference/reasoning requirements as these models evolve. Currently, around 80% of AI-related demand is for training tasks—which are computationally demanding—compared with 20% for inference.[26] But as models mature and training becomes more efficient, the focus is expected to shift more towards inference tasks, which require low latency (the time it takes for data to travel from the source to the destination and for a response to return), and therefore will need to be closer to end-users. Over the next five to ten years, the training to inference ratio is forecast to reverse, with 80% of the demand coming from inference/reasoning tasks.[27]

In addition, new research on AI-model training methods challenges the conventional assumption that ever-larger clusters of GPUs (graphics processing units; AI chips) clusters are the key to progress. Approaches such as Google's Distributed Low-Communication Training of Language Models (DiLoCo) and experiments by Prime Intellect suggest that distributing training across multiple smaller data centres could reduce communication overhead and improve efficiency.[28,29] Although models trained this way might struggle to reach peak performance on familiar tasks, their application to new tasks is improved. If these methods gain traction, demand for hyperscale data centres could stabilise, with AI workloads shifting towards a more decentralised computing model. Such developments complicate the long-term outlook for energy consumption in AI infrastructure.

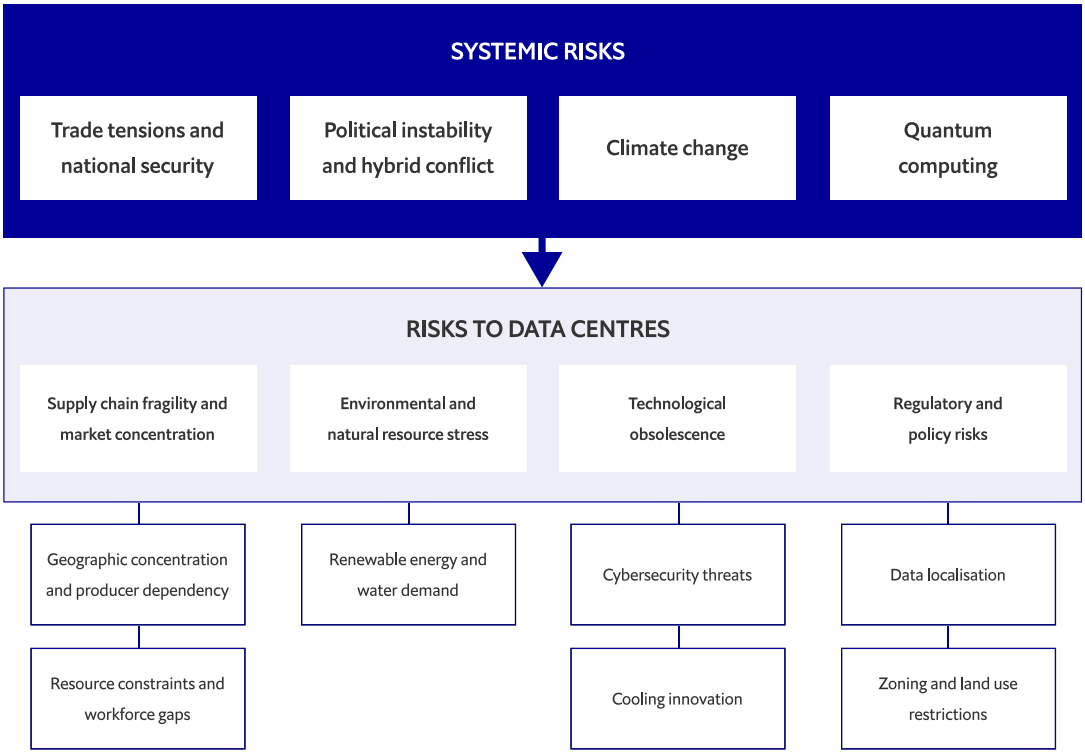
[26] Alvarez & Marsal. Rethinking AI Demand Part 1: AI Data Centers Are Experiencing a Surge of Training Demand — What Happens When the Surge Is Over? February 25 2025. Available at: https://www.alvarezandmarsal.com/insights/rethinking-ai-demand-part-1-ai-data-centers-are-experiencing-surge-training-demand-what
[27] Ibid.
[28] Google DeepMind. DiLoCo: Distributed Low-Communication Training of Language Models. November 14 2023. Available at: https://deepmind.google/research/publications/57039
[29] Prime Intellect. State-of-the-art in Decentralized Training. April 23 2024. Available at: https://www.primeintellect.ai/blog/our-approach-to-decentralized-training

Cascading risks facing data centres

The systemic risks discussed in the previous section are not isolated shocks but catalysts that interact with and amplify other vulnerabilities in the data centre operating environment. Their ripple effects cascade across technological, environmental and economic domains, compounding operational complexity and exposing fragilities. For instance, trade restrictions on semiconductors and critical minerals choke the global hardware supply chain, delaying the construction of new facilities and inflating costs for operators and their clients. Climate-induced extreme weather events not only threaten physical data centre assets but also strain regional energy and water systems, exacerbating local tensions over scarce resources. Escalating hybrid conflicts and sabotage campaigns raise the spectre of targeted attacks on undersea cables or national data infrastructure, undermining regional connectivity and business continuity. Meanwhile, the looming quantum threat is triggering urgent but costly overhauls in encryption standards and hardware design, with consequences for cybersecurity preparedness across sectors.

These systemic shocks expose and accelerate existing vulnerabilities, ranging from skilled labour shortages and energy constraints to regulatory hurdles and technological obsolescence, demanding a fundamentally more adaptive and distributed approach to infrastructure design and governance.

Figure 4: The ripple effects of systemic risks



Supply-chain fragility and market concentration in the digital infrastructure ecosystem

The data centre ecosystem relies on a complex web of globally interconnected supply chains that are vulnerable to systemic disruptions at multiple levels. Vulnerabilities span availability of key resources (such as energy, water and land), labour shortages and the availability of key technical equipment such as critical hardware.

Geographic concentration and producer dependency

Advanced semiconductors—critical to data centre operations—are largely produced by a handful of firms in limited geographies. The high level of market concentration raises concerns about competition and pricing, potentially affecting downstream consumers. Taiwan manufactures around 90% of the most advanced chips, primarily through TSMC, and ASML (Netherlands) dominates lithography machine supply.[30,31] Similarly, Nvidia controls over 80% of the GPU market.[32] This geographic and vendor concentration also introduces systemic risk. Any disruption, whether geopolitical, environmental or industrial, could halt data centre construction

[30] Davidson H, Lin C. The Guardian. How Taiwan secured semiconductor supremacy – and why it won't give it up. July 19 2024. Available at: https://www.theguardian.com/world/article/2024/jul/19/taiwan-semiconductor-industry-booming
[31] Sloan D. Fortune. This $362 billion 'beyond well-positioned' Dutch company is quietly winning the global AI chips race. April 18 2024. Available at: https://fortune.com/2024/04/18/asml-semiconductor-ai-manufacturing-uev-lithography-chips-act-nvidia-tsmc-wafers/
[32] Allan D. TechRadar. Nvidia now owns 88% of the GPU market — but that might not be a bad thing ... yet. June 7 2024. Available at: https://www.techradar.com/computing/gpu/nvidia-now-owns-88-of-the-gpu-market-but-that-might-not-be-a-bad-thing-yet

and operations globally. The risk is compounded by the dominance of a few hyperscale cloud providers (AWS, Azure and Google), whose infrastructure forms the backbone of digital businesses.

Resource constraints and workforce gaps

The primary concern is that data centre demand may lead to energy shortages, particularly in regions where there is already a high density of data centres. Data centres accounted for more than 10% of the total electricity consumption in five US states (Virginia, Iowa, Nebraska, North Dakota and Oregon) in 2023.[33,34] In Ireland, data centres now account for over 20% of all electricity consumption.[35] The rapid expansion of data centres, combined with slow progress in upgrading power grids and expanding generated capacity, increases pressure on local power networks. Furthermore, the clustering of data centres in prime urbanised locations, such as the European hubs of London, Frankfurt, Amsterdam and Paris, may increase pressure on already stretched energy grids, potentially leading to higher energy costs for operators, businesses and consumers.

Local governments are in some cases intervening to stop further expansion in data centre capacity in cities, owing to power capacity issues. In Ireland, grid operator EirGrid has imposed a moratorium on new data centre developments in Dublin until 2028. In November 2023 the UK government rejected a plan for a new hyperscale farm in London owing to pressures on the energy supply.[36] Countries like Germany, Singapore and China have also imposed restrictions on new data centre projects.

Shortage of skilled professionals in this industry is prevalent across the entire data centre lifecycle, ranging from data centre construction to AI development roles. This creates further operational risks as the likelihood of human errors increases. Industry reports reveal that operators are experiencing a chronic shortage of skills, particularly qualified personnel to design, operate and maintain data centre infrastructure. According to a global data centre survey conducted annually by Uptime Institute, over 50% of data centre operators report difficulty hiring and retaining qualified staff.[37] Staffing and skills pressures remain one of the highest operational challenges across the sector, with industry leaders calling for more efforts to expand labour pools and skillsets to match the pace of capacity growth.[38] Labour shortages pose an operational risk to data centres. An overstretched workforce may lead to fatigue and mistakes, which may put the security of data centres and business operations at risk. Human error remains a leading cause of data centre outages. Uptime Institute estimates human factors contribute up to 50% of outages.[39]

[33] Spencer T, Singh S. International Energy Agency. What the data centre and AI boom could mean for the energy sector. October 18 2024. Available at: https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector
[34] EPRI. Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption. 2024. Available at: https://www.epri.com/research/products/3002028905
[35] Moss S. Data Center Dynamics. Irish data centers used more than 21 percent of nation's total metered electricity. July 23 2024. Available at: https://www.datacenterdynamics.com/en/news/irish-data-centers-used-more-than-21-percent-of-nations-total-metered-electricity/ Datacenter Dynamics
[36] Savills Research. Spotlight: European Data Centres. May 2024. Available at: Savills PDF
[37] Uptime Institute. Global Data Center Survey 2024. July 2024. Available at: https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2024.GlobalDataCenterSurvey.Report.pdf?version=0
[38] Ibid.
[39] Uptime Institute. Annual Outage Analysis 2024—Executive Summary. March 2024. Available at: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2024

Environmental and natural resource stress

Renewable energy and water demand

Renewable energy has become a critical concern worldwide owing to data centres' rapidly growing energy demands and the pressure to reduce carbon emissions in the light of climate change. Data centre power demand is expected to increase by 12% annually until 2030, potentially doubling the tech sector's current carbon emissions.[40] This surge in energy consumption, coupled with constraints on renewable generation growth, implies that about 60% of new demand in the US could be met by natural gas, affecting the sector's decarbonisation efforts.[41] The gap between rapid data centre construction and the slower pace of expanding and strengthening renewable energy grids and generation capacity is exacerbating the strain on local power networks.[42]

Water usage for manufacturing chips and cooling data centres also poses sustainability risks for data centre operators and businesses at large. The semiconductor industry, crucial for producing chips used in data centres, is extremely water-intensive. It is estimated that a single semiconductor fabrication plant can use up to 10m gallons of water per day, equivalent to the water consumption of a city of 60,000 to 300,000 people.[43] This intensive water use puts pressure on local water resources, especially in water-stressed regions. Water consumption for air-based cooling systems is a major concern for data centre operators. A 1-MW data centre using traditional air-based cooling methods can use as much as 26m litres of water a year.[44] As the demand for data processing grows, driven by technologies such as AI, water usage is expected to increase substantially.[45] For instance, Google reported that its data centres collectively consumed 23bn litres of water in 2024.[46] This high water consumption is particularly problematic in water-stressed areas, where data centres compete with local communities and agriculture over scarce water resources. In some cases, this has sparked local protests against data centre developments, as seen in Uruguay.[47]

Technological obsolescence

Cybersecurity threats

Data centres and the systems that they host are prime targets for cyber-attacks, which represent a growing technological risk. Damage to critical infrastructure from cyber-attacks is one of the top global risks facing major economies, according to EIU risk scenarios.[48]

[40] S&P Global Ratings. Data Centers: Rapid Growth Will Test U.S. Tech Sector's Decarbonization Ambitions. October 30 2024. Available at: https://www.spglobal.com/ratings/en/regulatory/article/241030-data-centers-rapid-growth-will-test-u-s-tech-sector-s-decarbonization-ambitions-s13302390
[41] Goldman Sachs Asset Management. Powering America: Investing in the Nation's Energy Future. 2025. Available at: https://am.gs.com/en-se/advisors/insights/article/2025/powering-america-investing-in-the-nations-energy-future
[42] Spencer T, Singh S. International Energy Agency. What the data centre and AI boom could mean for the energy sector. October 18 2024. Available at: https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector
[43] Singer P. Semiconductor Digest. Managing the Impact of Semiconductor Manufacturers' Use of Freshwater. January 10 2025. Available at: https://www.semiconductor-digest.com/managing-the-impact-of-semiconductor-manufacturers-use-of-freshwater/
[44] Sensorex. Data Center Water Usage Challenges and Sustainability. August 16 2022. Available at: https://sensorex.com/data-center-water-usage-challenges/
[45] Li P, Yang J, Islam M, et al. Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models. March 2025. Available at: https://arxiv.org/pdf/2304.03271
[46] Gunyol A. Anadolu Agency. Google data centers used nearly 6B gallons of water in 2024. February 11 2025. Available at: https://www.aa.com.tr/en/world/google-data-centers-used-nearly-6b-gallons-of-water-in-2024/3478721
[47] Spindler W, Hahn-Petersen LA, Hosseini S. World Economic Forum. Why circular water solutions are key to sustainable data centres. November 7 2024. Available at: https://www.weforum.org/stories/2024/11/circular-water-solutions-sustainable-data-centres/
[48] Economist Intelligence Unit. One-click report (EIU country/sector snapshot). Available at: https://viewpoint.eiu.com/analysis/article/1422167142

Escalating tensions between rival countries in geopolitical flashpoints (Russia-Ukraine, the Middle East, US-China) may increase tit-for-tat cyber-attacks targeting key state infrastructure. Cloud-based infrastructure, which is attracting more business and government data, is a vulnerable target. Such attacks could disrupt national communications and payment systems for businesses, as well as causing the loss of customer data.

Cooling innovation

As central processing unit (CPU) and GPU processing capabilities continue to grow exponentially, data centres are getting bigger, requiring more energy, higher-density racks and more efficient cooling systems. Older data centres outfitted with conventional cooling systems are at risk of becoming obsolete or being considered stranded assets as growing demand from AI processing requires more efficient cooling systems to run energy-intensive workloads. AI servers also consume higher levels of energy, requiring a shift from air-based to liquid-based cooling systems. Air-based cooling—a process that transfers heat by circulating cold air around servers—is considered to be effective only up to power densities of 50 kW per rack, an inadequate level for training AI workloads.[49] The shift towards liquid-based cooling systems such as direct-to-chip and liquid immersion cooling allows for power densities of up to 150 kW per rack, owing with higher thermal-transfer properties.[50,51] This also enables operators to reduce power usage by as much as 90% compared with air-based cooling methods.[52] Scaling liquid-cooling systems across AI data centres globally remains a challenge owing to higher component and retrofit costs to existing infrastructure. It also poses additional risks owing to increased thermal concentration in the event of a system failure. Uncontrolled heat build-up—known as thermal runaway—can lead to equipment damage and potential fire risks.[53]

Regulatory and policy risks

Data localisation

Governments are increasingly introducing stricter data localisation regulation. Localisation laws pose a risk to the operations of data centres and their clients, as more countries are mandating how data is stored, processed and transferred across different jurisdictions. Governments implement data localisation measures primarily to enforce privacy protections, such as those under the EU's GDPR, which restricts cross-border data transfers, as well as for regulatory compliance in sectors like banking and insurance.[54,55] More notably, data localisation measures are falling under national security and industrial policy considerations as governments implement digital protectionism to develop strategically important high-tech

[49] McKinsey & Company. AI power: Expanding data center capacity to meet growing demand. October 29 2024. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand
[50] CyrusOne. The Future is Liquid: How In-Rack and Direct-to-Chip Cooling are Revolutionizing Data Centers. August 8 2024. Available at: https://www.cyrusone.com/resources/blogs/in-rack-and-direct-to-chip-cooling-revolutionizing-data-centers
[51] McKinsey & Company. AI power: Expanding data center capacity to meet growing demand. October 29 2024. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand
[52] Ramachandran K, Stewart D, Hardin K. Deloitte Insights. As generative AI asks for more power, data centers seek more reliable, cleaner energy solutions. 19 November 2024. Available at: https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/genai-power-consumption-creates-need-for-more-sustainable-data-centers.html
[53] Van Gorp P. HKA. Navigating Data Centre Fire Protection: Understanding Lithium-ion (Li-ion) Battery Hazards. April 22 2024. Available at: https://www.hka.com/article/navigating-data-centre-fire-protection-understanding-lithium-ion-li-ion-battery-hazards/
[54] European Union. General Data Protection Regulation (Regulation (EU) 2016/679). April 2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[55] Organisation for Economic Co-operation and Development (OECD). The Nature, Evolution and Potential Implications of Data Localisation Measures. November 10 2023. Available at: https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html

sectors amid strong geopolitical rivalries.[56]

According to the OECD, as of 2023 close to 100 localisation measures had been introduced across 40 countries.[57] Two-thirds of these measures are restrictive: governments impose local storage and processing requirements without the possibility of data flows outside of the country. These measures are found to have an impact on both data centre operators and businesses. Data localisation laws increase operating costs for cloud service providers, who rely on economies of scale to offer cheaper services, affecting small and medium-sized enterprises disproportionately. Restrictive localisation laws also raise concerns around cybersecurity risks, as operators are not freely able to share threat data across jurisdictions to identify specific types of threats and vulnerabilities.[58] Restrictive localisation laws increase data management costs by 16-55%, according to a business survey conducted by the OECD and the World Trade Organisation.[59,60]

Rules on zoning and land use

Land pricing and data centre construction costs have steadily risen across key markets that provide access to power, fibre connectivity, proper zoning, water and sewage management. According to a report by Savills, a real-estate firm, greenfield data centre construction costs have increased by 6% year on year in 2022-23, with key markets in Europe (Zurich, London and Frankfurt) the most expensive globally for new data centre development.[61] Growing constraints on land availability and land pricing in prime urbanised areas have prompted data centre development to shift towards secondary cities in key markets.[62] In Europe, the Nordics and secondary cities in Germany, Belgium and the UK are emerging as options for new data centre construction owing to lower land prices, abundant renewable energy sources, robust grid infrastructure and low energy prices. Since innovations in AI—for example through chain-of-thought reasoning—no longer require low latency, data centre operators can now prioritise location, cost and sustainability over proximity to end users when developing new infrastructure.[63]

[56] Yayboke E, Ramos C, Sheppard L. Center for Strategic & International Studies (CSIS). The Real National Security Concerns over Data Localization. July 23 2021. Available at: https://www.csis.org/analysis/real-national-security-concerns-over-data-localization
[57] OECD. OECD in Figures 2024: Data on the World Economy. 2024. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf
[58] Ibid.
[59] Depending on the type of localisation measure.
[60] OECD/World Trade Organisation. Economic Implications of Data Regulation. 2025. Available at: https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf
[61] Savills Research. Spotlight: European Data Centres. May 2024. Available at: Savills PDF
[62] Cushman & Wakefield. 2024 Global Data Center Market Comparison. 2024. Available at: https://www.cushmanwakefield.com/en/insights/data-center-advisory-group/2024-global-data-center-market-comparison
[63] Lee V, Seshadri P, O'Niell C, et al. Boston Consulting Group. Breaking Barriers to Data Center Growth. January 20 2025. Available at: https://www.bcg.com/publications/2025/breaking-barriers-data-center-growth

Recommendations

The nexus of geopolitical, environmental, technological and economic risks necessitates a comprehensive strategy for data centre operators, businesses and policymakers. Although broad systemic risks are often difficult to mitigate, addressing idiosyncratic risks requires coordinated efforts to ensure the resilience and sustainability of digital infrastructure. The following recommendations provide a roadmap for data centre operators, businesses and policymakers to mitigate these cascading risks more effectively.

1. Geographic diversification

Geographic diversification is foundational to digital resilience. It ensures that no single outage, whether caused by climate, conflict, grid failure or regulatory intervention, can disrupt the continuity of services or compromise data integrity. In December 2021 an outage at an AWS data centre in northern Virginia disrupted services for a wide range of global clients, including major platforms like Netflix, Disney+, Slack and Robinhood, across Europe and the US. The outage affected cloud computing, streaming, smart-home devices and even logistics and package delivery, highlighting how many systems depended on a single regional hub.[64] It is essential for data centre operators and businesses to spread across different geographic locations to minimise co-dependency risks.

In order to avert similar events, data centre operators must diversify their infrastructure through the development of redundant, geographically distributed data centre architecture. These should span different climate zones to hedge against regional weather volatility, cross national borders to avoid sovereign risk concentration and make use of edge locations closer to users for latency-sensitive applications.[65]

Policymakers can help to promote a more geographically balanced distribution of digital infrastructure across regions. The high concentration of data centres in select regions and urban centres such as Dublin, Frankfurt and northern Virginia has not only strained local grids and water supplies but also created national security vulnerabilities. New markets, such as the Nordic countries, have successfully attracted large-scale hyperscaler investment by offering low-cost renewable energy, stable grids and cooler climates that reduce the need for active cooling.

2. Supply-chain restructuring

Diversifying supply chains is critical to mitigating risks associated with geopolitical tensions and component shortages. There are several strategies that data centre operators and businesses can employ to boost resilience, given the current environment. Dual- and multi-sourcing strategies should be formalised for all

[64] Palmer A. CNBC. Amazon Web Services outage brings some delivery operations to a standstill. December 7 2021. Available at: https://www.cnbc.com/2021/12/07/amazon-web-services-outage-causes-issues-at-disney-netflix-coinbase.html
[65] Digital Realty. What Is an Edge Data Centre? Available at: https://www.digitalrealty.co.uk/resources/articles/what-is-an-edge-data-centre digitalrealty.co.uk

critical components. This includes identifying and entering agreements with alternative vendors in geopolitically neutral or low-risk jurisdictions. For instance, some European data centre firms now prioritise sourcing servers and cooling units from vendors with diversified manufacturing bases—within Eastern Europe, Vietnam and India—to hedge against US-China decoupling risks.[66]

Governments have a crucial role in reducing structural dependencies on external suppliers for critical inputs to data centre infrastructure. This entails relocalising parts of the supply chain domestically, investing in local manufacturing capabilities and fostering partnerships between the public and private sectors to reduce reliance on foreign suppliers. One priority is to invest in or incentivise local or regional production of high-risk components, like semiconductors, power supplies and specialised cooling systems. For example, India's Production Linked Incentive scheme for electronics and chip assembly offers a replicable model that provides financial rewards for domestic production linked to output growth.[67]

3. Use scenario planning and regulatory foresight to anticipate policy shifts

Engaging in scenario planning enables organisations to anticipate and prepare for various future regulatory and market conditions. By developing multiple plausible scenarios, businesses can assess potential impacts on operations and make informed investment decisions. Both data centre operators and businesses should employ foresight tools to anticipate possible policy shifts in the digital infrastructure environment. This will be the best way for them to make informed decisions when it comes to future investments.

Anticipating new regulations, particularly related to environmental factors and use of resources, is key to decreasing investment risk associated with operating, managing or relying on data centres in geographies that are already constrained by environmental risks.

Zoning restrictions are being used as tools to address sustainability concerns. Many municipalities now require data centres to adopt measures such as enhanced buffering near residential areas or stricter noise standards to mitigate their environmental footprint. The city of Chandler in Arizona has restricted data centre development to specific zones owing to concerns over noise and environmental impacts. These changes reflect growing tension between the industry's expansion needs and local communities' concerns about resource strain and environmental degradation.[68]

More attempts are being made to increase the transparency of data centre resource use, especially around water and heat reusage. The EU recently introduced a bloc-wide scheme to rate the sustainability of data centres.[69] This sets out key sustainability-related performance indicators that data centre operators need to report on. Water resources will become increasingly contested when balancing the need to grow digital infrastructure with the need to ensure adequate water supplies for communities.

[66] Pieke FN, Hofman B, et al. LeidenAsiaCentre. Dealing with Decoupling: Business Strategies in a Changing World. February 2024. Available at: https://leidenasiacentre.nl/wp-content/uploads/2024/03/Dealing-with-Decoupling-Business-Strategies-in-a-Changing-World-3.pdf Leiden Asia Centre

[67] Franklin Templeton. India: Production Linked Incentives (PLI). Available at: https://www.franklintempleton.co.uk/campaigns/india-new-developments-to-drive-growth-and-earnings/india-production-linked-incentives

[68] Judge P. DatacenterDynamics. Re-zoning: Noisy, power-hungry data centers face criticism.July 22 2022. Available at: https://www.datacenterdynamics.com/en/opinions/re-zoning-noisy-power-hungry-data-centers-face-criticism/

[69] European Commission. Commission adopts EU-wide scheme for rating sustainability of data centres. March 15 2024. Available at: https://energy.ec.europa.eu/news/commission-adopts-eu-wide-scheme-rating-sustainability-data-centres-2024-03-15_en

Germany has led the charge on legislation around heat reuse requirements for data centre operators and businesses. Under the 2023 Energy Efficiency Act, all businesses—including data centres—with average annual energy consumption exceeding 2.5 GWh over the preceding three years are required to minimise waste heat as much as technically and economically feasible.[70] Wherever possible, data centres must also reuse the waste heat that they produce. The law introduces a specific energy reuse factor (ERF) requirement for new data centres: facilities commencing operations from July 1st 2026, must achieve a minimum ERF of 10%. This threshold increases to 15% for data centres starting from July 1st 2027, and 20% for those beginning operations after July 1st 2028. These targets must be met within two years of a facility becoming operational, based on average annual performance.

4. Building out national data centre capacity and critical-components production

Building national data centre capacity—including independent and sovereign cloud infrastructure—is essential for economic resilience, digital autonomy and national security. Businesses should diversify their hosting and cloud strategies to include trusted domestic providers, especially for workloads involving critical infrastructure, sensitive personal data or government contracts. The UK's initiative to designate data centres as Critical National Infrastructure reflects the importance of bolstering domestic capabilities.[71] By developing local expertise and infrastructure, businesses can ensure greater control over data and compliance with national regulations.

Governments play a crucial enabling role in catalysing national data centre operating environments, not only by supporting domestic cloud providers but also by investing in strategic industries that supply critical inputs to digital infrastructure, such as semiconductors, advanced cooling technologies and fibre-optic infrastructure. For example, Brazil currently produces only a small fraction of the semiconductors that it consumes. The relaunch of the CEITEC semiconductor plant in Porto Alegre (announced in 2023) is a promising first is a promising first step, although broader industrial policy is required.[72] Additionally, with traditional air-based systems reaching their limits owing to AI computing demands, domestic firms should be incentivised to develop liquid immersion cooling and direct-to-chip solutions. Government-backed research and development partnerships with technical universities and manufacturers could accelerate the availability of climate- and water-efficient cooling systems locally. Countries like Singapore have already begun to trial seawater- and liquid-cooled data centres to reduce dependence on potable water sources.[73]

5. Invest in a diversified portfolio of renewable energy sources on- and off-grid

To meet the growing energy demands of data centres sustainably, operators should invest

[70] Telyatnykov R, Burmeister T, Iffert PK. White & Case. Data center requirements under the new German Energy Efficiency Act. October 25 2023. Available at: https://www.whitecase.com/insight-alert/data-center-requirements-under-new-german-energy-efficiency-act
[71] UK Parliament. Designation of UK Data Infrastructure as Critical National Infrastructure—Written Statement HCWS89. September 12 2024. Available at: https://questions-statements.parliament.uk/written-statements/detail/2024-09-12/HCWS89
[72] Taiar E. Valor International. State-owned company promises chips for electric vehicles in two years. January 24 2025. Available at: https://valorinternational.globo.com/business/news/2025/01/24/state-owned-company-promises-chips-for-electric-vehicles-in-2-years.ghtml
[73] Li Ying L. The Straits Times. S'pore launches test bed for energy-efficient cooling for data centres in the tropics. November 29 2023. Available at: https://www.straitstimes.com/singapore/s-pore-launches-testbed-for-energy-efficient-cooling-for-data-centres-in-the-tropics

in a diverse mix of renewable energy sources, including solar, wind, nuclear power and battery storage solutions, both on- and off-grid. The recent power outages in Spain and Portugal have highlighted the need to ensure that mitigation measures are in place to counter energy-grid failure driven by climate and non-climate related factors. Both data centres and businesses must be prepared to ensure continuity of operations in the event of nationwide grid failures. Governments must also step in to mandate more robust energy redundancy plans that shift reliance away from the national grid, alongside deploying more diversified sources of renewable energy.

Data centre operators are integrating energy storage solutions, such as lithium-ion batteries, to reduce the risk of outages and provide power-supply reliability, in light of the intermittency of solar and wind energy sources. Nuclear power is emerging as a viable solution for data centres' growing energy demands and sustainability goals. In 2024 the industry advanced efforts to integrate nuclear energy generation, particularly through small modular reactors (SMRs). This shift is driven by the need for clean, reliable power sources to meet the sector's rapidly increasing energy consumption, which is expected to reach 1,000 TWh by 2026, more than doubling 2022 levels.[74]

Operators are also realising the appeal of nuclear power in its ability to provide stable, zero-carbon energy with high efficiency. SMRs offer sustainable and reliable power, crucial for data centre operations.[75] They are gaining traction owing to their scalability and potential for on-site deployment. They also offer energy generation from minimal fuel consumption, aligning with industry sustainability initiatives while meeting growing data-processing demands.[76] Key players in the sector are actively pursuing nuclear energy solutions for data centres. In October 2024 amazon announced partnerships with Dominion Energy and X-energy to develop 5 GW of nuclear energy for powering its data centres. Google is collaborating with Kairos Power to build up to seven SMRs, providing 500 MW of power, with the first unit expected online by 2030.[77]

6. Invest in quantum-proof/ quantum-safe technologies

Data centre operators and enterprises should begin the transition to post-quantum cryptography by assessing current cryptographic assets and implementing cryptographic agility—the ability to quickly swap out cryptographic algorithms without disrupting services.[78] Google has already begun testing post-quantum cryptographic algorithms such as Kyber, a lattice-based encryption system developed as part of a US National Institute of Standards and Technology project.[79] Similarly, AWS is piloting hybrid encryption schemes and offering quantum-resistant key exchanges through AWS Key Management Service and CloudHSM.[80]

Governments will continue to play a critical role in accelerating the safe transition towards

[74] JLL. Is nuclear a viable power solution for data centres? Available at: https://www.jll.com/en-us/guides/is-nuclear-a-viable-power-solution-for-data-centers
[75] Ibid.
[76] CyrusOne. The Future of Data Centers: Embracing Nuclear Power and Small Modular Reactors. October 18 2024. Available at: https://www.cyrusone.com/resources/blogs/embracing-nuclear-power-and-small-modular-reactors
[77] Chernicoff D, Vincent M. Data Center Frontier. How 2024, the year that re-energized nuclear power, foretells ongoing "new nuclear" developments for data centers in 2025. January 2 2025. Available at: https://www.datacenterfrontier.com/energy/article/55252205/how-2024-the-year-that-re-energized-nuclear-power-foretells-ongoing-new-nuclear-developments-for-data-centers-in-2025
[78] SecureW2. What is Cryptographic Agility and Why Does it Matter?. Available at: https://www.securew2.com/blog/cryptographic-agility-why-it-matters
[79] National Institute of Standards and Technology (NIST). NIST releases first 3 finalized post-quantum encryption standards. August 13 2024. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[80] Amazon Web Services. Post-Quantum Cryptography. Available at: https://aws.amazon.com/security/post-quantum-cryptography/

a quantum future. This includes developing national strategies for quantum preparedness, such as the US National Security Memorandum (NSM-10), which mandates federal agencies to migrate to quantum-resistant cryptography within a decade.[81] Brazil, although not yet at this regulatory maturity, has taken early steps through the launch of the EMBRAPII Quantum Competence Centre and FAPESP's Quantum Technologies Initiative (QuTIa), both of which are aimed at developing domestic expertise and applications in quantum science. This initiative provides a 42-month framework for businesses to engage in research and development activities related to quantum computing.[82] All but two of the 12 countries in this assessment have started implementing their national strategy for quantum preparedness, with South Africa and Indonesia publishing a strategy but falling short of implementation.

7. Build circularity

Integrating circular-economy principles into the design and operations of data centres can significantly reduce environmental impacts. Reusing waste heat for district heating or agricultural purposes, as demonstrated by a data centre in Finland partnering with a local fish farm, showcases innovative approaches to resource efficiency.[83] Water conservation is equally important. Cooling systems account for substantial water usage in data centres. Adopting water-efficient technologies and recycling systems can mitigate water stress, particularly in arid regions. Practices such as closed-loop cooling systems that use wastewater recycling or rainwater harvesting have the potential to reduce water use by between 50% and 70%.[84]

Policymakers should establish regulations that encourage or mandate the adoption of circular practices in data centres. This includes setting standards for energy and water efficiency, providing incentives for waste heat recovery projects, and supporting research into sustainable technologies. Successful implementation of heat-reuse regulations in northern Europe (Germany, Denmark and Finland) and water-use reporting across the EU provide successful models to harness further growth in data centres globally as demand for AI accelerates.

Of the 12 countries assessed in this programme, only Singapore currently has regulations mandating water reusage in data centres. As per the Public Utilities (Water Supply) Regulations, data centres (and other entities) that have an annual water consumption of at least 60,000 cubic metres must comply with the Mandatory Water Efficiency Management Practices of the Public Utilities Board (PUB), the water-sector regulator. These practices include: submitting records showing the volume of water supplied to the site in the previous year; submitting a Water Efficiency Management Plan to the PUB; installing private water meters in key water usage areas within the premises to monitor water use; and appointing at least one Water Efficiency Manager. This is part of the government's effort for data centres in Singapore to achieve a Water Usage Effectiveness of 2 cubic metres/MWh or less within the next ten years.[85]

[81] Russell J. HPCwire. NIST Issues Draft Post-Quantum Cryptography Transition Strategy and Timeline. November 14 2024. Available at: https://www.hpcwire.com/2024/11/14/nist-issues-draft-post-quantum-cryptography-transition-strategy-and-timeline/
[82] Potter J. Quantum Insider. 4 Countries That Began Funding Quantum Initiatives in 2022. April 20 2024. Available at: https://thequantuminsider.com/2023/05/16/4-countries-that-began-funding-quantum-initiatives-in-2022/
[83] Datacenters.com. From Byproduct to Resource: How Data Centers are Turning Waste Heat into Valuable Energy. September 19 2024. Available at: https://www.datacenters.com/news/from-byproduct-to-resource-how-data-centers-are-turning-waste-heat-into-valuable-energy datacenters.com
[84] Spindler W, Hahn-Petersen LA, Hosseini S. World Economic Forum. Why circular water solutions are key to sustainable data centres. November 7 2024. Available at: https://www.weforum.org/stories/2024/11/circular-water-solutions-sustainable-data-centres/
[85] Singapore Statutes Online. Public Utilities (Water Supply) Regulations (Rg 5). Updated April 2024. Available at: https://sso.agc.gov.sg/SL/PUA2001-RG5?DocDate=20240328&Timeline=On

Some views and opinions expressed in this report are those of the author and do not necessarily reflect the official policy or position of FM.

ECONOMIST IMPACT

LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com