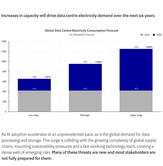
Foundations at risk: assessing the resilience of data centres and digital infrastructure

Modern businesses are critically dependent on data centres: the unseen yet crucial backbone of the global economy.

There are over 11,800 data centres worldwide, almost half of them in the US.

AI is driving an unprecedented surge for data centre capacity. Data centre capacity may grow by up to three times its current levels by 2035



Increases in capacity will drive data centre electricity demand over the next six years.

As AI adoption accelerates at an unprecedented pace, so is the global demand for data processing and storage. This surge is colliding with the growing complexity of global supply chains, mounting sustainability pressures and a fast-evolving digital stack, creating a dense web of emerging risks. **Many of these threats are new and most stakeholders are not fully prepared for them.**

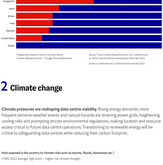
The underlying risks affecting data centres vary significantly. They can be categorised, affecting specific facilities through isolated events such as technical failures or localised disruptions, or systemic, where interconnected vulnerabilities lead to wider economic or infrastructure repercussions. Economist Impact identifies four systemic risks that particularly threaten the resilience of data centres and digital infrastructure:

1 Trade tensions and national security

Market concentration in digital infrastructure has created structural fragility. Over-reliance on a few dominant providers in critical functions creates structural fragility—where a single disruption, such as a US-China trade conflict, could impact global data centre operations, delay expansion and drive up costs.

Germany is most exposed to the risk of a trade war with the US, owing to its industry- and export-oriented economy. Meanwhile, trade between Australia and the US is limited, suggesting that the country will not experience the same direct shocks that other economies are facing from the US government's import tariffs.

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)

Cloudbusting
Share of cloud computing availability zones* controlled by largest Chinese or American cloud providers, October 2025, %

*Independent availability zones in cross-data centre.
**Tencent, Alibaba, Huawei, ByteDance, Baidu, JD.com, Kingsoft, Meituan

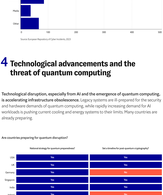
Source: Tinamo and Lehvoslai (Huawei) for Jacobin Institute for Strategic Research (Taiwan), October 2025

Source: Cybersecurity & Infrastructure Security Agency (2025)

2 Climate change

Climate pressures are reshaping data centre viability. Rising energy demands, more frequent extreme weather events and natural hazards are straining power grids, heightening cooling risks and promoting stricter environmental regulations, making location and natural access critical to future data centre operations. Transitioning to renewable energy will be critical to safeguarding data centres while reducing their carbon footprint.

How exposed is the country to climate risks such as storms, floods, hazardous etc.?
(1000-2022 average, high score = higher risk climate change)



Source: Germanwatch Global Risk Index (2022)

Source: Lawrence Berkeley National Laboratory (2024)

3 Political instability and hybrid conflict

Data centres are increasingly targeted in geopolitical conflicts; yet many stakeholders are unprepared for the escalating risks. As hybrid warfare intensifies, data centres face rising vulnerabilities—ranging from cyber attacks and service shutdowns to physical sabotage—making these strategic assets highly susceptible to global political instability and revealing a significant lack of preparedness across the sector.

Exposure to cyberattacks or cyberspionage
(weighted of attacks (0=none risk, 10=higher risk) + (0=no likely to enthusiast cyber attacks) + (0=no likely to enthusiast cyber attacks) + (no likely to enthusiast cyber attacks) + (no likely to enthusiast cyber attacks))
Proportional (0 = more likely to enthusiast cyber attacks, 4 = less likely to enthusiast cyber attacks)

Source: Economist Intelligence Unit (2025)

Critical infrastructure—including data centres—is a top target:

Number of worldwide political cyber attacks aimed at various sectors

Source: European Repository of Cyber Incidents, 2022

4 Technological advancements and the threat of quantum computing

Technological disruption, especially from AI and the emergence of quantum computing, is accelerating infrastructure obsolescence. Legacy systems are ill-prepared for the growth and hardware demands of quantum computing, while rapidly increasing demand for AI workloads is pushing current cooling and energy systems to their limits. Many countries are already preparing.

Are countries preparing for quantum disruption?

Source: Economist Impact (2025), official national sources (2025)

Why do these systemic risks matter?

These systemic risks act as catalysts that interact with and amplify a broader array of vulnerabilities in the data centre ecosystem. Their ripple effects cascade across technological, environmental and economic domains, compounding operational complexity and exposing fragilities.

Supply chains fragility and market concentration	Environmental and natural resource stress	Technological obsolescence	Regulatory and policy risks
Geographic concentration and particular dependency	Renewable energy demand	Cybersecurity threats	Data localisation
Resource constraints and workforce gaps	Water demand	Cooling innovation	Zoning and land use restrictions

A multifaceted risk landscape demands coordinated action

Geopolitical, environmental, technological and economic pressures are converging to challenge the resilience of digital infrastructure. While systemic risks are complex, targeted, coordinated interventions can strengthen data centre operations. The following recommendations offer a roadmap for data centre operators, businesses and policymakers to build more robust, sustainable and future-ready infrastructure.

So what can data centre operators, business users and governments do to boost resilience?

Geographic diversification is essential for digital resilience. To reduce co-dependency and operational vulnerability, operators must build distributed, cross-border infrastructure across varied climates and jurisdictions. Policymakers can support this shift by offering incentives for investment in underserved regions with stable grids and favourable environmental conditions, as seen in the Nordics. However, this comes with added data risks.

Diversifying digital infrastructure supply chains reduces systemic exposure. Businesses should adopt dual- and multi-sourcing strategies across low-risk jurisdictions and partner with alternative vendors for critical components. Governments must invest in domestic production of semiconductors and cooling technologies to reduce reliance on imports and support strategic autonomy.

Scenario planning and regulatory foresight are critical to future-proofing infrastructure. Proactively anticipating coming changes in environmental regulations and sustainability mandates enables data centre operators to avoid stranded assets and regulatory non-compliance. As policies on heat reuse, noise and water conservation tighten, organisations must use foresight tools to assess future risks and embed adaptability into infrastructure and investment decisions.

National capacity building enhances sovereignty and infrastructure security. Developing domestic cloud services and core infrastructure, including semiconductors and advanced cooling, is essential for national resilience. Government action—through industrial policy, R&D investment, and strategic designation of data centres as critical infrastructure—can help countries like Brazil and the UK to secure their digital sovereignty and reduce foreign dependence.

A diverse mix of renewable and resilient energy sources is vital. To meet surging demand while mitigating climate and grid-related outages and reducing carbon footprint, data centres must invest in solar, wind, nuclear and storage technologies both on and off grid. With initiatives such as Amazon and Google's investments in small modular reactors (SMRs), the sector is exploring pathways to more reliable power solutions. Governments must also reinforce energy-efficiency standards and grid independence planning.

Quantum-safe technologies must be adopted now to secure the future against emerging cybersecurity threats. Transitioning to post-quantum cryptography is imperative. Operators should build cryptographic agility and start piloting quantum-resistant algorithms. Governments must lead with national strategies, funding R&D and mandating secure standards—as seen in the US, and emerging efforts in Brazil—to ensure digital infrastructure remains secure in a quantum-enabled world.

Circular-economy principles must underpin sustainable data centre growth. Embedding heat reuse, water recycling and energy efficiency into data centre operations can significantly reduce environmental impact and operational inefficiencies. Policymakers can incentivise adoption through tax incentives and mandates. Models from Germany, Denmark and Singapore show how targeted legislation can drive innovation and sustainability as AI and digital demand continue to accelerate globally.

By adopting key strategies such as diversification, proactive planning, risk management, domestic capability development and circular design, stakeholders can strengthen the resilience and sustainability of digital infrastructure.

Acting quickly, collaboratively and decisively will help to address emerging threats and secure long-term performance and value in an increasingly dynamic global environment.

Sponsored by

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