

Data Centres: Building Resilience in India's Digital Infrastructure Boom

HOWDEN

How Growth, Risk and Insurability Are Converging

India's digital economy is expanding at an unprecedented pace. Cloud adoption, artificial intelligence, hyperscale computing and digital-first enterprises are driving significant investment in data centre infrastructure across the country. As capacity scales, so do the risks that threaten uptime, operational resilience and long-term insurability.

This edition explores the evolving data centre landscape, the risks that matter most, emerging global trends, and the insurance and risk management considerations that owners, operators and investors cannot afford to overlook.

India's Data Centre Growth Story

Data centres have become the backbone of India's digital economy. They host critical applications, support cloud services, power AI workloads and enable business continuity for organisations that increasingly rely on always-on digital infrastructure.



Industry projections indicate that India's installed data centre capacity could increase fivefold by 2030 to exceed 8GW. The majority of this capacity remains concentrated in Mumbai, Chennai, Delhi-NCR and Bengaluru, supported by strong connectivity infrastructure, undersea cable landing stations and favourable policy support.

The market is now entering a new phase, with operators, corporates and hyperscalers increasingly exploring opportunities beyond traditional hubs, including Tier-II cities.

This expansion positions India as a critical node in the global digital infrastructure ecosystem, but it also creates new operational, financial and insurance challenges.

Understanding the Modern Data Centre

A data centre is a physical facility that houses computing resources, storage infrastructure and networking equipment required to deliver applications, services and data. At its core, every data centre relies on three critical components:

Network Infrastructure

Connects servers, storage and digital services to ensure uninterrupted delivery of data.

Storage Infrastructure

Stores and safeguards the information that powers business applications and analytics.

Computing Resources

Provides the processing power, memory and local storage required to run workloads and applications.

Together, these systems form the foundation of every digital ecosystem.

Common data centre models include:

- Enterprise Data Centres
- Cloud Data Centres
- Colocation Facilities
- Managed Services Data Centres
- Edge Data Centres
- AI Data Centres designed for high-performance AI workloads and low-latency computing requirements.



Growth Brings Concentrated Risk

As India's data centre footprint expands, capacity is increasingly concentrated across a limited number of cities, utility networks and infrastructure corridors. This creates a growing accumulation risk.

Key concentration challenges include:

- Shared power grids and power dependency
- Common water infrastructure
- Flood and climate-related exposure
- Interconnected tenants and users
- Concentrated hyperscale demand

This means a single regional event can have implications across multiple facilities, customers and service providers. For operators, resilience is no longer just a technical objective. It is becoming a strategic requirement.



What Causes Most Data Centre Outages?

Despite advances in design and technology, the majority of outages continue to stem from a relatively small number of causes.

1. Power Failure and Electrical Instability

Grid outages, UPS failures, generator breakdowns and electrical disturbances remain among the leading causes of downtime. As demand for power rises globally, maintaining reliable power infrastructure is becoming increasingly challenging.

2. Cooling and HVAC Breakdown

Cooling systems are essential for maintaining stable operating conditions. Failure of chillers, CRAH or CRAC units can result in rapid temperature increases and operational shutdowns.

3. Fire and Smoke Events

Electrical faults, battery-related incidents and smoke contamination can create losses that extend well beyond physical damage to equipment.





4. Flooding and Water Ingress

Monsoon exposure, pipe failures, coastal risks and underfloor water ingress continue to be significant concerns for operators.

5. Cyber and Physical Security Risks

Operational technology systems, building management systems, insider threats and access control failures can all result in service disruption and operational downtime.

6. Human Error

Operational mistakes, maintenance failures and inadequate change management remain important contributors to major outages globally.

Emerging Challenges Facing the Industry

Beyond day-to-day operational risks, several macro-level challenges are shaping the future of data centre risk management.



Increasing Energy Demand

According to the International Energy Agency, electricity demand from data centres worldwide is expected to more than double by 2030, reaching approximately 945TWh. This places significant pressure on grid infrastructure and long-term energy availability.

Climate Risk

Heatwaves, severe storms, flooding and water scarcity are increasingly influencing site selection and operational planning. Rising temperatures also increase cooling requirements and operational costs.



Supply Chain Constraints

Rapid construction activity is creating challenges around equipment availability, specialised labour, inflation, permitting delays and geopolitical disruptions.



04

Fire and Battery Risks

The growing use of lithium-ion batteries has introduced new fire and thermal runaway exposures that require specialised mitigation measures.



05

Regulatory Scrutiny

Governments and regulators globally are placing greater emphasis on environmental impact, cybersecurity, energy use and resilience standards.

Why Insurers Are Looking More Closely

Data centres are highly interconnected assets where a relatively minor failure can create significant downstream losses.

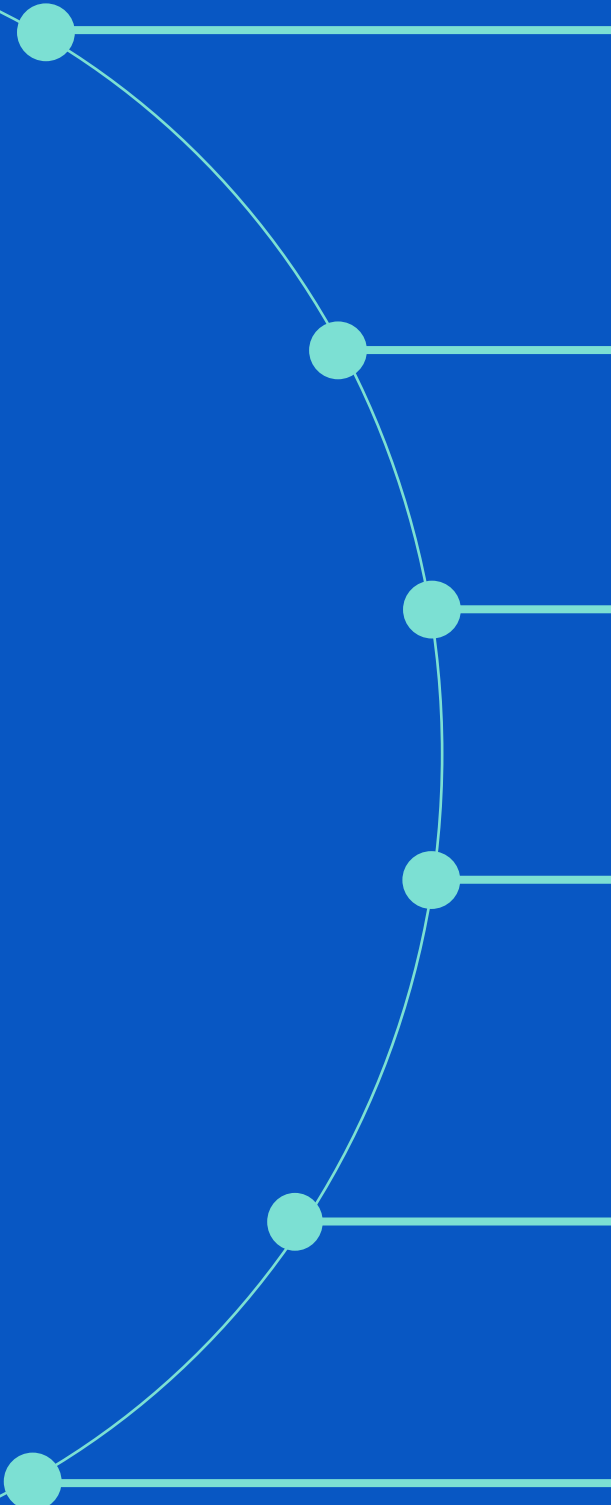
Insurers and underwriters are increasingly focusing on:

- Natural catastrophe exposure
- Power and cooling dependencies
- Regional accumulation risk
- Correlated loss potential
- Redundancy architecture
- Business interruption severity

A growing concern for insurers is that downtime-related losses can often exceed the cost of repairing physical assets. As a result, operational resilience and risk engineering have become central to underwriting discussions.

Building Resilience by Design

Resilience is no longer limited to infrastructure specifications. It requires a combination of technology, operational discipline and risk management. Key focus areas include:



Power Resilience

- Redundant utility feeds
- Backup generation
- UPS redundancy
- Regular failover testing

Cooling Reliability

- Redundant cooling architecture
- Continuous monitoring
- Preventive maintenance programmes

Fire Prevention and Detection

- Advanced smoke detection systems
- Clean-agent suppression technologies
- Thermal runaway mitigation measures

Water and Flood Management

- Flood protection planning
- Drainage systems
- Leak detection solutions
- Underfloor water monitoring

Operational Discipline

- Standard operating procedures
- Maintenance governance
- Robust change management protocols

Cyber and Physical Security

- Building management system protection
 - Access control
 - Continuous monitoring
-

Insurance Solutions for Data Centres

Given the complexity of data centre operations, a comprehensive insurance programme should consider multiple areas of exposure.

Construction and Engineering Covers

Protection during construction, expansion, commissioning and delay-in-start-up phases.

Operational data centre risk

Coverage for physical damage to buildings, IT equipment, electrical systems and supporting infrastructure.

Equipment Breakdown Insurance

Protection for transformers, switchgear, UPS systems, cooling equipment and other critical infrastructure.

Business Interruption Insurance

Coverage for revenue loss and additional expenses resulting from business disruption.

Cyber Insurance

Protection against ransomware, cyberattacks, incident response costs and operational disruption.

Liability Insurance

Coverage for third-party claims involving customers, contractors and visitors.

Global Trends to Watch

Recent developments across North America, Europe, Asia-Pacific and the Middle East highlight several themes shaping the future of digital infrastructure globally.

AI Is Driving Capacity Expansion

Governments, hyperscalers and private investors are committing billions of dollars towards AI-focused digital infrastructure, hyperscale campuses and computing facilities.



Energy Has Become a Strategic Priority

Organisations are exploring renewable energy agreements, dedicated power generation and alternative energy sources to support future demand.

Geopolitical Risks Are Increasing

Recent incidents involving drone attacks, military actions and infrastructure disruption have highlighted the growing exposure of critical digital assets to geopolitical events.

Sustainability Is Reshaping Development

Energy usage, environmental impact and resource consumption are influencing both regulation and investment decisions across several markets.



Looking Ahead

India's data centre sector is entering a period of accelerated growth supported by cloud adoption, AI-driven workloads and increasing digitalisation across industries. As capacity expands, operators will need to strengthen resilience, improve risk management and align insurance strategies with emerging exposures.

The data centres that will succeed in the future will not simply be the largest or most technologically advanced. They will be the facilities that are designed for resilience, operated with discipline and insured to reflect their true risk profile.

Resilient data centres are more than operational assets. They are critical infrastructure. As India's digital economy continues to scale, risk, resilience and insurability must scale alongside it.

Want to know more? Reach out to our experts



Burzin Umrigar

Head Construction & Renewable energy

burzin.umrigar@howdengroup.com



Suresh Ram Matcha

Head Operational Risk & Marine

SureshRam.Matcha@howdengroup.com



Rajesh Kumar Singh

Head - Property & Risk Management

rajesh.singh@howdengroup.com



<https://www.howdengroup.com/in-en>

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Howden.

Howden Insurance Brokers India Private Limited (Howden India) is an associate of the Howden Broking Group Limited, UK, the broking arm of the Hyperion Insurance Group. Howden Insurance Brokers India Private Limited is authorized and regulated by the Insurance Regulatory & Development Authority of India under License number 263. License Validity Period: 18/05/25 to 17/05/28, CIN: U67200MH2004PTC144558. Broker category: Composite. Registered in India with registered office at B Wing, 6th Floor, Supreme Business Park, Hiranandani Gardens, Powai, Mumbai – 400076