Addressing Service Outages

Mains: GS*III – Security*

Why in News?

The recent Microsoft 365's global outage (Nov. 12–13, 2026) highlighted gaps in India's outage-reporting framework and accountability of cloud service providers.

What are the Relevant Outage Regulatory Frameworks in India?

> *An **outage** is a period of time when a service, machine, or facility is temporarily shut down or unavailable.*

- **CERT-In Directions, 2022** – Mandates reporting of specified cybersecurity incidents within 6 hours.
  - Primarily covers cyberattacks, intrusions and security incidents.
  - Technical failures and non-malicious service outages are not explicitly covered.
  - CERT-In can seek information under Section 70B(6) of the IT Act, 2000.
- **RBI Outsourcing Directions** – Banks must assess risks associated with outsourced IT/cloud services.
  - Mandates vendor risk assessment, business continuity and exit strategies.
  - Banks remain accountable for outsourced services and may seek remedies from vendors contractually.
- **Digital Personal Data Protection (DPDP) Act, 2023** – Defines personal data breach to include loss of access to personal data.
  - Breach reporting obligations under the notified Rules are expected to become applicable from May 2027, as stated in the article.
  - Potential penalty for failure to comply with breach reporting – up to ₹200 crore.
  - Uncertainty remains over whether temporary service outages constitute reportable personal data breaches.

What are the Key Regulatory Gaps in India?

- **Limited reporting scope** – CERT-In reporting focuses on cybersecurity incidents, not outages caused by technical or infrastructure failures.
- **Absence of outage thresholds** – No uniform criteria based on outage duration, number of users affected or service criticality.

- **Ambiguity in data breach definition** – Temporary loss of access to personal data may or may not qualify as a reportable breach.
- **Indirect accountability** – Cloud providers are often accountable through contractual agreements rather than direct statutory outage-reporting obligations.
- **Fragmented regulation** – Different regulators oversee specific sectors, creating gaps in cross-sector digital infrastructure governance.

What are some International Outage Regulatory Practices?

Country/Region	Regulatory framework	Key provision
European Union	DORA	Direct oversight of critical ICT service providers to the financial sector
European Union	NIS2	Significant cloud outages trigger reporting obligations; initial notification within 24 hours and detailed reporting within 72 hours
United Kingdom	Financial-sector oversight	Critical technology providers placed under financial regulators' supervision
Singapore	Digital infrastructure legislation	Licensing of major data centres/cloud firms and reporting of service disruptions
South Korea	Data centre/platform regulation	Disaster management and resilience plans for major digital infrastructure

- **Global trend** – Moving from contractual accountability towards direct regulatory oversight, resilience requirements and mandatory outage reporting.

What are the Impacts of Service Outages?

- **Economic & operational impact** – Disrupts businesses, aviation, communication and digital workflows. Causes financial losses and productivity decline.
- **Digital dependency risks** – Concentration of services in a few cloud providers. Single points of failure in interconnected systems.
- **Consumer and trust impact** – Loss of access to essential services. Reduced trust in digital platforms and service providers.

What are the Options Available to Indian Customers?

- **Service Level Agreements (SLAs)** – Seek compensation, service credits or remedies where contractual uptime commitments are breached.
- **Business continuity arrangements** – Maintain backup communication channels and alternative systems.
- **Contractual remedies** – Invoke dispute resolution or other remedies available under service agreements.

- **Sectoral grievance mechanisms** – Approach relevant regulators where regulated services are affected.

What is the Way Forward?

- **Expand CERT-In reporting** – Include major service outages irrespective of whether they arise from cyberattacks or technical faults.
- **Introduce threshold-based reporting** – Define thresholds based on outage duration, user impact and service criticality.
- **Direct oversight of critical cloud providers** – Regulate providers supporting essential public and private digital infrastructure.
- **Strengthen resilience** – Mandate disaster recovery, redundancy, backup systems and periodic stress testing.
- **Clarify DPDP obligations** – Explicitly define when temporary loss of access to personal data constitutes a reportable breach.
- **Promote digital sovereignty** – Encourage diversification of cloud providers and development of domestic alternatives without compromising reliability or competition.

What lies ahead?

- As India advances towards a digital economy, cloud services and digital infrastructure are becoming essential utilities.
- Accountability cannot remain limited to contractual remedies or cybersecurity incidents.
- A transparent, threshold-based outage-reporting framework, stronger resilience standards and clear regulatory responsibility are essential to protect consumers, businesses and public institutions.

Reference

The Hindu| How does India address service outages?

SHANKAR IAS PARLIAMENT
Information is Empowering