Quote by Sameer Jain, Managing Director, Primus Partners

Published in Outlook Business
July 16, 2026| 08:04 PM IST

Kudankulam Nuclear Power Plant Data Breach Exposes Gaps, Risks In India's Critical Infra Security

Read on: [How Kudankulam Nuclear Power Plant Data Breach Exposes Gaps, Risks In India's Critical Infra Security – Outlook Business]

Article Content:

A reported data breach involving documents linked to the Kudankulam Nuclear Power Plant (KKNPP) has turned the spotlight on the cybersecurity risks surrounding India's critical infrastructure — not because hackers penetrated the nuclear facility itself, but because they allegedly accessed sensitive project information through one of its contractors.

Ransomware group World Leaks published nearly 19,000 files allegedly connected to India's largest nuclear power plant after claiming to have compromised systems belonging to Reliance Infrastructure, an engineering contractor involved in Units 3 and 4 of the Kudankulam project, as per a report by Reuters.

The documents reportedly included engineering drawings, supplier information, inspection records, meeting minutes and insurance documents.

According to the report, Reliance Group acknowledged a "partial breach" involving data hosted on a server managed by third-party data centre provider Yotta, saying the government had been informed. Yotta, meanwhile, stated that it detected suspicious activity on a Reliance-hosted server in May, blocked the suspected ransomware execution and later supported the ongoing investigation after external threat actors claimed to possess stolen data.

Govt Says Nuclear Safety Systems Not Affected

Following media reports, the Nuclear Power Corporation of India Limited (NPCIL) sought to reassure the public that no nuclear safety or security systems had been compromised.

In its official statement, NPCIL clarified that Reliance Infrastructure was awarded the Engineering, Procurement and Construction (EPC) contract in 2018 for the Common Services – Balance of Plant (BoP) package through a public tender.

The engineering drawings prepared by Reliance Infrastructure were based on indicative drawings and technical specifications supplied during the tendering process and were reviewed before acceptance, the government agency said.

However, while the government downplayed any operational risk to the plant, cybersecurity specialists say the incident highlights a much larger challenge — protecting the digital supply chains that support critical infrastructure.

Supply-Chain Attacks Replacing Direct Attacks

Experts said modern ransomware groups increasingly avoid attacking heavily protected facilities directly and instead compromise contractors, vendors and service providers with privileged access to sensitive information.

The attackers often view contractors as intelligence sources rather than secondary targets. A contractor's cloud infrastructure, though not directly impacting the plant, keeps information about engineering projects, building plans, software upgrades, and maintenance records, among others.

And this could be the best source of intelligence for the hackers.

"The modern cyberattack almost never starts from the direct breach of the most secure target. It goes through the process of establishing trust. Contractors can secure their presence in the critical infrastructure thanks to their dependence on cloud services, remote repair, or other digital processes. Once trust has been lost, the attackers know how to manage the system," said Ashish Kumar, Managing Director at OptiValue.

According to the latest State of Ransomware Report 2026 by Sophos, security gaps were the most cited reasons that exposed the organisations to attacks. This was followed by lack of people or skills (58%), and poor-quality protection at 57%.

The vendor-agnostic report surveyed 2,158 IT and security leaders across 17 nations, and said that malicious emails (26%) and phishing (24%) have become the top root causes of ransomware attacks, while exploited vulnerabilities fell to 18% as the cause of an attack.

Sameer Jain, Managing Director at Primus Partners, argued that the Kudankulam incident represents a shift from the malware incident of 2019 involving the plant's administrative network.

"Third-party vendor risk is now the single most volatile and complex cybersecurity challenge facing critical infrastructure globally. The traditional concept of a 'hardened perimeter' is dead," Jain said.

He said that while the reactor's Operational Technology (OT) remained air-gapped, storing engineering drawings on commercial cloud infrastructure effectively bypassed the physical security surrounding the plant.

"We can build a digital fortress around a nuclear reactor, but if the engineering firm building its secondary cooling loops stores the blueprints on an unencrypted, commercial cloud server, the fortress has already been bypassed," he added.

Contractors Are Weakest Link In Critical Infra

The Kudankulam episode illustrates how engineering contractors, cloud providers, equipment suppliers and maintenance vendors now form part of the security perimeter around national infrastructure.

Contractors may not have access to operational systems but often possess valuable engineering documents that can be exploited during future attacks, according to Rajesh Chhabra, General Manager, APAC, Large Markets at Acronis.

Experts call for continuous vendor monitoring, real-time threat intelligence sharing, Zero Trust access and secure virtual environments where contractors can work without downloading sensitive files.

"Protecting critical infrastructure now requires protecting the information itself rather than only the systems where it originates," said Mandar Patil, Executive VP at Cyble.

He recommended document-level encryption, strict access controls, data classification and continuous monitoring to reduce the impact even if files are stolen.

India's Legal Framework Still Leaves Gaps

Legal experts believe India has developed a robust cybersecurity framework for infrastructure operators but lacks a comprehensive statutory regime governing contractors and vendors.

"While India enforces a robust IT framework that stipulates multiple cybersecurity responsibilities for different stakeholders, a critical gap remains as this framework lacks a cohesive, defined mandate which prescribes the cybersecurity responsibilities of third-party contractors and vendors handling critical infrastructure," said Harsh Walia, Partner at Khaitan & Co.

Existing laws — including the Information Technology Act, CERT-In Directions and sector-specific regulations — remain largely operator-centric. Therefore, the law must evolve from protecting infrastructure operators to securing the entire digital supply chain that supports them.

India already has provisions covering Critical Information Infrastructure under Sections 70, 70A and 70B of the IT Act, alongside the CERT-In Directions of 2022. However, Arzu Chimni, Associate Partner at Obhan Mason, said that the framework remains focused on protected systems rather than the broader ecosystem of contractors handling sensitive engineering information.

According to Chimni, contractual indemnities may allocate financial liability, but operators and vendors cannot eliminate regulatory responsibility in matters involving critical infrastructure.

Who Is Accountable In A Data Breach?

The Kudankulam incident has ignited debate over where accountability should lie when sensitive infrastructure data is compromised through a third-party contractor. Legal experts broadly agree that responsibility should be shared, though in different ways.

While the IT Act places responsibility on every body corporate handling sensitive information, infrastructure operators also remain bound by CERT-In's six-hour breach reporting requirement, Khaitan's Walia said.

Kunal Sharma, Managing Partner at TARAksh Lawyers and Consultants, argued that infrastructure operators cannot outsource their statutory responsibility by delegating work to vendors.

"They remain responsible for vendor due diligence, access management, monitoring and incident response. At the same time, contractors entrusted with sensitive operational data should face independent statutory cybersecurity obligations if they fail to implement adequate safeguards or disclose breaches," Sharma said.

Global Practices Point Towards Continuous Oversight

Cybersecurity specialists say international best practices increasingly rely on Zero Trust architecture, least-privilege access, network segmentation and continuous monitoring instead of periodic audits.

Identity-first security, temporary access privileges, cloud security posture management and behavioural analytics can help prevent cyber attacks.

"Zero Trust, least privilege and network segmentation are essential controls to prevent attackers from moving laterally if one system is compromised," Chhabra said.

What India Must Do Next

Across experts, there is broad consensus that India's next phase of cyber reforms must extend beyond infrastructure operators to the wider contractor ecosystem.

Among the recurring recommendations were mandatory cybersecurity standards for vendors, continuous third-party audits, faster incident disclosure, stronger procurement rules, software supply-chain verification and statutory obligations for critical contractors.

"A resilient critical infrastructure ecosystem depends not merely on securing the operator, but on securing every participant in the digital supply chain," said TARAksh's Sharma.

Cybersecurity should no longer be viewed as an issue confined to infrastructure owners, he said.

Experts also stressed that organisations should classify vendors according to the sensitivity of information they handle rather than simply their contractual value.

Primus' Jain also advocated creating a national registry of strategic contractors handling critical infrastructure, with continuous security assessments before they participate in sensitive projects.

"If we do not secure the weakest links in our supply chain, we are essentially leaving the back door wide open while heavily reinforcing the front gate," he remarked.