INDIALAW

Cybersecurity and Incident Response

Cybersecurity and Incident Response Law Firm in India for CERT-In Compliance

PRACTICE PROFILE • MAY 2026

Overview

We assist clients in designing resilient cybersecurity frameworks and in responding swiftly to cyber incidents. Our expertise spans both legal and operational aspects of cybersecurity, from breach notification to regulatory engagement.

Our Services

- Incident response planning and breach management
- Legal advisory on cybersecurity regulations and frameworks (CERT-IN, IT Act, NIST, ISO 27K etc.)
- Support during ransomware and data theft attacks
- Forensic coordination and evidence preservation
- Crisis communication and liability mitigation
- Regulatory notifications and investigations
- Compliance audits and readiness assessments
- Cyber insurance and contractual liability analysis

Frequently Asked Questions

Q1 **What does a cybersecurity and incident response practice actually cover?**

It covers the legal and operational dimensions of protecting digital infrastructure. This includes designing cybersecurity frameworks, managing data breaches, coordinating forensic investigations, handling regulatory notifications under the IT Act and CERT-IN directions, and advising on liability exposure after an incident.

Q2 **When should a company engage a cybersecurity lawyer, and why now?**

Ideally, before an incident occurs. The 2022 CERT-IN directions mandate reporting of cyber incidents within six hours. Companies facing ransomware attacks, data theft, or regulatory scrutiny need immediate legal support. Post-breach, delays in response significantly increase regulatory and financial exposure.

Q3 **Which Indian laws and regulators govern cybersecurity compliance?**

The IT Act 2000, CERT-IN Directions 2022, and the DPDP Act 2023 form the primary framework. Sector-specific rules from RBI, SEBI, IRDAI, and TRAI add additional obligations. CERT-IN is the nodal agency for incident reporting and coordinates national cyber response.

Q4 **What does a typical incident response engagement look like in terms of process?**

It begins with containment and forensic preservation within the first few hours. Legal assessment of notification obligations follows immediately. We then coordinate with forensic vendors, draft regulatory filings, manage communications, and advise on downstream liability. Most acute responses span two to six weeks.

Q5 **What documents or information should a company have ready to start an engagement?**

We typically need the company's existing IT security policies, network architecture overview, incident logs or alerts, any prior CERT-IN correspondence, cyber insurance policy details, relevant vendor and data processing agreements, and a list of affected systems or datasets.

Q6 **What is the most common mistake companies make after a cybersecurity breach?**

Delaying or mishandling the initial response. Many organisations attempt internal fixes before preserving forensic evidence, which compromises investigations and regulatory filings. Others miss the six-hour CERT-IN reporting window, triggering separate compliance violations on top of the original breach.