There are five predominant laws to cover when it comes to cybersecurity:

Information Technology Act, 2000

The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.

But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act is the salient one, guiding the entire Indian legislation to govern cyber crimes rigorously:

**Section 43** - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

**Section 66** - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

**Section 66B** - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

**Section 66C** - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

**Section 66 D** - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000.

The primary relevant section of the IPC covers cyber frauds:

* **Forgery (Section 464) Forgery pre-planned for cheating (Section 468)**
* **False documentation (Section 465)**
* **Presenting a forged document as genuine (Section 471)**
* **Reputation damage (Section 469)**

Companies Act of 2013

**The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cements all the required techno-legal compliances, putting the less compliant companies in a legal fix.**

**The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even more proactive and stern in this regard.**

**The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cybersecurity obligations and responsibilities upon the company directors and leaders.**

NIST Compliance

**The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body.**

**NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness. It promotes the resilience and protection of critical infrastructure by:**

* **Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs.**
* **Determining the most important activities and critical operations - to focus on securing them .**
* **Demonstrates the trust-worthiness of organizations who secure critical assets**
* **Helps to prioritize investments to maximize the cybersecurity ROI .**
* **Addresses regulatory and contractual obligations .**
* **Supports the wider information security program.**

**By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST.**