THE ECONOMIC TIMES | tech

Companies grapple with costs, complexity of overlapping cybersecurity laws

By Himanshi Lohchab & Surabhi Agarwal, • Last Updated: Dec 31, 2024, 06:00:00 AM IST

Synopsis
India's digital economy faces increasing compliance burdens due to overlapping cybersecurity laws from various regulatory bodies. Companies are challenged with inconsistent requirements in breach reporting, audits, and vulnerability assessments. Experts call for harmonization under a single governance body to reduce complexity and costs, especially urging the Data Protection Board under the DPDP Act to take on this role.

ETtech

The compliance burden of overlapping cybersecurity laws, experts believe, is becoming increasingly onerous for companies as pertinent legal frameworks multiply to reflect the challenges facing India's galloping digital economy.

ET Year-end Special Reads
The mother of all Indian IPOs: Is it coming in 2025?
10 big events India witnessed in 2024
Thriller or mystery? How India's economy can unfold in 2025

Currently, there are six cybersecurity guidelines and frameworks with reporting requirements to six different governing bodies - SEBI, RBI, IRDAI, DoT, Cert-IN and the Cyber Regulations Appellate Tribunal.

The legal frameworks include the IT Act, the Indian SPDI Rules, and the National Cybersecurity Policy, along with other sectoral guidelines. The latest such mandate has come from SEBI.

Additionally, there are the overarching mandates under the Digital Personal Data Personal (DPDP) Act, with its Rules around the corner, which not only holds organisations accountable for data security but also could penalise them with hefty fines.

The inconsistencies in certification requirements, vulnerability assessments, controls, audit requirements and incident notification requirements have made it challenging for global companies to comprehend local and foreign laws, Jared Ragland, Senior Director – Policy, APAC, BSA - The Software Alliance told ET.

“Even worse, in many countries, including the United States, Australia and India, the rules aren't even entirely consistent within a single country, and our companies who are offering services across various sectors (power, telecom, finance) are dealing with unnecessary inconsistency.”

The West

He added that there are similar problems in nations like the US and Australia dealing with “a network of cybersecurity rules.”

“We have been talking about this issue, both to MeitY and to the National Cyber Security coordinator. I think that they kind of understand our challenges ... Where can we break down the barriers, reduce the unnecessary cost, because it doesn't do anybody any good,” he added.

“Currently, a patchwork exists pulling people in all directions but (there is) no strict enforcement, that's why we see plethora of data breaches, no relief for consumers, no nationwide cyber security policy for our data and infrastructure,” said Mishi Choudhary, founder of Software Freedom Law Centre.

“An omnibus legislation is supposed to be comprehensive to solve all issues related to the subject matter. However, for instance, the **DPDP act** doesn't consider health or financial data differently. That's why the need of all the institutions to have their own policies. Also, these policies predate the DPDP act that has still not come into force with its Rules,” she added.

While sectoral governance strengthens the ecosystem, the complexities have created compliance cost and confusion among organisations in areas such as breach reporting and audit requirements. Policy experts and lawyers are calling for harmonization of such requirements under one single governance body.

State focus

“Cybersecurity is clearly a prime focus of the government and hence we are seeing increased legal mandates coming from sectoral regulators as well, which is a positive outcome,” said Huzefa Tavawalla, Head - Disruptive Technologies Practice Group at Nishith Desai Associates.

“But this has created complexities on some counts. For instance, who do you report a data breach to and in what timeframe? Therefore, we need harmonisation of all applicable laws in breach reporting requirements,” he said.

He recommended that the **Data Protection** Board to be constituted under the DPDP Act could act as a single governing body for all data-related cyber incidents.

“India's cybersecurity regulatory landscape is indeed complex, with multiple overlapping laws, regulations, and guidelines,” said Kazim Rizvi, Founding Director of Delhi-based policy think group The Dialogue. “A few of these laws are entirely sectoral. It is primarily the IT Act that is sector-agnostic.”

He explained that **cybersecurity compliance** costs may not be a considerable barrier for larger companies but for new-age startups that struggle to keep up with day-to-day operation costs, overlapping laws may prove challenging.

“The legislation should be incentivized in a way that encourages ‘security-by-design’ approach. Additionally, a national cybersecurity strategy could serve as a blueprint for coordinated governance, fostering resilience against evolving cyber threats,” Rizvi said, calling for the need for a centralised cybersecurity regulatory authority which also supports the small and medium-sized businesses.