Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/20758
DOI URL: http://dx.doi.org/10.21474/IJAR01/20758

RESEARCH ARTICLE

CYBERSECURITY RISKS AND CORPORATE ACCOUNTABILITY IN INDIA: DIRECTOR RESPONSIBILITY, LEGAL REFORMS, AND THE ROLE OF REGULATORY BODIES IN DATA PROTECTION.

Rohit Kumar[1], Monika Rastogi[2] and Shilpa Sharma[3]

1. LLM student, School of Law Lingayas's Vidyapeeth(Deemed to be University), Faridabad Haryana.
2. HOD Law Department Lingayas's Vidyapeeth(Deemed to be University), Faridabad, Haryana
3. Assistant Professor, School of Law Lingayas'sVidyapeeth(Deemed to be University), Faridabad Haryana.

Manuscript Info

Manuscript History
Received: 15 Febuary 2025
Final Accepted: 18 March 2025
Published: April 2025

Abstract

Amid rising cyberattacks and frequent data breaches, India has enacted major legal reforms to strengthen data protection and enhance corporate responsibility. This paper explores the changing landscape of cybersecurity threats in India, with a focus on the duties of corporate directors, recent legislative changes, and the functions of regulatory agencies in upholding data privacy. By analyzing the Digital Personal Data Protection Act, 2023 (DPDP Act), and the formation of the Data Protection Board of India, the study outlines directors' legal obligations, the consequences of non-compliance, and the practical difficulties organizations face. The findings highlight the urgent need for stronger governance, comprehensive cybersecurity strategies, and more effective regulatory oversight to protect personal data in India's digital economy.

Introduction:-

India's rapid digital transformation has heightened exposure to cyber risks, making data security a top priority for organizations. The DPDP Act, 2023, marks a pivotal move towards more rigorous data protection, placing greater accountability on corporate directors to ensure compliance. The creation of the Data Protection Board of India underscores the government's commitment to robust enforcement of data privacy laws. This paper examines the evolving legal duties of directors, the impact of new reforms, and the critical role of regulators in advancing data protection and corporate accountability.

Objectives.

1. To examine the legal duties of corporate directors regarding cybersecurity risks in India.
2. To assess how effectively the DPDP Act, 2023, addresses cybersecurity challenges.
3. To evaluate the enforcement role of regulatory bodies, especially the Data Protection Board of India.
4. To identify compliance challenges for organizations and recommend improvements.

Corresponding Author:-Monika Rastogi
Address**:-**HOD Law Department Lingayas'sVidyapeeth(Deemed to be University), Faridabad, Haryana.

Review Of Literature.

Cyber security and corporate accountability have emerged as critical areas of concern in India's rapidly digitizing economy. The literature reviewed highlights the evolution of legal frameworks, the rising responsibilities of corporate directors, and the role of regulatory bodies in addressing cyber threats and safeguarding data.

Pavan Duggal's Cyber Law in India (2017) provides a foundational understanding of the Information Technology Act, 2000, and its amendments. It offers valuable insights into the statutory mechanisms used to combat cybercrime and places strong emphasis on corporate liability. Duggal argues that Indian businesses often underestimate the importance of legal compliance in cybersecurity, thus exposing directors to potential litigation and penalties.

Reema Saxena's Cyber Laws and IT Protection (2022) builds on this foundation by discussing recent amendments and practical challenges faced by Indian corporations. The book is particularly relevant for its coverage of how data fiduciaries—an important concept under the DPDP Act—must balance business interests with legal compliance, and how directors serve as the ultimate custodians of data security within a corporate structure.

Simran Singh and Vaishnavee Upreti's article, "Corporate Governance and Cyber Security" (International Journal of Law Management & Humanities, 2021), explores the symbiotic relationship between strong corporate governance and effective cybersecurity practices. The authors argue that cyber risk is no longer just a technological concern but a governance issue, requiring board-level oversight. Their work underscores the need for formal board policies and director education programs tailored to cyber resilience.

In a more recent publication, Singh's "Digital Transformation and Corporate Governance" (2024) extends this conversation by highlighting how emerging technologies increase risk exposure. The paper emphasizes that Indian directors must evolve from passive overseers to proactive risk managers, especially in light of evolving data protection regulations. The article also notes gaps in India's enforcement mechanisms and suggests a need for harmonization among regulatory agencies.

The review article, "Corporate Governance in India: A Systematic Review and Synthesis for Future Research" (Corporate Governance: The International Journal of Business in Society, 2020), offers a broader macro-level perspective on governance in India. Although not solely focused on cybersecurity, it identifies accountability and transparency as key pillars that can extend to digital governance. It calls for more empirical studies to understand how Indian directors respond to cyber threats.

The article "Framework and Challenges of Cyber Security in India: An Analytical Study" (International Journal of IT & Computer Engineering, 2022) provides a technical and regulatory overview of cybersecurity frameworks in India. The authors identify key issues, such as inadequate regulatory coordination, lack of preparedness among SMEs, and insufficient penalties, that hamper effective cyber risk management.

Research shows a growing consensus on the need for stringent cybersecurity in India. The Information Technology Act, 2000, was the initial step in addressing cybercrimes like hacking and identity theft, but its limitations led to the introduction of the DPDP Act, 2023, which offers broader data protection and harsher penalties for violations. Studies indicate that many directors lack sufficient awareness and training on cyber security, resulting in governance gaps and increased vulnerability to attacks. The Data Protection Board of India, established under the DPDP Act, is expected to play a central role in investigating breaches and ensuring accountability. However, overlapping regulations from multiple agencies continue to complicate compliance for businesses.

Synthesis And Research Gap.

The reviewed literature reveals a growing body of work supporting the idea that cyber security is a core component of modern corporate governance. While legal texts like those by Duggal and Saxena provide a statutory and regulatory perspective, journal articles by Singh et al. focus on practical implementation and the governance culture within Indian corporations.

A common theme is the lack of cohesive enforcement, exacerbated by overlapping jurisdictions (CERT-In, RBI, SEBI, etc.). This has resulted in regulatory fatigue for companies and confusion for directors. Despite the introduction of the DPDP Act, 2023, several authors note the need for capacity-building initiatives and clearer operational guidelines for the newly created Data Protection Board of India.

Methodology.

This research uses a qualitative, doctrinal approach, analyzing statutes, case law, and regulatory guidelines. Primary sources include the DPDP Act, 2023, the Information Technology Act, 2000, and official reports from CERT-In and the Data Protection Board. Secondary sources include peer-reviewed journals, legal commentaries, and industry whitepapers on India's cybersecurity and regulatory environment.

Results and Discussion

The Digital Personal Data Protection (DPDP) Act, 2023 represents a landmark shift in India's approach to data governance. It introduces several key protections, including the right of individuals (data principals) to provide informed consent, mandates for data fiduciaries to process data responsibly, and the imposition of substantial financial penalties for non-compliance. These measures signal a clear intent by lawmakers to prioritize the privacy and security of personal data in an increasingly digital economy.

However, despite these legislative advancements, the implementation of the Act faces considerable practical hurdles. One of the foremost challenges is the lack of clarity in the statutory language, which has led to varying interpretations of core terms and obligations. For example, definitions around "consent," "reasonable security safeguards," and "legitimate use" remain open to interpretation, complicating compliance efforts for organizations. These ambiguities can result in inconsistent application and enforcement, undermining the Act's efficacy.

Additionally, India's regulatory ecosystem currently lacks the capacity and coordination necessary to fully enforce the DPDP Act. The newly established Data Protection Board of India is envisioned as a centralized authority for adjudicating data breaches and ensuring compliance. However, at this early stage, questions persist about its independence, staffing, and technical capabilities. Without adequate resources and clearly defined procedures, the Board may struggle to effectively execute its mandate, especially in the face of rising cyber incidents and growing volumes of data processing.

The accountability of corporate directors has become a focal point under the new data protection regime. Legal provisions now increasingly hold directors personally liable for failures in data governance, particularly when companies are found to have acted negligently or failed to implement adequate safeguards. This evolution in legal accountability signifies a shift toward board-level responsibility for cybersecurity and data privacy, moving beyond traditional IT and compliance departments.

Case studies and industry reports suggest that enforcement activities have grown more robust in high-risk sectors such as banking, healthcare, and information technology. These industries handle vast volumes of sensitive personal data, making them prime targets for cyberattacks. Regulatory scrutiny in these sectors has also increased, resulting in tighter audits, mandatory breach disclosures, and higher compliance expectations.

Nevertheless, a persistent challenge is the existence of overlapping regulatory frameworks. Organizations operating in India must often comply with multiple and sometimes conflicting regulations from CERT-In, the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and now the Data Protection Board. This fragmented oversight has led to compliance fatigue, especially among small and medium enterprises (SMEs) that lack the legal and technical infrastructure to manage multiple regulatory requirements efficiently.

As a result, many businesses are caught between the imperative to comply with an evolving legal framework and the operational difficulties of doing so. This situation underscores the urgent need for harmonized regulations, clear compliance roadmaps, and targeted support for capacity building—especially for resource-constrained firms.

Conclusion.

India's cybersecurity landscape is at a pivotal moment of transformation, driven by the surge in digital adoption, increasing sophistication of cyber threats, and growing public awareness of privacy rights. The introduction of the Digital Personal Data Protection (DPDP) Act, 2023, and the establishment of the Data Protection Board of India mark significant strides toward building a robust data governance regime. These reforms reflect a deliberate shift from a reactive, fragmented approach to a more structured and proactive model that aligns with global best practices.

At the heart of this transformation is the increasing emphasis on corporate governance and director-level accountability. Under the new legal regime, corporate directors are not merely passive overseers but are expected to take active responsibility for cybersecurity oversight, risk mitigation strategies, and compliance with data protection norms. This reorientation of responsibility demands a cultural and operational shift within organizations—moving from viewing cybersecurity as an IT function to treating it as a board-level governance issue.

Despite the commendable progress on paper, enforcement and compliance mechanisms remain a work in progress. The implementation of the DPDP Act faces several challenges, including regulatory ambiguity, limited preparedness among stakeholders, and a lack of clarity on the procedural powers of the Data Protection Board. Furthermore, the coexistence of multiple regulatory bodies such as CERT-In, SEBI, RBI, and sectoral regulators has led to overlapping compliance mandates, creating regulatory fatigue and confusion, especially for small and medium-sized enterprises (SMEs).

To ensure long-term cybersecurity resilience, it is imperative that India adopts a unified and harmonized regulatory framework. This would involve establishing clearer roles among regulators, streamlining data breach reporting obligations, and developing sector-specific guidelines that are both rigorous and practical. The government must

also invest in strengthening the institutional capacity of enforcement bodies to ensure timely, fair, and technologically informed adjudication.

Moreover, corporate leadership must be educated and empowered to understand their evolving legal duties. Board members and senior management must be equipped with the knowledge to evaluate cybersecurity risks, allocate sufficient resources for data protection, and establish a culture of compliance across the enterprise.

Finally, sustained investment in cybersecurity infrastructure—both technological and human—is critical. This includes adopting advanced threat detection tools, building internal cybersecurity teams, and investing in training and awareness programs for employees at all levels. Public-private partnerships can also play a crucial role in advancing threat intelligence sharing and in developing national-level frameworks for incident response and cyber hygiene.

In summary, while India has taken bold steps toward modernizing its cybersecurity and data protection laws, real success will depend on holistic execution—combining legal clarity, strong governance, regulatory coherence, and industry readiness. Only through such a multi-pronged approach can India safeguard its digital ecosystem and foster trust in its growing digital economy.

References.

1. "Companies Grapple with Costs, Complexity of Overlapping Cybersecurity Laws."*The Economic Times*, 2024. https://economictimes.indiatimes.com/tech/technology/companies-grapple-with-costs-complexity-of-overlapping-cybersecurity-laws/articleshow/116807492.cms.
2. "Corporate Governance in India: A Systematic Review and Synthesis for Future Research."*Corporate Governance: The International Journal of Business in Society*, 2020.
3. "Cybersecurity Laws and Regulations Report 2025: India."*International Comparative Legal Guides (ICLG)*, 2025. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india.
4. Duggal, Pavan.*Cyber Law in India*. 4th ed., Universal Law Publishing, 2017.
5. "Data Protection Board of India."*Wikipedia*, 2024. https://en.wikipedia.org/wiki/Data_Protection_Board_of_India.
6. "Digital Personal Data Protection Act, 2023."*Wikipedia*, 2024. https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act,_2023.
7. "Framework and Challenges of Cyber Security in India: An Analytical Study."*International Journal of Information Technology & Computer Engineering*, vol. 2, no. 4, 2022, pp. 27–34.
8. "India's Data Protection Bill Threatens Global Cybersecurity."*Wired*, 2023. https://www.wired.com/story/opinion-indias-data-protection-bill-threatens-global-cybersecurity.
9. "Information Technology Act, 2000."*Wikipedia*, 2023. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000.
10. "Legal Challenges of Cybersecurity Risks."*CXO Today*, 2023. https://www.cxotoday.com/specials/legal-challenges-of-cybersecurity-risks.
11. Saxena, Reema.*Cyber Laws and IT Protection*. Kalpaz Publications, 2022.
12. Singh, Simran. "Digital Transformation and Corporate Governance: Shaping the Future of Business in the Technological Era." *International Journal of Law Management & Humanities*, vol. 7, no. 2, 2024, pp. 3005–3017.
13. Singh, Simran, and Upreti, Vaishnavee. "Corporate Governance and Cyber Security." *International Journal of Law Management & Humanities*, vol. 4, no. 4, 2021, pp. 2808–2821.