ROLE OF DIRECTORS IN CORPORATE CYBERSECURITY: A CRITICAL ANALYSIS

Apoorva Saxena, LLM, Chandigarh University

Dr Amrita Rathi, Associate Professor, UILS, Chandigarh University

ABSTRACT

The board of directors plays a pivotal role in governing corporate cybersecurity, especially in India's rapidly digitizing economy. Directors are expected to act with due diligence, integrating cyber risk management into overall governance. Indian corporate law and regulators have gradually recognized this need: the Companies Act, 2013 imposes a duty of care on directors[1] and SEBI's Listing Obligations mandate risk management systems. The Information Technology Act, 2000 (as amended) and CERT-In directives require organizations to report cyber incidents promptly, while the new Digital Personal Data Protection Act, 2023 compels data fiduciaries to implement strong safeguards.

This paper critically examines how these laws and guidelines impact directors' responsibilities. It surveys judicial trends (e.g. Shiv Kumar Jatia v. Delhi) stressing that directors are not automatically liable for corporate crimes absent evidence of personal wrongdoing and analyses enforcement patterns under the IT Act and data protection laws. Contemporary challenges – including directors limited technical expertise and fast-evolving cyber threats – are discussed, and best practices (board-level cyber committees, periodic audits, expert training) are recommended to strengthen corporate resilience. Throughout, an Indian legal perspective is foregrounded, with relevant case studies and comparative insights.

[1] Companies Act, 2013, §166(3) – duty of care of directors (see discussion: India Corp Law, Directors' Duty of Care under Section 166.

Introduction

In the wake of high-profile data breaches and ransomware attacks, corporate cybersecurity has become a board-room priority. Directors can no longer view cyber-risk as solely a technical issue; rather, cybersecurity is a strategic enterprise risk requiring board oversight. Globally, regulators have begun to hold boards accountable for cyber preparedness. In India, too, the legal framework is evolving: the Companies Act, 2013 implicitly encourages boards to manage all material risks (including cyber risks) as part of their fiduciary duty, while sectoral regulators (SEBI, RBI) and the Indian Computer Emergency Response Team (CERT-In) have issued guidelines on cyber governance and incident reporting.[2] The recent enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) further underscores the importance of data security in corporate governance.

Against this backdrop, this paper critically analyses the role of directors in corporate cybersecurity from an Indian legal perspective. We first survey the legal and regulatory framework: relevant provisions of the Companies Act, IT Act, data protection laws, SEBI rules, and CERT-In directions. Next, we examine directors' duties: how the general duties of care and due diligence under company law extend to cyber governance, and the extent to which directors must oversee internal controls, risk management, and incident response plans. We then review judicial interpretation and case law, noting that Indian courts have generally been cautious about imposing automatic liability on directors absent personal culpability.

This is illustrated by cases like Shiv Kumar Jatia v. State of Delhi, where the Supreme Court held that a managing director could be prosecuted for criminal negligence only if there was evidence of active involvement and intent.

The discussion proceeds to enforcement trends and liabilities. We analyze how regulators like CERT-In and future Data Protection Authority can sanction companies (and potentially their officers) for failures. Under the IT Act, non-compliance with CERT-In's 2022 directions[3] (e.g. 6-hour breach reporting) may lead to penalties up to one year imprisonment and fines. The DPDPA prescribes staggering fines (up to INR 2.5 billion for serious violations), meaning directors must ensure compliance to avoid corporate liability. Judicially, while direct

[2] The Companies Act, 2013 mandates that the board's annual report include the risk management policy, "which should also include cyber risks.

[3] CERT-In Directions (28 Apr 2022) under §70B IT Act – "Any service provider… body corporate… shall mandatorily report cyber incidents… within 6 hours".

precedents on cyber are rare, cases on directors' duties emphasize that liability depends on breach of specific obligations, not on the mere occurrence of a cyber-incident.

We then turn to contemporary challenges. Indian boards often lack cybersecurity expertise and directors must balance digital innovation against privacy and security concerns. The regulatory landscape is complex and evolving, posing compliance burdens. Finally, we propose best practices and recommendations: e.g. appointing cyber-savvy directors, establishing dedicated IT committees, conducting periodic cybersecurity audits, and aligning with international frameworks. Emphasis is placed on a proactive, board-driven security culture.

This comprehensive analysis is grounded in statutes (Companies Act 2013, IT Act 2000, DPDPA 2023), regulations (SEBI's Cybersecurity and Cyber Resilience Framework), CERT-In guidelines, and authoritative commentary. Footnotes reference relevant legal provisions and scholarly sources to support the discussion.

I. Legal and Regulatory Framework

India's approach to corporate cybersecurity governance is shaped by a mosaic of laws and regulatory directives. At the core is the Companies Act, 2013. While the Act does not explicitly mention "cybersecurity," it codifies directors' general duties, many of which bear on cyber-risk oversight. For instance, Section 166(3) of the Act imposes on every director the duty "to exercise his duties with due and reasonable care, skill and diligence".

In practice, this requires directors to ensure that the company has adequate internal controls and risk management – including for information security. The Act's Schedule IV (Code for Independent Directors) further highlights that boards should bring independent judgment on "strategy, performance, risk management, and resources" and that independent directors must ensure "financial controls and the systems of risk management are robust and defensible".

Thus, directors (especially independent ones) have a statutory obligation to scrutinize risk management processes, which logically extend to cyber risks.

Company law also mandates formal risk management structures. Rule 9 of the Companies (Meeting of Board and its Powers) Rules, 2014, requires certain classes of companies to constitute a Risk Management Committee. Corporate governance disclosures (under SEBI's LODR Regs) compel listed entities to report details of their risk management policy, which implicitly includes technological and cybersecurity risks.

In short, the Companies Act and related corporate governance rules expect boards to lay down procedures to inform directors about material risks, and to integrate cyber-risk into their assessment of business uncertainties. As one commentator notes, the Act mandates that a company's annual report include details of its risk management policy "which should also include cyber risks"

Beyond company law, India's Information Technology Act, 2000 (IT Act)[4] and its rules provide the cyber legal backbone. Under Section 70A, the IT Act empowers the National Critical Information Infrastructure Protection Centre (NCIIPC) to monitor "critical information infrastructure" (CII) (e.g. finance, telecom, energy).

Section 70B (6) authorizes CERT-In to issue binding directions for incident reporting and security practices. In April 2022, CERT-In issued detailed directions requiring "any service provider, intermediary, data centre, body corporate and Government organization" to report cyber security incidents listed in an Annexure to CERT-In within 6 hours of occurrence.[5]

Failure to comply with these directions can attract prosecution: under Section 70B (7), non-compliance with Section 70B (6) (the source of the directions) is punishable by imprisonment up to one year and a fine up to ₹100,000.

These provisions mean that the company and its officers could, in theory, be held liable for failing to report cyber incidents promptly. (In practice, enforcement by CERT-In has focused on improving readiness rather than punishing individual directors to date).

Sector-specific regulators also impose governance norms. SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF) (applying to stock brokers and depositories) oblige the board to adopt cyber policies. For example, SEBI's CSCRF requires boards to "approve the list of critical systems" and to sanction any exceptions to a software bill of materials with a proper rationale.

SEBI additionally requires boards to review periodic audit reports of cyber practices. Similarly, the RBI mandates that banks adhere to a comprehensive cyber security framework; all scheduled banks must appoint board-level IT and risk committees and implement the Reserve Bank's stringent cyber guidelines.

[4] Information Technology (Reasonable Security Practices, 2011) and Digital Personal Data Protection Act, 2023 – require data fiduciaries to implement "appropriate technological and organisational measures" for data security.
[5] Ashima Obhan & Associates, "Overview of CERT-In Cyber Security Directions, 2022" (Lexology, Aug 2022) – notes that failure to comply with §70B attracts up to 1 year imprisonment or fine Rs 100,000.

In the realm of data protection, India has enacted the Digital Personal Data Protection Act, 2023 (DPDPA).[6] Although not yet in force, it will become the principal law governing personal data. The DPDPA imposes duties on data fiduciaries (typically, the company handling personal data) to implement organizational and technical safeguards and to notify breaches to regulators and affected principals. Penalties for non-compliance under the DPDPA are severe – ranging from INR 50 crore to INR 250 crore (approximately €5–28 million) per breach.[7]

While the statute focuses on the corporate entity, its obligations create a strong incentive for boards to ensure compliance. The DPDPA thus adds another layer: directors must oversee data governance frameworks or risk catastrophic fines and enforcement action by the proposed Data Protection Board.

Cert-In's annual report (2023)[8] and government policy further reinforce these regimes. The National Cyber Security Policy (2013)[9] emphasizes capacity building and cyber-risk management, and NCIIPC issues guidance to strengthen sector resilience.

Courts have also noted the growing emphasis on cyber readiness as a board responsibility.

Together, this regulatory framework makes it clear that Indian companies are legally bound to treat cybersecurity as a governance issue. Directors must be aware of these laws – not only to avoid regulatory penalties, but as part of their statutory duties under company law to safeguard the company's interests.

II. Directors' Duties in Cybersecurity Governance

Directors' duties under Indian law are fiduciary and statutory, requiring them to act in the company's best interests, with due care, and in compliance with law. These duties have been interpreted to encompass oversight of major risks, including technological ones. The duty of care (Companies Act 2013, Section 166(3)) requires a director to exercise the care, skill, and diligence a reasonably prudent person would exercise in similar circumstances.

As information security issues can pose existential risks, boards must ensure that reasonable security standards are adopted. Indeed, jurisprudence in India and elsewhere holds that directors will be liable if they willfully ignore known risks.

[6] Digital Personal Data Protection Act, 2023.
[7] Latham & Watkins LLP, "India's Digital Personal Data Protection Act 2023 vs. the GDPR" – notes DPDPA fines range from INR 50,000,000 to 2,500,000,000
[8] Cert-In's annual report (2023).
[9] National Cyber Security Policy (2013).

Thus, it is generally recognized that directors should be informed about cyber-threats and demand regular reporting on the company's cybersecurity posture.

The fiduciary duty of good faith (Section 166(2)) and the broader duty to act in the company's best interests similarly mandate that directors consider stakeholders' interests. In the modern age, safeguarding data of customers, employees, and partners is part of the company's obligations. Directors who turn a blind eye to cyber-defense may breach these duties. The board must ensure ethical conduct in IT usage, reflecting Schedule IV's admonition to uphold integrity and not to allow extraneous considerations to vitiate objective judgment.

For example, if a breach could harm shareholders or reputation, directors must act, not merely defer to management.

Legally, directors also have a duty to ensure compliance with law. If cybersecurity laws (IT Act) or data protection requirements are flouted, directors may be held accountable under Section 134(3)(a) which requires the directors' report to state that the company has complied with all statutory requirements. In extreme cases, directors have been prosecuted for corporate offences under separate statutes (e.g. the Securities Board of India Act includes a vicarious liability provision for directors– indicating that wrongful acts by the company can sometimes extend to those in charge. Although directors cannot insulate themselves entirely from corporate liability, Indian law generally insists that some personal element of wrong (knowledge or negligence) be shown.

In practice, directors discharge these duties through governance structures. Boards are advised to establish an IT/cybersecurity committee or allocate oversight to the Audit/Risk Committee. Major companies are increasingly including cyber risks in their Enterprise Risk Management frameworks. Directors should ensure the company adopts recognized security standards (ISO/IEC 27001, COBIT etc.), and that senior management regularly reports on cyber incidents and remediation. Independent directors, in particular, are expected to bring outside expertise (including IT security) to board discussions. International experience shows many boards now even appoint a Chief Information Security Officer (CISO) who reports to the board.

Importantly, directors should integrate cybersecurity into strategic decision-making. For instance, any adoption of emerging technologies (AI, cloud computing) requires a board-level review of associated cyber risks. Contracts with vendors (outsourced IT services) need board scrutiny to ensure third-party risk management. The SEBI CSCRF mandates that the board

approve major cybersecurity policies and emergency plans, reflecting the growing expectation that directors set the tone for security culture.

Given these obligations, directors should actively educate themselves on cybersecurity matters. Regulators and professional bodies recommend periodic training. Boards must also ensure that company secretaries or compliance officers keep them apprised of developments (e.g. CERT-In advisories). A failure by directors to remain informed may violate their duty of care. Recent corporate governance guidance underlines that an "empowered board" can effectively manage cyber risks.

In sum, directors' duties in cybersecurity governance arise from general corporate law obligations to act prudently and in compliance with law. Cybersecurity should be treated as an integral part of the risk management policies that boards oversee. Failure to do so can expose directors to liability (civil or criminal) if their negligence contributes to a breach or non-compliance.

III. Judicial Interpretation and Case Law

Indian courts have not yet developed a rich body of case law specifically on cybersecurity and directors. However, general principles of corporate liability are instructive. The Supreme Court has repeatedly held that directors are not automatically vicariously liable for the company's offences absent statutory provision. In Sunil Bharti Mittal v. CBI,[10] the Court ruled that an individual director can be prosecuted for the company's crime only if there is evidence of his personal role and intent.

The later Shiv Kumar Jatia v. State of Delhi[11] reaffirmed this: the court quashed charges against a managing director because there was no allegation of his active negligence causing the harm.

Both cases underscore that, in India, directors cannot be held culpable merely by virtue of their position; there must be tangible fault.

This principle has important implications for cyber incidents. If a data breach occurs, courts would likely examine whether any director personally knew of, or willfully ignored, obvious security lapses. Absent such proof, courts would be hesitant to convict directors for the breach itself. For instance, if a director can show that reasonable security measures were in place and

[10] Sunil Bharati Mittal vs. CBI.

[11] Shiv Kumar Jatia v. State of Delhi (SC, 2019), (via Nishith Desai review) – affirmed that absent a statutory vicarious liability, a director is culpable only if there is evidence of his active role with criminal intent.

that the breach was due to unforeseeable malice, she may avoid liability. The burden on prosecutors is high: they must link the director's actions to the offence.

In the context of the IT Act, there is no reported case where directors were prosecuted under Section 43A (the erstwhile data-security liability provision) or Section 72A (privacy breach) for corporate failures. However, criminal penalties for disclosure of data without consent (Sec. 72A) can reach up to three years imprisonment.

Theoretically, a director who authorizes an unlawful data disclosure could be prosecuted. But again, courts would likely require proof that the director personally conspired or was negligent in breaching the contract. Section 72A's language is directed at the "service provider" performing the contract, which could include key managerial personnel. In practice, enforcement under Sec. 72A has focused on lower-level officers.

Aside from cyber-specific laws, directors can face liability under broader statutes if their corporate governance fails. For example, under the Prevention of Corruption Act or Competition Act, directors have been convicted for willful default.

Similarly, if a breach of cybersecurity leads to fraud or other offences (e.g. phishing-based theft), implicated directors could potentially be charged. However, courts have consistently required that mens rea be proved. This remains true for cyber: a mere breach, without evidence of director complicity or negligence, is unlikely to attract conviction.

In commercial litigation, shareholders or stakeholders might sue directors for negligence if a data breach causes financial loss. Though Indian law traditionally grants directors a degree of immunity under the "business judgment rule" egregious failures could lead to civil liability. A claim might allege a breach of Section 166(3) (duty of care). To succeed, plaintiffs would have to show that directors did not act on an informed basis or disregarded known cyber-risk. No reported Indian case has tested this scenario yet. By analogy, Tamil Nadu cases on directors' negligence (in other contexts) suggest courts will scrutinize board minutes, risk disclosures, and audit reports.

Finally, it is worth noting that Indian courts may increasingly consider international developments. For instance, U.S. and UK courts have begun to hold directors accountable for cyber governance failures. While Indian jurisprudence is not bound by these decisions, they may influence judicial thinking over time – especially where statutory duties are similar. In the short term, though, case law remains limited. To date, regulators and legislators have been the

main drivers of change, rather than the judiciary.

IV. Enforcement Trends and Liabilities

Regulatory enforcement in India is accelerating. The CERT-In directions of 2022 expanded enforcement authorities: now any person "in charge" of a body corporate could theoretically face penalties for non-compliance. Under Section 70B of the IT Act, CERT-In can call for reports and issue security directions; refusal or failure is a punishable offence. In practice, CERT-In's approach has been to issue advisories and press companies to self-report incidents rather than immediately penalize. However, the law now provides a stick: repeated non-reporting can attract prosecution (jail up to 1 year, fine up to ₹100,000). Directors should note that these provisions do not exempt them – a "body corporate" offence can implicate officers if they authorized the non-compliance. Thus, if a company fails to report a breach, both the company and responsible directors may theoretically be liable under 70B (7).

Sectoral regulators also signal stricter enforcement. SEBI's CSCRF requires cyber incidents at stock exchanges/brokers to be reported to SEBI within six hours, in addition to CERT-In. Non-reporting could invite action under the Securities Laws (loyalty of governance standards), although no public penalties have been announced yet. In banking, the RBI's Cyberfraud circulars mandate immediate reporting to the RBI for any cyberfraud; failure could lead to supervisory action against the bank's board and management. These trends indicate that in India, like elsewhere, the emphasis is shifting from ex-post fines to ex-ante prevention and swift disclosure.

The new Data Protection Act, 2023 will further tighten the noose. Although operational details are pending rules, the Act itself imposes personal liability on "data fiduciaries" for breaches of data subject rights. Directors, as the ultimate controllers of data fiduciaries, will need to ensure compliance with consent, purpose, and security requirements or risk the company facing fines from INR 5 crores up to 250 crores (₹50–250 billion).

In other jurisdictions (e.g. EU's GDPR), regulators have begun fining companies millions, and sometimes issuing notices to board members to explain failures. India's data protection board (once formed) may adopt a similar stance, requiring companies to demonstrate board-level governance of data.

Notably, Indian legislators have debated making directors individually accountable for data breaches. The Joint Parliamentary Committee on the 2019 Personal Data Protection Bill

recommended including independent and non-executive directors in liability provisions, but only if they were complicit or negligent.

The final DPDPA did not explicitly name directors, but the parliamentary concern highlights the policy direction: directors could not plead ignorance if laxity leads to breach.

Judicially, one enforcement case in 2022 involved an Indian company where a client's data was posted on its website without consent. The Madhya Pradesh High Court declined to quash First Information Report under the IT Act, implying that company directors could be interrogated.

This reflects that courts are willing to allow investigation of officers when personal information is mishandled. Although no high-profile director conviction has yet followed, the message is clear: data security lapses by the company can trigger law enforcement scrutiny of its leadership.

In civil proceedings, directors risk derivative suits by shareholders or customers. If a breach causes a quantifiable loss (loss of market value, legal claims, contract penalties), plaintiffs may sue directors for breach of fiduciary duty. Indian courts have recognized shareholder suits in cases of managerial misconduct. A cyber incident could become such a mismanagement case if it was due to gross oversight failure. Insurers have reported a rise in D&O (Directors & Officers) claims related to cyber events globally; Indian D&O policies may soon be tested similarly.

In short, enforcement is moving towards greater accountability. Regulators – especially CERT-In and sectoral watchdogs – now expect rapid reporting and robust security measures, backed by statutory penalties.

Liability for directors is not automatic, but it is not remote: a director who knowingly allows non-compliance, or who fails to act on repeated warnings, could face consequences under corporate or criminal law. The increasing regulatory focus on boards (SEBI's amendments, parliamentary reports) suggests that directors will be held to account not just within the company, but in law, if companies suffer avoidable cyber incidents.

V. Contemporary Challenges

Indian boards face several challenges in fulfilling these cybersecurity duties. First is the knowledge gap. Many directors (especially independent directors) come from non-technical backgrounds and may not fully understand cyber threats. Studies show a majority of board

members worldwide lack deep IT expertise.

In India, this gap can be larger given the traditional composition of boards. As a result, boards may rely heavily on management and external advisors for cyber updates. However, boards must push for plain-language briefings and independent verification of cyber readiness.

Second, the pace of technological change outstrips governance frameworks. Novel threats (AI-driven attacks, deepfakes, IoT hacks) emerge rapidly, and regulations lag. Directors must therefore stay informed through continuous education. For instance, even as the DPDPA was being passed, its enforcement rules were unsettled, leaving companies guessing about compliance details. Directors must balance waiting for clearer rules with the urgent need to improve security now.

Third, resource constraints are a concern. Implementing top-notch cybersecurity can be costly. Small and mid-sized companies (which make up the majority of India's corporate sector) may struggle to invest sufficiently in security infrastructure or hire CISOs. Directors of such companies must find cost-effective risk mitigations (e.g. outsourcing security monitoring to trusted vendors, leveraging government support initiatives) while ensuring not to under-budget this critical area. Stakeholders increasingly scrutinize cyber investment – as part of ESG (Environment, Social, Governance) – so boards have a reputational incentive to commit resources.

Fourth, the interplay of global and local laws creates complexity. Many Indian companies operate internationally or process data of foreign nationals, implicating regulations like GDPR. Directors must ensure dual compliance: for example, implementing consent mechanisms that meet GDPR and forthcoming Indian standards.

This duality complicates board oversight, requiring familiarity with multiple legal systems. Directors of multinational companies often rely on global policy frameworks, but must adapt them to India's context (e.g. local data localization requirements in CERT-In rules).

Fifth, there is a cultural and organizational challenge. Cybersecurity is often viewed as an IT problem, not a strategic one. Shifting this mindset requires the board to champion a security culture top-down. Directors must work with management to integrate cybersecurity into enterprise risk culture – for instance, including cyber objectives in executive KPIs. Resistance can come from executives focused on short-term goals. The board needs to articulate the

business case: ransomware losses, regulatory fines, and consumer trust all hinge on cybersecurity.

Lastly, enforcement inconsistency poses a challenge. As a relatively new emphasis, regulators' action patterns are still evolving. Directors may be unsure of what constitutes adequate compliance. For instance, CERT-In's list of "prescribed security incidents" is broad, and companies are adapting reporting systems to cover it all. Directors may find themselves in grey areas (what incidents qualify, how to interpret "due diligence"). This uncertainty requires boards to adopt the precautionary principle: if in doubt, report and prepare, as regulators have signaled a low tolerance for lapses.

In sum, Indian directors must navigate a rapidly evolving cyber landscape with limited precedent. They must educate themselves on technology, allocate resources judiciously, and instill a culture of security – all while satisfying ever-tightening laws. If unaddressed, these challenges can undermine the efficacy of corporate governance in the digital era.

VI. Best Practices and Recommendations

To meet their cybersecurity responsibilities, directors should adopt a proactive, structured approach. First, board composition should evolve. Companies should consider nominating at least one director with IT or cyber expertise (sometimes called a "Cybersecurity Director"). If not available, training existing directors is imperative. Leading governance guides advise regular cybersecurity workshops for board members. Given the Schedule IV mandate to bring independent judgment to risk matters, boards might appoint an external consultant or rotate director attendance at cyber conferences.

Second, boards should formally assign responsibility. An IT/Cyber Committee of the board can focus on technical security issues, reporting on readiness, incidents, and improvements. Alternatively, the Audit or Risk Committee's mandate should explicitly include cyber-risks. This ensures periodic review of cyber policies and breach response plans at the highest level. Companies should document these delegations in board charters to create clear accountability.

Third, implement rigorous risk management frameworks. This includes mandating annual cybersecurity risk assessments and penetration testing by independent auditors. The board should approve the scope and review findings. Regulatory frameworks like ISO/IEC 27001 or NIST CSF can guide these assessments. India's Companies (M&A) Rules 2014 explicitly require that electronic records are secure and that audit trails are maintained, so companies

should align internal controls accordingly. Directors must oversee implementation of these controls (e.g. encryption, access controls, log monitoring) and ensure compliance with (soon-to-be mandatory) data protection rules.

Fourth, establish a robust incident response and reporting protocol. Given the CERT-In directions, companies must have a plan to detect, escalate and report incidents within 6 hours. The board should review this incident response plan annually. Practice drills (tabletop exercises) are advisable to test readiness. Management should immediately inform the full board (or its cyber committee) of any breach, and the board should supervise communication with regulators, customers, and media. Transparent reporting builds trust and is likely to mitigate regulatory penalties.

Fifth, focus on stakeholder communication and governance. Boards should ensure cyber policies (e.g. data privacy statements, security policies for employees) are not just technical documents but reflect corporate values. Customer trust is a key asset; in the event of a breach, prompt public disclosure and remediation plans can reduce reputational damage. Some global best practices involve directors signing off on public cybersecurity disclosures. While not mandatory in India yet, companies may voluntarily include a cybersecurity governance section in the annual report, like financial risk disclosures – demonstrating board oversight.

Sixth, leverage external expertise. Directors should demand audits by CERT-In empaneled auditors (as now required under SEBI CSCRF) and hire cybersecurity specialists to advise the board. Indian industry bodies (NCIIPC, ISC^2 India Chapter) offer guidance and training. Networking with peers (e.g. director forums) can help share lessons learned. Also, engage external counsel to navigate compliance; for example, lawyers should brief the board on cybersecurity law updates (CERT-In advisories, DPDP Board guidelines).

Finally, directors should encourage a security-aware culture within the company. This means budgeting for continuous employee training (against phishing, social engineering), and incentivizing IT teams. The board should periodically review KPI metrics (e.g. mean time to detect/respond to incidents, patching cycle times). In essence, cybersecurity must be treated as an enterprise risk like any other: covered in board risk registers, subjected to audit, and managed at the strategic level. As one international board handbook puts it, boards must frame cybersecurity as a corporate governance issue, not just an operational one.

By following these practices, Indian boards can meet both legal expectations and stakeholder trust. Notably, proactive governance can also be a competitive advantage: companies that

demonstrate strong cyber oversight may find it easier to attract investment or win contracts with security-conscious clients. Ultimately, directors who embed robust cybersecurity into corporate strategy will better safeguard the company's assets and reputation in the digital age.

Conclusion

The role of directors in corporate cybersecurity is an emergent but critical dimension of governance. In India, legal developments – from company law to IT regulations and data protection – are converging to place cybersecurity squarely within the board's remit. Directors must therefore recognize cybersecurity as integral to their fiduciary duties of care and compliance.

While Indian courts have not yet spelled out a detailed test, existing cases affirm that directors can only be held liable for cyber-failures if there is evidence of active neglect or complicity.

Thus, the prudent approach for directors is to oversee and document a genuine cybersecurity program, so that if a breach occurs, they can show they took reasonable measures.

Enforcement is becoming more rigorous. CERT-In's binding directives on incident reporting and log-keeping are backed by criminal penalties, and the new data protection regime threatens heavy fines for compliance lapses.

India's regulators have signaled they expect accountability at the top: parliamentary committees and SEBI explicitly contemplate board responsibility for cyber incidents.

In the face of this, Indian boards cannot remain passive. They must build cyber-resilience proactively.

Contemporary challenges – knowledge gaps, evolving threats, resource limits – are significant but surmountable with leadership. Directors should follow global best practices adapted to India's context: ensure cyber expertise on the board, implement standard security frameworks, mandate regular audits, and foster a security culture. It is advisable to treat cyber-risk on par with other strategic risks in board deliberations. In doing so, directors not only protect their companies from attack and liability, but also fulfill their legal and ethical duties to stakeholders.

In conclusion, the "role of directors in corporate cybersecurity" in India is rapidly transitioning from implicit to explicit. Legal requirements and evolving norms now demand that boards oversee information security with the same rigor as financial controls. While the law is still catching up to technology, directors must act as if it already has: by exercising vigilant

oversight and integrating cybersecurity into corporate strategy, they will best serve the interests of their companies and the investing public.

References

1. Companies Act, 2013, §166(3) – duty of care of directors (see discussion: India Corp Law, Directors' Duty of Care under Section 166.

2. The Companies Act, 2013 mandates that the board's annual report include the risk management policy, "which should also include cyber risks".

3. SEBI, Cybersecurity and Cyber Resilience Framework (CSCRF) FAQs (2024) – e.g. "Board shall approve list of critical systems".

4. SEBI, Cybersecurity & Cyber Resilience Framework – e.g. "Board/Partners shall approve any deviation (e.g. SBOM absence) with rationale".

5. CERT-In Directions (28 Apr 2022) under §70B IT Act – "Any service provider… body corporate… shall mandatorily report cyber incidents… within 6 hours".

6. Ashima Obhan & Associates, "Overview of CERT-In Cyber Security Directions, 2022" (Lexology, Aug 2022) – notes that failure to comply with §70B attracts up to 1 year imprisonment or fine Rs 100,000.

7. Information Technology (Reasonable Security Practices, 2011) and Digital Personal Data Protection Act, 2023 – require data fiduciaries to implement "appropriate technological and organizational measures" for data security.

8. Companies (Management & Admin) Rules, 2014, Rule 27–28: require companies to keep electronic records secure and maintain audit trails.

9. IT Act 2000, §§70A–70B: establishes NCIIPC for critical infrastructure and mandates stringent security controls (enforced via §70B).

10. Latham & Watkins LLP, "India's Digital Personal Data Protection Act 2023 vs. the GDPR" – notes DPDPA fines range from INR 50,000,000 to 2,500,000,000.

11. Times of India, "Data breach: 'Make independent and non-exec directors liable'" (Sept 2021) – reports a parliamentary committee recommending that directors (incl. independents) be liable for data breaches if negligence proven.

12. Nishith Desai Assocs., "Data Security and Cybercrime in India" (Lexology, Feb 2022) – Section 72A IT Act (personal data disclosure) prescribes penalty up to 3 years jail and ₹500,000 fine.

13. Shiv Kumar Jatia v. State of Delhi (SC, 2019), (via Nishith Desai review) – affirmed that absent a statutory vicarious liability, a director is culpable only if there is evidence of his active role with criminal intent.

14. Companies Act, 2013, Schedule IV (Code for Independent Directors) – para II(1) states IDs shall exercise independent judgment on "risk management".

15. Schedule IV, para II (4): IDs must ensure "systems of risk management are robust and defensible".

16. Heidrick & Struggles, Board Monitor India 2024 (Feb 2025) – notes that Indian boards face "emerging technologies, cybersecurity concerns" and that SEBI is continuously updating LODR for stronger governance.

17. Afsharipour & Paranjpe, "Risk Management Oversight by Indian Boards" (National Law Sch. Ind. Rev. 2021) – observes Indian boards play a critical role in enterprise risk oversight (the regime now largely mirrors global standards).

18. Afsharipour & Paranjpe (2021) – notes that despite improvements, major Indian corporate crises (e.g. IL&FS) highlight ongoing challenges for directors in managing complex risks.

19. Cybersecurity Laws & Regulations 2025: India (ICLG) – notes that NCIIPC monitors national threats, and the National Cyber Security Policy, 2013 aims to protect information.

20. ICLG India (2025) – the RBI Cyber Security Framework mandates all banks adhere to strict cybersecurity guidelines (board oversight, risk assessment).