# CORPORATE ACCOUNTABILITY OF BOARD OF DIRECTORS IN CYBERSECURITY: AN ANALYSIS IN INDIAN LEGAL FRAMEWORK

Haribaskar B, School of Law, SASTRA Deemed-To-Be-University

**ABSTRACT**

While the India has transformed businesses digitally, the shift had raised concerns regarding corporate liability and cyber security. The Board of Directors of every company plays a crucial role in cyber governance. The Board have act with due diligence in cybersecurity in order to prevent cyber attacks. In India, the legal frameworks governing cybersecurity compliance and accountability of Board of Directors are: the Companies Act, 2013, the Digital Personal Data Protection Act, 2023 The Information Technology Act, 2000 and its subsequent amendments. These laws impose duties to the Corporate Companies to ensure protection of data, maintain adequate security measures, report the cyberattack incidents and data breaches.

This paper explores the evolving cyber threat landscape facing by corporate companies. It analyse the current legal provisions and judicial trends dealing with the duties and liabilities of directors in cyber risk management, mitigation after cyber threats and liabilities of the board for non-compliance. Based on the analysis and findings, it provides valuable recommendations to make such other regulations to the corporate actors to prevent data breaches, ensure accountability and secure the personal data from cyber attacks.

**Keywords:** Corporate liability; Board of Directors; Cybersecurity.

## BACKGROUND OF THE STUDY

The digitalisation of the business activities is increased the dependence of the corporate companies on information technology, digital transactions and personal data processing. But, the rise of the cyber threats has created financial, operational and reputational risks to the companies. Therefore, cybersecurity is the most significant aspects of the corporate governance and risk management in the board level.

The Board of Directors plays a vital role in oversight risks in the affairs of the company and ensuring sufficient internal controls. The Companies Act laid down one of the crucial duty to the directors: to act with due care and reasonable care and skill diligence. This duty was codified for concerns in financial governance in relation to corporate fraud, related-party transactions and protection of minority shareholders.

The IT Act, 2000 was enacted to give legal recognition to the electronic transactions and digital signatures, with obligations for protection of data and security. Section 43A of the aforesaid Act was included in the amendment due to raising fears in the data breaches relating to outsourcing in the IT and business process outsourcing sectors. A decades later, there was a raising concern to make a statute for data protection. The Supreme Court recognised the right to privacy as a fundamental right in the year of 2017, which led to constitution of the Justice B.N. Saikrishna Committee to draft a bill in the matter of protection of digital personal data, and the Digital Personal Data Protection Act is finally enacted in the year of 2023. It means the Indian legal system is younger in cybersecurity and data protection, and less in practice.

On the one hand, Companies Act impose duty of due diligence. But, on the other hand, laws enacted for the cybersecurity and data protection which are unclear and untested. In recent years, there are various cyber incidents affecting listed and unlisted companies, banks, insurers. This was led to enacting framework for Cybersecurity and cyber resilience by the SEBI, to interfere in the obligations of the Board of Directors beyond the requirement under the Companies Act. This research paper examines on determining the applicability of the duty of standard of care in cybersecurity, and analyse the liabilities of the company under the IT Act and DPDP Act and identify the gap between company and personal liability of individual directors.

## REVIEW OF LITERATURE

1. Goyal, in his paper, argued that the duties under Section 166(3) of the Companies Act requiring due and reasonable care, skill and diligence. It falls under the normative vagueness. It is not meaningless, but these obligations have to be construed by the Courts. The vagueness in the Section 166(2) and (3) tolerates the provisions of the Constitution, it does not fall under manifest arbitrariness. But it forces directors to make defensive decision which led to inconsistent outcomes among different categories of the directors.[1]

2. Wanchoo engages in the comparative analysis of Director's duty of care in UK and US Frameworks, she finds the inadequacy in the clarity of the concept. India is the only country which implements Business Judgement Rule indirectly. She argues that the UK and US are implement these codified duties through mechanisms like disclosure rules and business judgement rule. She recommends that it have to follow in India.[2]

3. The Mohnot and Merchant, in their work, engaged in the analysis to find that to whom the duty is owed to, and to analyse the standards of the duty. She seeks to apply four alternatives such as subjective standard, subjective-objective standard from agency law, duty of care under UK Companies Act, 2006 and business Judgement rule in US. They did not accept all these alternatives as these are unfit in Indian Context. It suggests to include reasonable man standard under tort law because it helps the court to inquire the actual state of mind to the directors.[3]

4. In this paper, Deepanshu and Ashok Kumar examines liability of the Corporate Companies under the DPDP Act by analysing its foundations, structure of the Act, and enforcement mechanisms. The DPDP Act's effectiveness depends on the regulatory clarity, independence of the institutions, integrating cybersecurity oversight in corporate governance structures.[4]

5. This paper gave a review of Cybersecurity framework in India, focused on the corporate and regulatory liability than personal liability. The analysis of this paper identifies various forms

[1] Section 166 And the Vagueness Problem: Director Duties, Article 14, And the Case for a Business Judgment Rule In India, Pawan Goyal, (SSRN), (2026)

[2] Directors' Duty of Care Under the Companies Act, 2013: A Critical Evaluation of Judicial Interpretation and Enforcement Mechanisms, Shreya Wanchoo (SSRN) (2026)

[3] Analyzing Directors' Duty of Care under the Companies Act, 2013, Rishabh Mohnot and Hrithik Merchant, India Corp Law (2023)

[4] Corporate Liability for Data Breaches under the Digital Personal Data Protection Act, 2023: Legal Challenges and Regulatory Responses" (Zenodo) (2026)

of corporate exposure than establishing liabilities of the individual directors. This paper builds that gap by examining legal duties of the companies for cybersecurity governance in the board level.[5]

## RESEARCH ISSUE

The pivotal legal issue of this paper are stated as follows:

1. Whether the duty of "due diligence" cast upon directors under Section 166 of the Companies Act, 2013 applicable for cybersecurity matters?

2. Whether the absence of the duty of the director allows the duties and penalties of the entity under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, leaving directors personally unaccountable for cyber governance failures?

## RESEARCH OBJECTIVES

- To examine the duties of Directors in the provisions of the Companies Act, 2013 in relation to the internal controls and risk management.
- To analyse the obligations and liabilities of the Companies imposed under the Information Technology Act, 2000, CERT-In Directions, 2022 and the Digital Personal Data Protection Act, 2023 and identify the personal accountability of the directors.
- To analyse the Judicial Trends on section 166(3) of the Companies Act, to know its applicability on the cybersecurity
- To identify the gap between accountability of single directors and companies for cyber governance failures.

## RESEARCH METHODOLOGY

This paper intends to use doctrinal research, which supports identify the particular law and applying the same. Both the primary and secondary sources are obtained and used in this paper.

[5] Cybersecurity Governance and Corporate Legal Responsibility in India, Kamasani Sudhakar Reddy & Dr. Nandini C.P. (IJRSI) (2026)

## INTRODUCTION

Nowadays, cybersecurity is a major concern in corporate companies in India, after they are relying on digital infrastructure. The digital transformation of the companies in India has increased the risks of various cyber threats such as ransomware attacks, data breaches, phishing and other cyber attacks. These issues are lead to damaging reputation of the company, regulatory action, financial loss and facing litigation against them.

In every corporation, the Board of Directors has the responsible to establish the appropriate governance structure for managing and supervising the company. It is the duty of the board to deal with risk management and ensure that its internal control systems are adequate to protect the company from certain cyber threats.

Section 166(3) of the Companies Act impose duties to the directors of the companies to exercise with due and reasonable care[6]. It is not clear that whether this duty is applicable in the matter of cybersecurity. However, this section does not explicitly refer the cybersecurity or managing the cyber risks.

The Information Technology Act, 2000 along with its rules and regulations provides various obligations to the corporate entities for data protection, reporting of cyber incidents and security practices. Companies may face penalties and other legal consequences if it fails to comply the provisions. The Digital Personal Data Protection Act, 2023 laid down duties to the companies for processing and protections of data and responsibilities for data fiduciaries. It further strengthens the accountability on the Board of Directors in cybersecurity and data protection.

The IT Act and DPDP Act impose duties and liabilities to the corporate entity, not individual directors of the company. it is unclear to determine the liability of the directors to held personally accountable for cybersecurity. It creates a significant legal gap between corporate liability and liability to the directors individually. This paper analyses the provision of section 166(3) of the Companies Act, 2013 to determine that whether it applies for cybersecurity. It also analyses the provisions of the IT Act, 2000 and DPDP Act, 2023 to determine the accountability gap between the company, board of directors and individual directors.

[6] The Companies Act, 2013

## EVOLVING CYBER THREATS IN INDIA

India is one of the developing digital economies, but this growth is lead to rise in cyber threats. According to CERT-In Annual Report in 2024, there are 20,41,360 cyber incidents were reported and handled by them.[7] Following are the various cyber threats facing by the corporations:

**Cyber attacks:** It is one of the malicious attempts to gain unauthorised access to the computer systems, networks, applications, or digital information. It was executed by the individuals, organised groups or other actors. These attacks may exploit the secret information, passwords, software vulnerabilities. The purpose of the attack is to steal data, obtain financial benefits, disrupt from function the system. It may affect the business infrastructure, operations, reputations. Some of the forms of the cyber attacks are hacking, denial-of-service attacks, malware attacks, and phishing.

**Ransomware:** Ransomware is a type of malware which is designed to stop the users or organisations from access their computer systems or files by encrypting their data. Then, the person who commits these kinds of acts demand the victim for payment of money to restore the access or providing the decrypting key. These attacks may disrupt the company operations by affecting company servers, databases, and applications. In such cases, the attackers are steal the sensitive information before they are encrypting the same. This is one of the most crucial cyber threats facing by the modern companies.

**Data Breaches:** Data Breaches is the access, theft, or disclosing confidential or sensitive information without any authorisation. It may occur through cyber attacks, insider threats, or misconfigured cloud storage. These data breaches will expose the financial details, passwords, business records. Such unauthorised use of data may lead to damage the company's reputation or financial loss, harming consumer trust. These data breaches will expose the financial details, passwords, business records.

## LEGAL FRAMEWORK IN INDIA

### The Companies Act, 2013: The Standard of Care Gap

[7] Indian Computer Emergency Response Team (CERT-In): Annual Report 2024. Ministry of Electronics & Information Technology (MeitY) Government of India.

Section 166 of the Companies Act, 2013 codifies the duties of the directors for the first time, which were previously recognised in the common law and equitable principles.

Section 166 (2) said that *"A director of a company shall act in good faith in order to promote the objects of the company for the benefit of its members as a whole, and in the best interests of the company, its employees, the shareholders, the community and for the protection of environment."*[8]

Section 166(3) of the Companies Act states that "*A director of a company shall exercise his duties with due and reasonable care, skill and diligence and shall exercise independent judgment.*" [9]

Section 166(7) provides that *"if a director of the company contravenes duties under this section, then he shall be punishable with fine from one lakh to five lakh rupees."*[10]

In addition, Section 134(5) requires to include Director's Responsibility Statement in the Board Report, contain that the directors had devised proper systems to ensure compliance with applicable laws and certain systems are sufficient and operating effectively.[11]

Section 166(3) applies to cyber oversight because it is written in general, but not enforceable in cybersecurity matters. None of the authority applying this duties, the standard of care is remain as unsettled. The duties of the Board of directors are currently arise through sectoral regulations.

This duty of reasonable care is an objective test not limited to director's ignorance or experience. However, when any director of the company holds particular skills or experience, then he was expected for a higher standard of care.[12]

It implies that every director must attend board and committee meetings; get advice of the experts when necessary; review financial statements and reports; participate actively in strategic decisions; monitor internal controls and risk management systems; and exercise his independent systems rather than accepting executive proposals without asking any question.

[8] The Companies Act, 2013
[9] The Companies Act, 2013
[10] The Companies Act, 2013
[11] The Companies Act, 2013
[12] Daniels v. Anderson (1995) 37 NSWLR 438

Therefore, directors have function as informed decision makers rather than acting in passive participants.[13] The risk management will include for cybersecurity.

The Supreme Court emphasized in the case of the ***Official Liquidator v. P.A. Tendolkar***, that directors cannot avoid their responsibility by claiming ignorance of company affairs or impose operational duties to subordinate officers. The court also held that the obligation of the directors shall be continue to exercise the supervision on the management of the company and cannot remain passive spectators in the event of mismanagement. This judgement reinforces the necessity in discharging director duties.[14]

In Mohnot and Merchant's analysis of Section 166(3) in the NUJS Law Review, it emphasised that there is no standard supplied in the due and reasonable care, skill and diligence. It was seeking the four alternatives such as subjective standard, subjective-objective standard from agency law, duty of care under UK Companies Act, 2006 and business Judgement rule in US. This article rejects all because these are all unfit for Indian context. It was recommended to include 'reasonable man' in Section 166(3), which is the legal standard in law of torts. The reasonable man standard means the conduct of the average person guides the court to decide that if someone was negligent.[15]

This duty creates vagueness in precise standard of care from directors. It had normative vagueness, which means where those valuable standards require content to be provided by the adjudicating person. The provision is not meaningless, but its content requires on the valuable judgements and contextual assumptions of the person.[16] It does not mention applicability of the duty especially in the matter of cybersecurity. But it could be interpreted by the court based on the facts and circumstances of the case.

In the case of Needle Industries (India) Ltd. v. Needle Industries Newey (India) Holdings Ltd. (1981), the court reveals the nature of the role of directors. Though, the Court is focused maximum on the duty of loyalty, but it was discussed about the duty of directors, it lacks judicial guidance to deal with claims under Section 166(3). It shows that lacking of

[13] Directors' Duty of Care Under the Companies Act, 2013: A Critical Evaluation of Judicial Interpretation and Enforcement Mechanisms, Shreya Wanchoo (SSRN) (2026)
[14] Official Liquidator v P.A. Tendolkar (1973) 1 SCC 602.
[15] Analyzing Directors' Duty of Care under the Companies Act, 2013, Rishabh Mohnot and Hrithik Merchant, India Corp Law (2023)
[16] Section 166 and the Vagueness Problem: Director Duties, Article 14, And The Case for a Business Judgment Rule in India, Pawan Goyal, (SSRN), (2026)

interpretation of courts in director's duty of care.[17]

The duty of standard of care has not such clarity that it is applicable in cybersecurity matters. Even though the courts are emphasising the directors to exercise the duties, it fails to interpret to which it applies. Scholars such as Mohnot & Merchant argues to import reasonable man in this provision. Even it was included, it is not possible to the Court to explain the application of the duty. Without the interpretation of the court, a person cannot determine that this duty applies for cybersecurity and other matters.

**The Information Technology Act, 2000: Duties and Penalties**

The Information Technology Act, 2000 is the important legislation in the cyber landscape. It is one of the legal frameworks governing electronic transactions, protection of digital data and prevent cyber threats prevailing in India. It grants legal recognition to electronic records and prescribes the civil & criminal liability for offences against the Act.

Section 43 of the Act imposes penalty and compensation for damage caused to computer systems and networks. It covers for unauthorised access, copying, or downloading any data, and damage or disruption to computer resources. Companies are also held to be liable for violations under this section.[18]

Section 43A impose obligation to the body corporate which handling *"sensitive personal data and information"* via computer resources to implement *"reasonable security practices and obligations"*. If the company fails to comply and leads to cause any wrongful loss and damage, then these entity will be held liable to pay compensatory damages.[19]

The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, was made under Section 43A of the IT Act. It requires body corporates to collect, store, or process sensitive personal data to maintain any information security programs which are documented and to strengthen security controls.

Section 66 of the Act states that when any person commits acts under section 43 in dishonest or fraudulent manner, he is punishable for imprisonment upto 3 years, a fine upto 5 lakh rupees

[17] Needle Industries (India) Ltd. v. Needle Industries Newey (India) Holdings Ltd. (1981) 3 SCC 333
[18] The Information Technology Act, 2000, No. 21 of 2000 (India) S.43
[19] The Information Technology Act, 2000 S.43A

or both. This section converts those acts from civil wrong to the criminal offence, because of the malicious intention.[20]

Section 70B(6) of the Act provide authority to the CERT-In to issue directions including to the Companies for security practices and reporting any incidents.[21]

The Indian Computer Emergency Response Team (CERT-In) had issued directions in April 2022 requiring the "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." [22]

Under Section 70B(7), non- compliance of these directions will be lead to punishable for up to one year imprisonment and one lakh fine.[23]

Section 72 penalises for unauthorised disclosure or access to, "sensitive, personal or confidential information", without the consent of the person by exercising the powers of the Act. Such person shall be punishable with imprisonment up to 2 years or fine upto 1 lakh or both.[24]

Section 72A imposes punishment for intentionally or unknowingly disclosing any personal information of such person, acquired for rendering services under a lawful contract, without the consent of the concerned person or in breach of a lawful contract. It is applied when such person commit act with the intention to cause wrongful loss or damage.[25]

Section 85 imposes liability to the company for the offence committed under this Act. The Company as well as the person responsible for its conduct will be held liable for the same unless if it is committed without his knowledge or exercising due diligence.[26]

**The Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act (DPDP), 2023 is a latest framework in India for

[20] The Information Technology Act, 2000 S.66
[21] The Information Technology Act, 2000 S.70B(6)
[22] Indian Computer Emergency Response Team. (2022). CERT-In Directions for Cyber Incident Reporting.
[23] The Information Technology Act, 2000 S. 70B(7)
[24] The Information Technology Act, 2000 S. 72
[25] The Information Technology Act, 2000 S. 72A
[26] The Information Technology Act, 2000 S. 85

protection of personal data and privacy. Although not in force, it regulates the collecting, processing, storing and sharing of personal data. It was enacted to recognise the right to individuals to protect their data and need to process such for lawful purposes.

It was defined data fiduciary which means, "any person or in conjunction with any other persons determines the purpose and means of processing of personal data."[27]

***Obligations of the data fiduciaries:*** The Act imposes obligations on the Data Fiduciaries as are mentioned in the following:

- It should Obtain free, informed, valid and specific consent form the data principal.
- It shall ensure that data shall not used unless if it is for lawful purposes
- It is the duty to Implement technical and organisational safeguards
- In the event of personal data breaches, it must be informed to Data Protection Board and affected individuals.
- It shall take certain measures to maintain the confidentiality and accuracy of personal data.[28]

The Data Fiduciary may be designated as Significant Data Fiduciary as notify by the Central Government. It has imposed their duties such as appointing data protection officer, conducting data audits and protection of data impact assessments in every period.[29]

The Act imposes penalties for non-compliance of its provisions. The maximum penalties ranging up to 250 crores for data breaches.[30]

**Sector-Specific Regulations**

***SEBI LODR Regulations (Listed Companies):*** Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations states that Top 1000 listed companies shall

[27] The Digital Personal Data Protection Act, 2023, Act No: 22 of 2023 (India) s.2(i) (definition of "data fiduciary")
[28] The Digital Personal Data Protection Act, 2023, s. 8
[29] The Digital Personal Data Protection Act, 2023 s. 10
[30] The Digital Personal Data Protection Act, 2023 s. 33(1) read with Schedule

constitute Risk Management Committee, which expressly includes cyber security risk. It is one of the clearest duty of the board for cybersecurity. But the breach is enforced only by the SEBI, not through the duty of due diligence under section 166.

***SEBI Cybersecurity and Cyber Resilience Framework (CSCRF), 2024:*** It was introduced by the SEBI to unify and upgrade digital safety standards across all entities under this framework. It is not applicable to listed companies generally. It applies to SEBI regulated entities (such as stock brokers, depositories, depository participants and mutual funds).

The duties of the directors in cyber oversight is applicable to the regulated and listed entities, but not unlisted companies. The sectoral regulations impose consequences on its regulated entities and its senior management through the regulator's powers, which reinforces rather than closing the gap for personal accountability.

**Analysis on Entity- Director Accountability**

The duty and liability under IT Act and DPDP Act is enforced to the companies or data fiduciaries, but not directors.

Section 43A of the IT Act, 2000 explicitly imposes liabilities upon body corporate, which means, "any company and includes a firm, sole proprietorship or her association of individuals engaged in commercial or professional activities."[31] Certain statutes, including section 85, expressly mention that "a person in charge of business" will be held liable for such violations. But, this section does not impose liability to such individual persons.

Section 85 specifies that not only the company, but also the directors or other officers, will be held liable if the offence is occurred with their consent, connivance or neglect. Section 43A mentions liability for civil damages, and Section 85 is about offence for companies. Section 85 cannot apply for civil damages in section 43A.

While directors, CEOs, and Managing Directors are not liable for every violation, and certain statutes are imposing vicarious liability for officers in default. The DPDP Act imposing primary obligations and liabilities upon Data Fiduciaries, but not providing vicarious liability.[32]

[31] The Information Technology Act, 2000 s. 43A Explanation (i) body corporate
[32] DPDP Act 2023: Director Liability and Board Responsibilities for Data Privacy Compliance, Dhruv Kaushal

Section 43A of the IT Act provides duty protection and liability to the body corporate, not any individual members of the company. The DPDP Act provides penalties for non-compliance of the security safeguards or data breaches. But, Section 44 of the DPDP Act explicitly omits the Section 43A of the IT Act.[33] If the 2023 Act is implemented, then the former will not in force. Then, the liability of the body corporate will be converted as liability of the Data Fiduciary i.e., not only companies but also such persons engaged in processing data. But it does not explicitly mention the individual directors.

The liability of the directors does not leave the director personally unaccountable, because section 85 of the IT Act provides liability to the members of the company for their neglect, but it is not tested in section 43A and strongest against executive directors. In DPDP Act, the statute provides no basis for holding an individual director to account, and the omission of Section 43A of the IT Act, will remove only the existing statutory route for personal data safeguard failures.

## SUGGESTIONS

- The Ministry of Corporate Affairs may codify the rules, prescribing minimum cybersecurity practices follow by the Board of Directors. For example, a requirement that every company, while making a board report, contains statement that the Board has reviewed the adequate cybersecurity risk management systems.

- It is not clear that which officers will be liable for breach of data fiduciary under the DPDP Act, 2023. It is necessary to include that officer in default will be held liable for the breach of the Data Fiduciary.

- SEBI's LODR Regulations, and the Cybersecurity and Cyber Resilience Framework (CSCRF) reveals its disclosure and governance model for listed companies. This model needs to extend to unlisted public companies and significant data fiduciaries under the DPDP Act. This change will make board oversight practices as visible and comparable beyond the listed company.

and Aniket Ghosh, Chambers (2026)

[33] The Digital Personal Data Protection Act, 2023 S. 44 2(a)

## CONCLUSION

The digital transformation of the Companies in India leads cybersecurity from technical concern to corporate governance issues. The cyber threats of the companies expose companies to financial loss, damage to its reputation, regulatory action and facing litigation. The Board of Director has the duty to supervise the affairs of the company, risk management, internal controls.

Section 166(3) of the Companies Act imposes director's duty as "duty and reasonable care, skill and diligence". But it was suffering normative vagueness. There was a confusion to determine to which it applies, including cybersecurity. While the courts make it clear that directors shall not plead ignorance, or remain as a passive spectator, it fails to interpret the provision.

Section 43A of the IT Act provides duties and liabilities of the body corporate, whereas the DPDP Act imposes liability upon the data fiduciary. Both the provisions are fails to mention the liability of the particular person in the body corporate and data fiduciary. While Section 85 of the IT Act imposes liability to the companies as well as the officers in default, the section 43A does not state the personal accountability of the directors. It is uncertain to apply section 85(offences by companies) in section 43A (civil damages).

The legislation made by India on Cybersecurity and data protection is remain young. The corporate laws fails to make provision to the directors in the matter of cybersecurity. It is necessary to make legislative reform and provide judicial guidance on Section 166(3) of the Companies Act. The legislature has also provide clarity that whether the liability of the company would also include the personal liability of the directors.