INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FROM IT RISK TO FIDUCIARY RISK: BOARD-LEVEL CYBERSECURITY OVERSIGHT AND DIRECTORS' LIABILITY UNDER INDIAN CORPORATE LAW

AUTHORED BY - S K S K VAISHNAVI

ABSTRACT

As companies become more reliant on digital infrastructure, cybersecurity is as much a corporate governance issue as it is a technical one. Financial stability, shareholder confidence, business continuity and regulatory compliance can be affected by cyberattacks, ransomware, data breaches and unauthorized access to corporate information. Cybersecurity is often thought of as the domain of the information technology departments, but the fallout from bad cybersecurity is often the domain of the board of directors. That begs the important question of the extent to which directors can be held liable for failures in corporate cyber security governance.

This Paper investigates the connections between cybersecurity oversight and the fiduciary duties of directors as contained in the Companies Act, 2013 and the requisite standards of care, skill, diligence and independent judgment in Section 166 of the Act. It further discusses the application of Sections 134, 149 and 177, the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, the Information Technology Act, 2000, the CERT-In Directions, 2022, and the Digital Personal Data Protection Act, 2023. The paper finds that while there is no specific presumption of a statutory duty of cybersecurity oversight under Indian corporate law, the various fiduciary and managerial responsibilities will extend reasonably to the identification, supervision and management of material cyber risks.

The dissertation employs a doctrinal and analytical methodology, and argues for a proportionate board-level cybersecurity accountability framework. It finds that board-level responsibility for cybersecurity should be viewed as an aspect of good corporate governance, and that personal liability should only arise in cases of proved, rather than presumed, neglect of oversight.

Keywords: Corporate Governance, Cybersecurity, Directors' Duties, Fiduciary Liability, Companies Act, 2013, SEBI, Data Protection, Board Accountability.

ISSN: 2582-6433

1. INTRODUCTION

Modern corporations are increasingly relying on digital devices. Businesses employ integrated information management systems for financial transactions, employee management, customer management, business operations, intellectual asset management, as well as aid in strategic decision making. As such, digital infrastructure has grown to be an integral part of business operations as opposed to a mere administrative facility.

It also leaves companies open to cybersecurity threats. Ransomware attacks, hack attacks, unauthorized access, theft of data, digital infrastructure downtime and breach of corporate confidential information can all be highly damaging in terms of cost and reputation. A cyber incident could affect how a business runs, and reveal personal data or cause regulators and investors to question it.

Until recently cybersecurity was considered a more specialized function within an organization's IT department, which was then handed over to the operational or technical staff to manage, as they would have acquired skills in their particular areas of expertise. Sadly, this "IT thing" completely misses the point; a breach is in fact much wider reaching. A significant breach can affect a company's profitability, its contractual and legal duties and ultimately its future sustainability.

The Companies Act, 2013[1] creates the legislative basis for the duties and responsibilities of directors; in particular:

1. The minimum standards of performance, skill and judgement and good-faith conduct are set out in section166[2]; and
2. The theme of "risk management" (and "internal financial controls") is explicitly invoked at section 134. Neither of these provisions explicitly mentions "cybersecurity", but their relevance in this context is clear.

This issue becomes more relevant in the case of listed companies. The SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 regulates matters relating to corporate governance, disclosure of material events and risk management. Any incident related to cybersecurity could result in an impact on the market and investors and this is relevant from the disclosure/ governance perspective.

Likewise, the Information Technology Act, 2000 and the CERT-In Directions, 2022 have similar duties relating to cybersecurity procedures and reporting of cyber incidents. The Digital

[1] The Companies Act, 2013, No. 18 of 2013 (India).
[2] The Companies Act, 2013, § 166.

ISSN: 2582-6433

Personal Data Protection Act, 2023 also acknowledges that the fiduciary has the obligation to take reasonable security measures. In this context, the question is whether a cybersecurity failure should be regarded as a mere operational failure, or also as a failure by directors' fiduciary care.

The paper argues that cybersecurity is emerging as an essential element of governance, is shifting responsibility to directors, who should not be left to personally oversee security technologies. Instead, directors should put the right controls in place, acquire sufficient knowledge of material cyber threats, monitor implementation and respond when necessary.

2. UNDERSTANDING CYBERSECURITY AS A CORPORATE GOVERNANCE ISSUE

Corporate governance in its earliest form refers to the mechanisms by which a company is directed, administered and controlled. It is a set of relationships between a company's management, its members and its various stakeholders.

Digitalization of business operations has broadened the scope of business risks. Cybersecurity is no longer about the security of computer systems only. It is about security of corporate assets, sensitive data, uninterrupted operation and stakeholder interests.

The potential implications of a cybersecurity incident may be:

To start with the question about the money loss, there are a number of reasons that could have, Business disruption, Ransom cost, A very large lawsuit, Enforcement and penalties, and Reparation cost. Second, effects relating to one's reputation may have an impact on consumer confidence and investor opinions. Thirdly, actions could be pursued in the event of violations of data protection requirements, contractual obligations, and statutory obligations to notify. The operation effects may prevent the company from being able to conduct normal business operations. These results prove that there is a direct link between cybersecurity and risk management of a corporation.

A totally outside board of directors may not see the relationship between technology risk and sustainability. There's a clear distinction. Cybersecurity technical implementation might be delegated to the IT department, but the requirement to put in place adequate systems of oversight and risk management cannot. Accordingly, cybersecurity governance requires a combination of technical expertise, management responsibility and board-level supervision.

ISSN: 2582-6433

3. STATUTORY FRAMEWORK UNDER THE COMPANIES ACT, 2013

3.1 Section 166: Duties of directors

Section 166 of the Companies Act, 2013 is the key to grasping the responsibility of Directors for Cybersecurity.

Section 166 (2) directors shall act in good faith to promote the objects of the company and to benefit the company, having regard to the interests of its employees, its shareholders, the community and the protection of the environment.

Section 166(3) sets out that directors must exercise their powers with due and reasonable care, skill and diligence and exercise independent judgment. While the provision does not explicitly cover cybersecurity, the words reasonable care, skill and diligence are sufficiently flexible to encapsulate any corporate threats of the future. For example, if a firm runs an online financial facility and is repeatedly warned about weaknesses in its system, the board cannot, a firm says, shift blame by claiming that the technical department has always been responsible for cyber safety. This question should be whether the directors adopted acceptable monitoring mechanisms and addressed the significant information provided to them. Even so, the fact that a cyberattack occurred will not, in itself, necessarily constitute a breach of Section 166. Cyber-attacks are impossible to prevent entirely, even by organizations that have a large amount of security infrastructure in place. Legal obligations should thus focus on the quality of governance, the quality of information to the directors and the reasonableness of their response.

Section 166(4) on directors not making themselves interested might also be used if a director has an interest, which has a financial interest in the cybersecurity service provider and/or vendor and which has not been made available to the company.

Overall then, Section 166 do provide some form of mechanism to test directors' actions as to cyber governance.

3.2 Section 134: Corporate responsibility and risk management

Section 134: Responsibilities relating to financial statements, the Board's report and corporate disclosures. The report of the Board to be included in the prescribed form and in the manner as may be prescribed shall include a statement indicating a development and a proper application of a risk management policy for the company including identification of elements of risk, that in the opinion of the Board, may threaten the existence of the company.

In terms of cybersecurity, this section is especially topical as serious cyber security events can jeopardize business continuity and corporate stability. Data protection and security risks may also involve failure or disruption by external service providers, digital infrastructure security

ISSN: 2582-6433

breaches, unauthorized access to data and systems. The board's role should not only be restricted to approving a generic risk management policy but also include governance of material cyber risks identification, risk assessment, and integration with an enterprise risk management system.

Likewise, Section 134(5)(e)[3] in relation to the existence of internal financial controls and whether such controls are operating effectively in the relevant companies, will also be relevant where information systems used for financial reporting purposes or transactions or information is compromised by cyber security vulnerabilities.

However, internal financial controls are not a substitute for a full cyber security programme. The two can be combined, but they are not the same. A company might, for example, have excellent controls in place over its financial statements, yet be exposed to an attack on its customer records or operations. Therefore, the company's oversight of cybersecurity needs to be more extensive.

3.3 Section 149 and the accountability of independent directors

Independent directors offer objective oversight and independent judgment. The liability of an independent director and other non-executive directors, who are not promoters or key managerial personnel, is restricted under section 149(12)[4] to any act or omission within their knowledge, attributable to them and Board process, and with their consent, connivance or where they have not acted diligently This provision plays a crucial role in the liability of independent directors for cybersecurity failure.

We may not be able to require an independent director to be a cybersecurity expert, but we should be able to expect an independent director to perform rigorous due diligence and not go entirely fishing off the water's edge. We should not be able to get a statutory "due care" reading that assumes an independence director can just go surfing the net and checks out of material company risks. If cybersecurity concerns have been continually raised in board meetings, in fact a major breach has occurred or management detects critical inadequacies in response, the independent directors might be called upon to assess the strength of the proposed response.

Section 149(12) immunity should not be used as a shield for conscious inaction or ignoring material information. Equally, the independent director should not be automatically held liable simply because the cyber incident happens at the time when he/she is in office. The difference between passive membership on the board and active participation in the

[3] The Companies Act, 2013, § 134(5)(e).
[4] The Companies Act, 2013, § 149(12).

ISSN: 2582-6433

oversight of the company is therefore significant.

3.4 Section 177: Audit Committee and risk oversight

Section 177[5] prescribes the constitution and role of Audit Committee in the prescribed classes of companies. The Audit Committee has a significant role in overseeing the company's financial reporting processes, internal controls and associated governance issues. Cybersecurity could impact the accuracy of financial information, the validity of accounting systems and the security of valuable company records.

Thus, the Audit Committee should consider cybersecurity risks to the extent that they impact internal controls, financial reporting, regulatory compliance and the accuracy of corporate information. This does not mean that the committee will take over from the chief information security officer or perform its own technical security analysis.

Instead it must help make sure proper reporting channels are in place, and that any matter of cybersecurity concern is properly weighted at the board level.

4. CYBERSECURITY OBLIGATIONS UNDER THE SEBI REGULATORY FRAMEWORK

Another major aspect of the discussion is the regulatory duties that listed companies carry out. The SEBI[6] (Listing Obligations and Disclosure Requirements) Regulations, 2015 provide for Governance and disclosures in the case of listed entities.

Regulation 17 is concerned with the duties of the board of directors and sets out board prescribed governance function.

Regulation 18 is to do with the Audit Committee and the corporate monitoring function. Regulation 27 – Corporate governance compliance reporting.

Regulation 30[7] is headed Material Events and Information.

Cybersecurity incidents could directly impact listed companies operational, financial and reputational standings. Consequently, disclosure obligations may be triggered where an incident meets the relevant materiality thresholds. SEBI has given special importance to incidents of cybersecurity and sharing or losing data or documents in its regulatory approach. By integrating these disclosures related to cybersecurity into its entire corporate governance

[5] The Companies Act, 2013, § 177.
[6] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, regs. 17, 18 and 27.
[7] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, reg. 30 and Schedule III, as amended.

ISSN: 2582-6433

reporting structure, the company has now shown that cybersecurity is not entirely a matter of internal technology.

It also highlights the need for transparency to prevent losing the investor's confidence. But the fact of disclosure and oversight are two separate duty. A firm could make a disclosure about a cybersecurity incident that has happened; however, this disclosure alone did not indicate that the board had had sufficient preventive governance. Hence, the inclusion of both preventive supervision and transparent disclosure, along with incident response should be the way forward.

5. THE INFORMATION TECHNOLOGY ACT, 2000 AND CERT-IN DIRECTIONS, 2022

Cyber law in India is based on Information Technology Act, 2000.

Section 43A, by its textual and statutory conditions, was primarily invoked for failure to protect sensitive personal data/information. Its current status must be analyzed in conjunction with the Digital Personal Data Protection Act, 2023, which enables omission of section 43A from its implementation.

Section 70B[8] Certification of agency. The CERT- in shall be the national agency designated for performing any cybersecurity task specified under this Act. Directions issued by CERT-In[9], under Section 70B(6): Directions issued on 28 the April 2022 by CERT-In on information security practices, procedures, prevention, response and reporting of cyber incidents.

As outlined in the Directions, bodies corporates and other entities need to report prescribed types of cyber incidents they become aware of, or observe, within six hours.

This reporting duty is all the more important for corporate management. A company that is in the middle of a high-impact security incident should still have communication channels internally to get the right information to the right person in a timely manner.

The board should verify that a reporting strategy has been established including the way in which incidents will be escalated, responded to and compliance will be maintained. While the CERT-In Directions place an obligation on certain entities, instead of creating a general fiduciary duty of a director to every director, corporate system flaws may lead to a question on the quality of the board's supervision.

[8] Information Technology Act, 2000, No. 21 of 2000 (India), § 70B.

[9] Indian Computer Emergency Response Team, Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In, 28 April 2022.

ISSN: 2582-6433

The requirement that it be reported within six hours also shows why cybersecurity cannot be something to be addressed only before the next board meeting. Good governance involves pre-planned work and established emergency decision-making processes.

6. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND CORPORATE ACCOUNTABILITY

Introduction to the Digital Personal Data Protection Act, 2023.

Section 8[10] imposes general obligations on a Data Fiduciary, including that of being responsible for processing carried out by such Data Fiduciary or on its behalf by a Data Processor. 8(5) The Data Fiduciary shall employ reasonable security safeguards to protect personal data to prevent its breach.

Section 8(6) deals with the duty to notify the prescribed authorities and Data Principals in the event of a personal data breach.

The above regulations relate to companies when handling personal data for business purposes. A significant aspect of Section 8 is that outsourcing the processing of data will not, by virtue of do so, automatically dis-apply the legal duties of the Data Fiduciary. This has significant corporate governance implications. Many companies outsource to cloud service providers, to external technology vendors or to third party data processors. Outsourcing to a cloud provider does not mean the total assumption of regulatory responsibility. The board therefore has to be satisfied that contractual, organizational and technical provisions are in place. The Statutory liability of the company as a Data Fiduciary should be distinguished from the personal liability of directors. DPDP Act does not automatically impose direct liability on every director for each breach – personal liability will depend on the provisions of the law that are relevant and the circumstances of each director's conduct. This distinction is important to prevent an unwarranted increase of directors' liability.

7. WHEN SHOULD A CYBERSECURITY FAILURE BECOME A FIDUCIARY FAILURE?

It is not whether the company was the victim of a cyber-attack but whether the directors have failed to exercise the care and skill they would have exercised if they had a duty to do so (non-executive directors). An incident can occur even when controls are in place. Consequently, an incident, even where controls at the company were inadequate, cannot be relied upon to

[10] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India), § 8.

ISSN: 2582-6433

establish Negligence or Breach of Fiduciary Duty. It seems far more reasonable to consider if the board was acting in a reasonable manner in the lead up to, during and after the event. Three categories of conduct may be distinguished.

7.1 Failure to establish reasonable oversight mechanisms

It can also be considered a failure on the part of the board if there is no process in place for the identification and ongoing review of material cybersecurity threats-although this is especially important where a company's operations rely on digital infrastructure. The level of control needs to be commensurate with the size of the organization, nature of the business, sensitivity of information and the extent of the exposure to cyber-attacks.

7.2 Disregard of known cybersecurity warnings

There are worse scenarios when directors are alerted to ongoing cyber risks that are severe enough that the board should have known but do not actually take reasonable precautions. For instance, a failure to act after internal auditors, cyber security professionals or senior management have warned about significant risks and the board has chosen not to respond may be viewed as a failure to discharge its duty of care and negligence.

7.3 Inadequate incident response and regulatory compliance

A board could also have a governance issue if an organization did not have appropriate procedures in place to respond to cyber events. These failures may consist of the lack of reporting procedures, insufficient escalation procedures, failure to preserve relevant records and non-compliance with relevant statutory reporting requirements. But the assessment still has to take account of the reasonably available information the directors had at the time in question.

You shouldn't judge a board solely by what you know in hindsight.

8. JUDICIAL APPROACH TO DIRECTORS' FIDUCIARY RESPONSIBILITIES

It is well settled that the directors occupy positions of duties of loyalty, good faith and responsibility towards the company. In Dale and Carrington Investment (P) Ltd. V. P.K. Prathapan[11], the Supreme Court acknowledged the fiduciary nature of the powers of directors

[11] Dale and Carrington Investment (P) Ltd. v. P.K. Prathapan, (2005) 1 SCC 212.

ISSN: 2582-6433

and found their misuse on account of allotment of shares. The judgment was not specifically in relation to cybersecurity, but its recognition of a director's fiduciary duties offers a solid footing for the extent of corporate accountability.

Again, in the case of official liquidator v. P.A. Tendolkar[12], the Supreme Court has considered the question of the duties of directors and their liability in cases of company misfeasance. However, the judgment also is relevant on the proposition that directors are not always able to wriggle out of the liability where by law their acts or omissions is relevant. N. Narayanan v. Adjudicating Officer[13], SEBI, the Supreme Court restated the importance of corporate accountability, and transparency in the regulation of securities. Though these holdings aren't providing a precise legal test for corporate cybersecurity oversight, they do suggest that holding corporate officer positions carries legal responsibilities that aren't necessarily dependent on attending board meetings.

9. COMPARATIVE PERSPECTIVE: THE UNITED STATES AND THE DUTY OF OVERSIGHT

With respect to the interaction of board oversight and risk management, comparative corporate law provides some information. The responsibilities of directors to oversee the corporation are frequently discussed in the United States in the context of the Delaware Supreme Court case of in re Caremark International Inc. Derivative Litigation[14]. The Caremark approach acknowledges that directors may be liable where there has been a persistent or serious failure to implement information or reporting systems, or a conscious disregard of these systems. The Delaware Supreme Court explored this concept in Marchand v. Barnhill[15] in the context of a company's key compliance risk.

These verdicts also deliver instructive signals for Indian corporate law in addressing the failures to secure the electronic governance framework. Cybersecurity may be a key operational and compliance risk for any organization relying on digital platforms or handling sensitive information in its business. But one cannot adopt this US method of revealing it here in India. Indian company law has the law also like company law Sections 149 & 166 of Companies Act, 2013. Lessons to learn from the comparison are that with regards to the board oversight, involved, informed, proportional and relevant to the risk level of the business.

[12] Official Liquidator v. P.A. Tendolkar, (1973) 1 SCC 602.
[13] N. Narayanan v. Adjudicating Officer, SEBI, (2013) 12 SCC 152.
[14] In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).
[15] *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).

ISSN: 2582-6433

10. CHALLENGES IN IMPOSING PERSONAL LIABILITY ON DIRECTORS

While acknowledging that cybersecurity has a governance dimension is a step in the right direction, shifting the burden of accountability onto individuals on the board without due protections can have a negative impact.

To start with, cybersecurity is a complex technical subject. Directors may lack expert knowledge on areas such as encryption, network design, malware, or spotting the signs of an attack.

Secondly, cyber-attacks are relentless. Organizations that have significant security infrastructure can also be under attack.

Thirdly, the risk of excessive personal liability may deter people from taking independent directorships, particularly where the company is information technology intensive.

Fourthly, the legal standard may lead to defensive compliance practices, instead of actual effective cybersecurity governance.

Fifth, this boundary should be maintained: the company (and its responsibility) versus the individual director. In general, the corporation will be the corporate actor principally in a position to meet the statutory obligations.

Only where the legal obligation of the individual director for his conduct and accountability has been established should he be made responsible.

The court was therefore correct in concluding that the appropriate test should be something more akin to reasonable diligence, knowledge, oversight and the factual situation of the case.

11. PROPOSAL FOR A BOARD-LEVEL CYBERSECURITY ACCOUNTABILITY FRAMEWORK

There are governance measures that can be adopted by the existing legal framework without a construction of an entirely separate statutory category of directors' liability. This paper proposes the following framework.

11.1 Acknowledgement that cybersecurity is a material corporate risk

Inclusion of cyber security risks as part of material enterprise risk management policy. The board should also monitor the organization’s cyber risks on an ongoing basis in light of its business model, digital architecture and information it handles.

ISSN: 2582-6433

11.2 Periodic cybersecurity reporting to the board

The management shall give regular reports related to material vulnerability, incident, security review and remedial measures.

The reporting should be transparent to non-technical directors and include areas of risk that can only be managed at board level.

11.3 Defined responsibilities within the board

Depending on the relevant legal framework and the company's regulations, companies may delegate the responsibility for cybersecurity oversight to an appropriate board committee, such as the Risk Management Committee or the Audit Committee.

Responsibility for material cybersecurity risks and control measures should be clearly defined.

11.4 Independent cybersecurity assessment

Organizations should regularly seek an independent review of their cybersecurity posture. They may also include identifying weaknesses, testing of incident response procedures and internal controls.

11.5 Procedures for cyber incident response

Boards ought to ensure that companies have documented processes for escalating, investigating and responding to cybersecurity events.

The process should take into account CERT-In reporting obligations and other applicable data protection obligations.

11.6 Directors' awareness of cybersecurity

Directors to be trained regularly on new cyber threats, data protection requirements and their governance role. This training should be proportionate to the exposure of the business and technology.

11.7 Clear standards for independent director accountability

The guidance should state that independent directors have the obligation to apply ordinary care and review substantial cybersecurity issues referred to the board.

Despite that they should not be considered the sponsors of the technical security nor be infected by the incidents, usually beyond their reasonable expertise and control.

ISSN: 2582-6433

11.8 Transparent disclosure and accountability

Listed companies should have in place adequate procedures for assessing whether a cybersecurity incident would constitute an event requiring disclosure as per SEBI regulations. The information provided in the disclosures should be accurate, timely, conform to legal and regulatory requirements and consider real security risks.

12. FINDINGS AND DISCUSSION

This analysis highlights the increasing relevance of cybersecurity as a new attribute of corporate governance in India. There is not specific statutory fiduciary duty in regard of cybersecurity in the Companies Act, 2013. However, Section 166 of Companies Act, 2013 broadly provides the statutory basis to explore whether directors have acted with reasonable care, skill, and diligence and independent judgment. Section 134 further elaborates on this by acknowledging the role of corporate risk management and internal controls. Section 149(12) is relevant to uphold the distinction between governance duties of independent directors as distinguished from the situations under which the personal liability of such directors may be incurred.

This point is also driven home by SEBI regulatory mechanism that also highlights material disclosures and board level oversight on part of the listed entities.

THE CERT-IN DIRECTIONS AND THE DPDP ACT, 2023 on reporting of cybersecurity incidents and on data privacy. But even as a stand-alone theory, it would not, in itself, be enough to establish a comprehensive approach to how a director's personal fiduciary obligation should be ascertained. A more structured approach is therefore desirable. This provides further argument for 'cybersecurity as a material business risk of corporate governance' with the personal liability element still subject to failures of oversight or diligence.

13. CONCLUSION

The digitalization of the daily operations of companies has revolutionized the nature of the risks incurred by companies. Cybersecurity breaches are no longer isolated to the information technology department. They are transferable to corporate assets, financials, confidence of investors, statutory compliance, business continuity. Indian corporate law, which are capable of dealing with these developments. Section 166 of the Companies Act, 2013 sets out the duties of good faith, reasonable care, skill and diligence, and independent judgment, while corporate risk management is recognized in Section 134, and many provisions relating to oversight are

ISSN: 2582-6433

set out in Section 149, and Section 177. The SEBI regulatory framework as well as the CERT-In Directions, 2022 and the Digital Personal Data Protection Act, 2023 continues to highlight the growing need of cybersecurity and information security in corporate governance.

In summary, this paper contends that cybersecurity should be recognized as falling within the scope of directors' responsibilities and that directors do not have to undertake a technical role, but must establish systems to identify, report and manage the risk. But when it does come to attack, we might want to exercise some restraint in blaming a person. That's an overly simplistic approach to hacking and sets the almost impossibly high bar to corporations.

Fortunately, a proportionate standard of board level oversight of cybersecurity should be developed which is proportionate to the type of company, the materiality of the risk, the information provided to the directors and the nature of the directors' response. However, in order for digital responsibility to be achieved in corporate governance, the perspective on cybersecurity must change from treating it as a specialized technical field to make it a piece of fiduciary responsibility.

IJLRA