Page: 238-263 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.128

CYBER DUE DILIGENCE IN MERGERS & ACQUISITIONS: THE OVERLOOKED RISK

Apoorva[1]

I. ABSTRACT

The research paper titled "Cyber Due Diligence in Mergers & Acquisitions: The Overlooked Risk" critically examines the growing significance of cybersecurity and data protection in corporate transactions. It highlights that in the digital era, data assets have become vital determinants of corporate value, yet cyber due diligence remains an underexplored area in mergers and acquisitions. The study analyzes how the absence of structured cybersecurity assessments exposes acquirers to legal, financial, and reputational liabilities. It explores India's existing legal framework under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, revealing substantial regulatory gaps compared to international models like the EU's GDPR and the U.S. SEC's disclosure-based approach. The paper argues that integrating cyber due diligence into the M&A process is crucial for risk mitigation, corporate governance, and investor confidence. It further recommends legal reforms, contractual safeguards, and regulatory enforcement mechanisms to make cybersecurity assessment a statutory obligation. By drawing on global jurisprudence and Indian corporate practices, the research provides a comprehensive blueprint for embedding cyber risk governance within India's M&A landscape, ensuring compliance, value preservation, and sustainable digital business integration.

II. KEYWORDS

Cyber Due Diligence, Mergers and Acquisitions, Data Protection Law, Cybersecurity Governance, Corporate Risk Management.

III. INTRODUCTION AND RESEARCH FRAMEWORK

A. Background of Study

Corporate mergers and acquisitions have entered a new era driven by digital transformation. Data has become a strategic asset that determines business value and competitive advantage. Yet, it also

[1] LLM Student at Geeta Institute of Law (India). Email: apoorva3551@gmail.com

introduces significant cybersecurity risks. Companies today rely on digital infrastructure to manage intellectual property, financial records, and sensitive consumer information. When an acquisition occurs, these data assets and vulnerabilities transfer to the acquiring entity, often without a full understanding of their hidden risks.[2]

In India, the rapid growth of the digital economy has heightened the importance of cybersecurity compliance. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) and the existing Information Technology Act, 2000 require organizations to adopt reasonable security practices. However, these laws do not explicitly prescribe cyber due diligence requirements in mergers and acquisitions, creating a compliance gap. As a result, many acquiring firms fail to evaluate the target company's cybersecurity posture or history of data breaches before finalizing deals.[3]

The consequences of neglecting cyber due diligence are significant. In 2017, Verizon's acquisition of Yahoo was impacted by undisclosed data breaches, reducing the deal value by USD 350 million. Similarly, Marriott International faced heavy penalties under the EU's General Data Protection Regulation (GDPR) for a breach discovered post-acquisition in the Starwood Hotels merger.[4] These cases highlight how inadequate cybersecurity assessment can directly affect transaction value, regulatory exposure, and corporate reputation.

Indian regulators, including the Securities and Exchange Board of India (SEBI), emphasize the disclosure of material risks during transactions. Yet, most corporate disclosures focus on financial liabilities and overlook cybersecurity risks. This oversight exposes investors and shareholders to hidden threats that may surface only after the transaction closes. The absence of a standardized framework for cyber due diligence in India makes it difficult for acquirers to evaluate digital risks effectively. Hence, there is a pressing need for a legal and policy-based approach that integrates cyber resilience into M&A governance.[5]

[2] KPMG, Cyber Due Diligence in M&A Transactions, KPMG Report (2023).
[3] The Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[4] Verizon Communications Inc. v. Yahoo! Inc., 2017 M&A Dispute (Del. Ch. 2017); In re Marriott International, Inc. Data Breach Litigation, 440 F. Supp. 3d 447 (D. Md. 2020).
[5] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, Reg. 30.

B. Statement of the Problem

Despite growing awareness, cyber due diligence remains underdeveloped in Indian M&A practice. Most due diligence checklists prioritize financial audits, tax liabilities, and corporate compliance while giving minimal attention to cybersecurity. This limited approach results in post-acquisition shocks when undisclosed data breaches or security weaknesses emerge. The lack of structured cybersecurity assessment not only increases operational risk but also exposes companies to legal penalties under data protection and IT laws.[6]

Indian legal frameworks remain fragmented in addressing this issue. Section 43A of the Information Technology Act, 2000 requires companies to maintain "reasonable security practices," yet it offers no clear guidance on evaluating these standards during M&A transactions. The DPDP Act, 2023 imposes obligations on data fiduciaries but omits specific provisions mandating cyber due diligence before acquisitions. This legal vacuum forces companies to rely on contractual protections such as warranties and indemnity clauses, which often prove inadequate once a cyber incident occurs.[7]

C. Objectives of the Study

1. To critically examine the significance of cyber due diligence in mergers and acquisitions and its role in identifying, mitigating, and managing cyber risks in corporate transactions.
2. To analyze the existing legal and regulatory framework governing cybersecurity and data protection in India, particularly under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, and assess its adequacy in addressing cyber risks in M&A.
3. To compare India's approach to cyber due diligence with international legal standards, including the frameworks of the European Union, the United States, and the United Kingdom, and identify best practices for integration into the Indian regulatory regime.

[6] Deloitte, Cybersecurity in M&A: Managing the Hidden Risk, Deloitte Insights (2022).
[7] Section 43A, Information Technology Act, 2000 (India); Rule 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

4. To propose legal, policy, and corporate governance reforms for institutionalizing cyber due diligence as a mandatory component of M&A transactions, ensuring compliance, transparency, and value preservation.

D. Research Questions

1. What is the legal significance of cyber due diligence in the context of mergers and acquisitions, and why has it emerged as a critical component in the digital era?
2. How effective are India's existing cybersecurity and data protection laws in regulating cyber risk assessment during M&A transactions?
3. What lessons can India draw from international legal frameworks such as the GDPR and SEC disclosure regulations in strengthening its cyber due diligence mechanism?
4. How can corporate governance, contractual frameworks, and statutory reforms enhance cyber due diligence practices to ensure accountability and investor protection in M&A?

E. Research Methodology

The research follows a doctrinal methodology, relying on a detailed examination of primary and secondary legal sources. Primary sources include statutory provisions such as the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, SEBI regulations, and relevant case law from Indian and international jurisdictions. Secondary sources include scholarly articles, law commission reports, journals, research papers, and institutional publications from global organizations like OECD, UNCTAD, and KPMG. The study adopts a comparative and analytical approach to evaluate the existing Indian legal framework against international practices. Through critical interpretation of legislation, judicial decisions, and policy reports, the research aims to develop a comprehensive legal understanding of cyber due diligence in M&A and suggest actionable reforms for strengthening compliance and governance in India's corporate landscape.

IV. UNDERSTANDING CYBER DUE DILIGENCE IN MERGERS & ACQUISITIONS

A. Concept and Meaning of Due Diligence

Due diligence forms the foundation of every merger or acquisition. It refers to the systematic examination of a target company's legal, financial, operational, and regulatory aspects before finalizing a transaction. The objective is to uncover hidden liabilities, assess compliance, and determine the true value of the business. The term originated from corporate practice but has expanded in scope to include technological, ethical, and cyber dimensions in the digital age.[8]

In the context of M&A, due diligence ensures that the acquirer has a complete understanding of the target's business model and risk exposure. Traditionally, this process focused on accounting records, contractual obligations, and corporate governance structures. However, the modern corporate ecosystem is intertwined with digital infrastructure, making cybersecurity and data protection equally vital. A company's digital assets-ranging from customer databases to proprietary algorithms-can now represent a large portion of its valuation. Hence, the process of due diligence must evolve beyond financial scrutiny to include an evaluation of cyber resilience and data governance frameworks.[9]

Indian corporate law recognizes the concept of due diligence through multiple statutes. The Companies Act, 2013, under Section 134, imposes obligations on directors to ensure compliance with applicable laws and to exercise due care. Similarly, SEBI's Listing Obligations and Disclosure Requirements (LODR) Regulations, 2015, require listed entities to disclose material risks, which may include cybersecurity vulnerabilities. These provisions establish that failure to perform adequate due diligence can constitute a breach of fiduciary duty and corporate governance principles.[10]

B. Evolution of Cyber Due Diligence in Corporate Transactions

The emergence of cyber due diligence corresponds with the increasing digitization of business processes. In the early 2000s, M&A due diligence largely ignored cyber issues, assuming that

[8] Bain & Co., Due Diligence in the Digital Age: Redefining Risk Evaluation (2022).
[9] The Companies Act, No. 18 of 2013, India Code (2013), §134.
[10] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, Reg. 30.

information technology risks were merely technical concerns. However, as data breaches became more frequent and costly, cyber resilience began to influence transaction outcomes. The 2013 Target Corporation data breach, which compromised 40 million customer records, demonstrated how cybersecurity failures could lead to financial loss and shareholder litigation. It marked a turning point where cyber risk became a material concern in corporate governance.[11]

The global regulatory landscape accelerated this evolution. The European Union's GDPR, enacted in 2016, imposed strict obligations on entities handling personal data, including cross-border data transfers. In the United States, the Securities and Exchange Commission (SEC) issued guidance requiring companies to disclose material cyber risks to investors. These developments forced acquirers to evaluate not only the target's compliance posture but also its incident history, data management protocols, and vendor security arrangements.[12]

In India, this transition has been gradual. The National Cyber Security Policy, 2013 and the subsequent DPDP Act, 2023 have created a legal infrastructure for data protection, but the integration of cyber diligence in M&A remains largely voluntary. Corporate acquirers, especially in technology-driven sectors like fintech, health tech, and e-commerce, have started adopting cyber audits as part of their due diligence checklists. However, small and medium-sized enterprises still lag behind due to lack of awareness and technical expertise.[13]

C. Key Components of Cyber Due Diligence

Cyber due diligence involves a structured evaluation of the target company's digital ecosystem. It encompasses several interrelated components, each addressing a distinct aspect of cyber risk. The first component is policy and governance review-assessing whether the target has formal cybersecurity policies, incident response protocols, and employee training programs. Weak governance structures indicate a higher likelihood of future breaches.[14]

The second component is technical infrastructure assessment, which examines network architecture, encryption methods, system vulnerabilities, and access control mechanisms. Penetration testing and security audits are crucial to identify exploitable weaknesses. The third

[11] In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).
[12] U.S. Securities and Exchange Commission, Cybersecurity Disclosure Guidance, Release No. 33-10459 (2018).
[13] National Cyber Security Policy, 2013, Ministry of Electronics and Information Technology, Govt. of India.
[14] PwC, The Role of Cyber Governance in Corporate Transactions (2021).

component is data management evaluation, which includes reviewing how personal and sensitive information is collected, stored, transferred, and deleted. Compliance with the DPDP Act, 2023 and IT Rules, 2011 must be verified, particularly for entities handling customer or employee data.[15]

Another vital component is third-party risk management. Many cyber incidents arise through vendors or service providers with inadequate security measures. The acquirer must review the target's vendor contracts, non-disclosure agreements, and indemnity clauses to ensure robust data protection obligations. The Equifax breach in 2017, caused by a third-party vulnerability, underscores the significance of supply-chain security in corporate transactions.[16]

D. Cybersecurity as an Element of Business Valuation

Cybersecurity directly influences a company's market value and attractiveness to potential investors. In today's digital economy, intangible assets like data, software, and intellectual property often constitute the majority of corporate worth. A breach that compromises these assets can therefore diminish enterprise value significantly. Analysts and valuation professionals increasingly consider cyber maturity as a non-financial metric of corporate health.[17]

A company with robust cybersecurity practices demonstrates operational efficiency, customer trust, and regulatory compliance-attributes that enhance valuation. Conversely, a history of breaches or weak cyber governance signals potential future losses. The Verizon-Yahoo case and the Marriott-Starwood merger serve as prominent examples where undisclosed cyber vulnerabilities led to valuation reductions. Similarly, studies by PwC and Deloitte indicate that companies with strong cyber programs experience higher post-deal integration success rates and fewer legal disputes.[18]

Under Indian law, the principle of material disclosure requires that all relevant information likely to affect an investor's decision be revealed. SEBI's LODR Regulations, 2015, mandate disclosure of material events, which may include data breaches. Non-disclosure can attract penalties and class

[15] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 8.
[16] U.S. House of Representatives, The Equifax Data Breach: Majority Staff Report (2018).
[17] EY, Valuing Cybersecurity: The Financial Dimension of Risk (2022).
[18] PwC, Cybersecurity in M&A: Redefining Transaction Value (2020).

action suits under Section 245 of the Companies Act, 2013. Thus, from a compliance perspective, cybersecurity must be treated as a material factor influencing valuation and disclosure.[19]

E. Relationship between Data Protection, Privacy, and Due Diligence

Data protection and privacy are central to cyber due diligence because they determine legal compliance and public trust. The increasing complexity of data flows across jurisdictions means that acquirers must evaluate how the target company handles personal data under applicable laws. In India, the DPDP Act, 2023 introduces the concept of "data fiduciary" and "data principal," creating obligations similar to the GDPR's controller-processor framework. An acquirer must confirm that the target has mechanisms to obtain consent, manage data access, and ensure cross-border data transfer compliance.[20]

Privacy assessments must extend beyond compliance checklists to include cultural and ethical dimensions of data handling. In cross-border transactions, failure to comply with international data protection regimes can result in severe penalties. For instance, in *Facebook Ireland Ltd. v. Data Protection Commissioner* (2021), the Irish High Court upheld restrictions on data transfers violating GDPR provisions, underscoring the global impact of privacy regulations on corporate transactions. Indian acquirers engaging with entities in the EU or UK must therefore align with these standards to avoid conflicts.[21]

Due diligence also requires an understanding of contractual privacy obligations. Many companies are bound by privacy terms in their contracts with customers and vendors. Breaching these terms through improper data transfer or unauthorized disclosure can result in legal actions. The intersection of privacy and due diligence becomes particularly critical in sectors like healthcare, banking, and e-commerce, where sensitive personal information constitutes the core asset of the transaction.[22]

F. Importance of Cyber Risk Assessment in M&A Transactions

Cyber risk assessment has become a strategic tool in mergers and acquisitions. It involves identifying, analyzing, and mitigating potential cyber threats that may impact the transaction or

[19] The Companies Act, 2013, §245; SEBI (LODR) Regulations, 2015, Reg. 30.
[20] Digital Personal Data Protection Act, 2023, §8.
[21] Facebook Ireland Ltd. v. Data Protection Commissioner, [2021] IEHC 336 (High Court of Ireland).
[22] Deloitte, Data Protection and Privacy in Cross-Border M&A (2023).

the combined entity post-acquisition. Unlike traditional risk assessment, cyber risk evaluation considers both external threats-like hacking and ransomware-and internal vulnerabilities such as weak governance, outdated systems, and insider threats.[23]

The process begins with a baseline cyber audit that assesses the target's security posture. This includes reviewing compliance with laws like the IT Act, 2000, DPDP Act, and international frameworks. The acquirer must also evaluate the financial implications of potential breaches, including cost of remediation, regulatory fines, and reputational damage. According to IBM's *Cost of a Data Breach Report 2023*, the global average cost of a data breach stands at USD 4.45 million, a figure that can substantially alter deal valuation.[24]

V. LEGAL AND REGULATORY FRAMEWORK GOVERNING CYBER DUE DILIGENCE

A. Overview of Indian Cybersecurity and Data Protection Laws

India's legal structure governing cybersecurity and data protection has evolved in response to growing digitalization and the risks of cyber incidents. The Information Technology Act, 2000 (IT Act) was the first comprehensive statute to address electronic transactions, unauthorized access, and data breaches. Its rules on "reasonable security practices" under Section 43A laid the foundation for corporate accountability in data protection. The Act, supplemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, created obligations for companies to protect personal data through managerial and technical safeguards.[25]

However, the IT Act's framework is more reactive than preventive. It focuses on penalizing unauthorized access or data theft but lacks a proactive mechanism for ensuring cybersecurity readiness during corporate transactions. The emergence of large-scale digital infrastructure, cloud computing, and cross-border data flows demanded a new regime capable of addressing these risks. This gap led to the introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act), a

[23] KPMG, Cyber Risk in M&A Transactions: A Global Perspective (2022).
[24] IBM, Cost of a Data Breach Report (2023).
[25] Information Technology Act, No. 21 of 2000, India Code (2000).

statute designed to align India's data protection framework with international standards like the GDPR.[26]

The DPDP Act establishes data fiduciary responsibilities, introduces consent-based processing, and sets penalties for non-compliance. Its scope extends to foreign companies processing the data of Indian citizens, thus impacting cross-border mergers. Alongside, sectoral regulators such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have issued guidelines mandating cyber resilience and reporting mechanisms. SEBI's circular of 2022 requires intermediaries to maintain robust cyber frameworks and disclose material incidents, reflecting a convergence between data protection law and corporate governance norms.[27]

India's corporate legal ecosystem, particularly the Companies Act, 2013 and SEBI regulations, further integrates cybersecurity obligations within the broader due diligence process. Under Section 134 of the Companies Act, directors must report internal control adequacy and risk management. In the context of mergers and acquisitions, these obligations extend to identifying cyber vulnerabilities that could affect business continuity. Despite these developments, India still lacks an explicit statutory requirement for cyber due diligence during M&A, relying instead on implied obligations under corporate and IT governance frameworks.[28]

B. The Information Technology Act, 2000 and its Relevance in M&A

The Information Technology Act, 2000 forms the bedrock of India's cyber law regime. Although originally enacted to promote e-commerce and regulate electronic records, its provisions now play a critical role in defining cybersecurity accountability. Section 43A imposes liability on a "body corporate" for negligence in implementing reasonable security practices leading to wrongful loss or gain. This provision creates a civil liability framework relevant for M&A transactions, where the acquirer inherits the target company's liabilities, including data protection failures.[29]

In mergers or acquisitions, the due diligence process must evaluate the target's compliance with the IT Act. This includes reviewing internal IT policies, data storage mechanisms, and third-party contracts to ensure adherence to security norms. Failure to comply can result in compensation

[26] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[27] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015; SEBI Circular on Cybersecurity Framework, June 2022.
[28] The Companies Act, No. 18 of 2013, §134, India Code (2013).
[29] Section 43A, Information Technology Act, 2000 (India).

claims under Section 46 and potential penalties under Section 66 for computer-related offenses. The acquisition of a company with prior breaches exposes the acquirer to regulatory inquiries and civil suits from affected stakeholders.[30]

The 2011 Rules under the IT Act specify what constitutes "reasonable security practices." Rule 8 mandates adherence to ISO/IEC 27001 standards or equivalent frameworks. This transforms cybersecurity from a technical requirement into a legal obligation. For instance, if an acquiring company fails to verify whether the target's IT infrastructure meets these standards, it risks assuming post-transaction liabilities. The ICICI Bank Ltd. v. Shanti Devi Sharma (2008) case highlighted the importance of data integrity and confidentiality under the IT regime, reinforcing that negligence in protecting personal data can attract civil damages.[31]

The IT Act also recognizes offenses like hacking, identity theft, and data alteration under Sections 65 to 67C. From an M&A perspective, these provisions underscore the importance of cyber audits to identify past violations. In cases where the target's systems have been compromised, even unknowingly, the acquirer could face reputational harm and litigation risks. Consequently, cyber due diligence under the IT Act is both a legal safeguard and a business necessity, ensuring the continuity and legality of digital assets acquired through M&A transactions.[32]

C. Digital Personal Data Protection Act, 2023: Implications for M&A

The Digital Personal Data Protection Act, 2023 represents a major shift in India's data governance landscape. It introduces a rights-based framework that prioritizes individual consent, transparency, and accountability in data processing. For mergers and acquisitions, the Act's implications are extensive because data now constitutes a valuable business asset and a potential liability. Under the Act, the acquirer assumes the role of a "data fiduciary" responsible for ensuring lawful processing of personal data inherited from the target company.[33]

Section 8 of the DPDP Act mandates that data fiduciaries adopt technical and organizational measures to prevent unauthorized processing. This requires acquirers to assess whether the target has complied with these requirements prior to the transaction. Inadequate compliance can lead to

[30] Sections 65–67C, Information Technology Act, 2000 (India).
[31] ICICI Bank Ltd. v. Shanti Devi Sharma, AIR 2008 Del 187.
[32] Rule 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[33] Digital Personal Data Protection Act, 2023, §8.

penalties under Section 33, which imposes fines up to ₹250 crore for breaches. The Act also mandates prompt reporting of data breaches to the Data Protection Board, making it essential for acquirers to review the target's past incident history and breach disclosure records.[34]

Another key implication lies in cross-border data transfers. Section 16 of the DPDP Act restricts data transfers to countries not approved by the Central Government. M&A transactions involving multinational corporations must ensure that data migration following the merger complies with these transfer restrictions. Failure to do so could result in both domestic and international legal conflicts, particularly in deals involving entities subject to the EU's GDPR or the U.S. CLOUD Act.[35]

D. International Legal Standards on Cyber Due Diligence

Global regulatory frameworks significantly influence the practice of cyber due diligence in cross-border mergers and acquisitions. The General Data Protection Regulation (GDPR) of the European Union is the most comprehensive and widely referenced regime. It establishes strict obligations for data controllers and processors, mandating due diligence to ensure compliance when transferring ownership or control of data. Articles 5, 32, and 33 of the GDPR require companies to maintain data integrity, ensure security, and promptly report breaches. Non-compliance can result in fines up to €20 million or 4% of annual global turnover, whichever is higher.[36]

In mergers involving EU-based entities, the acquirer must verify the target's GDPR compliance, particularly regarding lawful processing, data subject rights, and cross-border data transfer mechanisms. The Marriott International case demonstrates how regulators hold acquirers accountable for pre-existing breaches. The UK's Information Commissioner's Office fined Marriott £99 million for failing to detect a data breach at Starwood Hotels prior to acquisition, establishing a precedent that due diligence must include cybersecurity assessment.[37]

E. Comparative Analysis of the USA, EU, and UK Regulatory Approaches

The global regulatory environment around cyber due diligence varies across jurisdictions but shares a common intent-enhancing corporate accountability in digital risk management. The

[34] Digital Personal Data Protection Act, 2023, §33.
[35] Digital Personal Data Protection Act, 2023, §16.
[36] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), arts. 5, 32, 33.
[37] In re Marriott International, Inc. Data Breach Litigation, 440 F. Supp. 3d 447 (D. Md. 2020).

United States adopts a sectoral and disclosure-driven approach. There is no single federal data protection law, yet numerous statutes govern cyber obligations. The Securities and Exchange Commission (SEC) mandates listed companies to disclose material cybersecurity risks and incidents in filings under the Securities Exchange Act, 1934. In In re SolarWinds Corporation Securities Litigation (2023), the SEC charged company executives for misrepresenting cyber vulnerabilities, signaling that omission of cyber risk disclosure can constitute securities fraud.[38]

The Cybersecurity Information Sharing Act, 2015, encourages private entities to share cyber threat intelligence with the federal government, fostering a collaborative defense mechanism. Simultaneously, sector-specific laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) impose security and privacy obligations on healthcare and financial institutions respectively. These frameworks, when applied to M&A transactions, require acquirers to conduct detailed cyber risk assessments to prevent inheriting non-compliant systems. The Federal Trade Commission (FTC), under Section 5 of the FTC Act, has penalized companies for unfair or deceptive cybersecurity practices, extending the accountability to M&A contexts.[39]

In contrast, the European Union (EU) has developed a more unified, rights-based regulatory regime. The General Data Protection Regulation (GDPR) establishes comprehensive obligations concerning data protection, breach notification, and cross-border data transfers. Articles 24 and 32 of the GDPR impose due diligence obligations on data controllers and processors, requiring implementation of appropriate technical and organizational safeguards. Non-compliance during corporate restructuring or acquisitions may lead to massive administrative fines, as seen in the Marriott International case, where the UK's Information Commissioner's Office fined the company £99 million for failing to detect a pre-existing data breach in its acquired entity.[40]

The EU's Network and Information Systems Directive (NIS 2) further extends cybersecurity responsibilities to critical infrastructure sectors, mandating risk assessment and incident reporting. For M&A transactions, compliance with both GDPR and NIS 2 becomes indispensable for assessing cyber resilience and avoiding legal exposure.

[38] In re SolarWinds Corp. Sec. Litig., No. 1:21-cv-00138 (W.D. Tex. 2023).
[39] Federal Trade Commission Act, 15 U.S.C. § 45; Cybersecurity Information Sharing Act, Pub. L. No. 114–113, 129 Stat. 2242 (2015).
[40] In re Marriott International, Inc. Data Breach Litigation, 440 F. Supp. 3d 447 (D. Md. 2020).

F. Corporate Governance Obligations under SEBI and Companies Act

Corporate governance in India incorporates cyber resilience within its broader risk management mandate. The Companies Act, 2013, through Section 134, requires the Board of Directors to provide a report on the adequacy of internal controls and risk management systems. This implicitly includes cybersecurity, as it directly affects business continuity and investor confidence. The Company (Management and Administration) Rules, 2014 and Secretarial Standards (SS-1 and SS-2) issued by the Institute of Company Secretaries of India further emphasize directors' responsibility to safeguard digital assets and maintain compliance with statutory obligations.[41]

Section 166 of the Companies Act establishes fiduciary duties of directors to act with due and reasonable care, skill, and diligence. Failure to evaluate cybersecurity risks before approving mergers or acquisitions can constitute a breach of these duties. In Tata Consultancy Services Ltd. v. Cyrus Investments Pvt. Ltd. (2021), the Supreme Court underscored the primacy of board-level accountability in governance decisions affecting corporate integrity. By analogy, neglecting cyber diligence before an acquisition can expose directors to liability under both statutory and fiduciary principles.[42]

The Securities and Exchange Board of India (SEBI) has also advanced governance standards addressing cybersecurity. SEBI's Listing Obligations and Disclosure Requirements (LODR) Regulations, 2015, mandate listed companies to disclose material risks and events that may impact investors. SEBI's circular of June 2022 introduced the Cybersecurity and Cyber Resilience Framework for intermediaries, directing entities to maintain continuous monitoring, conduct vulnerability assessments, and report breaches within 24 hours. These obligations imply that acquiring companies must assess the target's compliance history and incident management protocols as part of due diligence.[43]

VI. CYBER RISKS AND LIABILITIES IN M&A TRANSACTIONS

Cyber risks in mergers and acquisitions extend far beyond data breaches and technical disruptions. They encompass financial, legal, reputational, and operational exposures that arise when an acquiring company inherits the digital vulnerabilities of its target. Inadequate cyber due diligence

[41] The Companies Act, No. 18 of 2013, §§134, 166, India Code (2013); Secretarial Standards (SS-1, SS-2).
[42] Tata Consultancy Services Ltd. v. Cyrus Investments Pvt. Ltd., (2021) 9 SCC 449.
[43] SEBI Circular on Cybersecurity and Cyber Resilience Framework for Intermediaries, June 2022.

can convert a strategically sound acquisition into a liability-laden transaction. The complexity of integrating digital infrastructures and data systems between two entities introduces vulnerabilities that cybercriminals often exploit during or immediately after the deal process.[44]

In the Indian context, cyber risks in M&A transactions are amplified due to evolving data protection laws and limited regulatory guidance on cybersecurity diligence. The Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 collectively impose obligations on entities to maintain "reasonable security practices" and protect personal data. An acquirer failing to verify the target's compliance with these statutes may later face penalties, breach notifications, or class action suits from affected individuals. The principle of successor liability, recognized under corporate law, makes the acquirer legally accountable for inherited regulatory non-compliance and pre-existing data breaches.[45]

One of the most common forms of cyber risk in M&A arises from undisclosed data breaches. Companies often fail to disclose past or ongoing cyber incidents during negotiations. When such breaches surface post-acquisition, they can erode company valuation, trigger enforcement action, and harm investor trust. The Verizon–Yahoo deal serves as a landmark example, where Yahoo's undisclosed data breaches led to a USD 350 million reduction in the purchase price and subsequent shareholder litigation. A similar pattern was observed in the Marriott-Starwood merger, where the discovery of a pre-existing breach led to penalties under the EU GDPR and severe reputational loss.[46]

Another layer of risk lies in inherited vulnerabilities within IT systems. Many Indian firms use legacy software lacking encryption or security updates, exposing the acquirer to potential hacking attempts. During integration, mismatched cybersecurity standards can create exploitable weaknesses. Cross-border acquisitions are particularly prone to such risks due to inconsistent global compliance frameworks. For example, an Indian acquirer taking over a European data-

[44] Deloitte, Cybersecurity in M&A Transactions: Hidden Risks and Liabilities (2022).
[45] Information Technology Act, No. 21 of 2000, §43A, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, §33, India Code (2023).
[46] Verizon Communications Inc. v. Yahoo! Inc., 2017 M&A Dispute (Del. Ch. 2017); In re Marriott International, Inc. Data Breach Litigation, 440 F. Supp. 3d 447 (D. Md. 2020).

driven enterprise must comply simultaneously with GDPR and Indian DPDP Act mandates, failing which dual jurisdictional liability may arise.[47]

Intellectual property (IP) theft and trade secret exposure also constitute significant cyber risks in corporate transactions. Many technology-based mergers involve transferring digital assets such as patents, algorithms, and proprietary codes. Cyber intrusions during the due diligence phase can lead to theft of trade secrets, undermining the entire commercial value of the acquisition. In DuPont v. Kolon Industries (2011), unauthorized data access and misappropriation of trade secrets resulted in damages exceeding USD 900 million, illustrating how cyber vulnerabilities during acquisition processes can cause catastrophic losses.[48]

Regulatory and litigation liabilities also form a major category of cyber risk. Under the DPDP Act, data fiduciaries are obligated to notify breaches to the Data Protection Board and affected individuals. If a target company fails to fulfill this obligation before the merger, the acquirer may inherit liability for non-compliance. The IT Act, through Section 43A, allows affected persons to claim compensation for negligence in maintaining security practices. When these statutory duties intersect with corporate law principles under Section 166 of the Companies Act, 2013, directors who fail to conduct cyber due diligence could be accused of breaching fiduciary obligations, leading to personal liability.[49]

Operational risks further complicate the scenario. Integrating cybersecurity systems between merging companies is challenging due to differing technologies and vendor networks. Weak access control, misconfigured cloud environments, or insecure data migration can lead to new vulnerabilities. Many data breaches occur within 12 months of acquisition as attackers exploit the transitional phase. Without structured post-acquisition cybersecurity integration, the entire deal may result in operational instability and legal exposure under both IT and corporate governance frameworks.[50]

The Indian judiciary and regulators are increasingly recognizing the significance of cyber diligence. While explicit statutory mandates are still developing, the trend underlines that cyber

[47] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), art. 32; Digital Personal Data Protection Act, 2023, §16.
[48] E.I. DuPont de Nemours & Co. v. Kolon Indus., 2011 WL 4625760 (E.D. Va. 2011).
[49] The Companies Act, No. 18 of 2013, §166, India Code (2013).
[50] KPMG, M&A Integration and Cybersecurity Risks Report (2023).

negligence is equivalent to corporate mismanagement. Boards are now expected to treat cyber risk as a part of enterprise risk management. In M&A transactions, the legal expectation is shifting from voluntary assessment to mandatory compliance verification, ensuring that digital integrity becomes a defining parameter of transactional success.[51]

VII. ROLE OF DUE DILIGENCE IN RISK MITIGATION AND VALUE PRESERVATION

Due diligence serves as the central mechanism for identifying, assessing, and mitigating potential risks in mergers and acquisitions. In the digital economy, this process extends far beyond financial auditing-it now involves evaluating a company's cybersecurity posture, data management systems, and compliance with data protection laws. By conducting structured cyber due diligence, acquirers can uncover hidden liabilities and safeguard both monetary and reputational value that could otherwise be eroded by post-acquisition cyber incidents.[52]

Cyber due diligence enables risk anticipation rather than mere risk response. A pre-transaction assessment of the target's IT infrastructure, encryption standards, and security policies allows acquirers to quantify exposure to data breaches or compliance failures. This forms the basis for negotiating price adjustments or indemnities in merger contracts. For instance, during the Verizon–Yahoo transaction, valuation adjustments were made after cyber vulnerabilities were discovered, demonstrating how due diligence directly impacts deal pricing and liability allocation.[53]

Legal risk mitigation is achieved by mapping the target's compliance with statutory frameworks such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. Acquirers that verify adherence to these laws reduce exposure to penalties, breach notifications, and litigation from data principals. Failure to conduct this verification can lead to successor liability, where the acquiring company becomes accountable for the target's pre-acquisition data violations. Hence, legal compliance diligence not only mitigates statutory risks but also ensures operational continuity post-merger.[54]

[51] PwC, Cyber Risk Management in Indian Corporate Transactions (2023).
[52] KPMG, Cyber Due Diligence: Managing Hidden Risks in M&A Transactions (2023).
[53] Verizon Communications Inc. v. Yahoo! Inc., 2017 M&A Dispute (Del. Ch. 2017).
[54] Information Technology Act, No. 21 of 2000, §43A, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, §§8, 33, India Code (2023).

From a corporate governance perspective, cyber due diligence reinforces directors' fiduciary obligations under Section 166 of the Companies Act, 2013. Directors are required to exercise due care and diligence in safeguarding company assets, including digital assets. Neglecting this responsibility may constitute a breach of fiduciary duty. Boards that integrate cyber diligence within their M&A strategy demonstrate proactive governance and resilience against potential shareholder actions arising from undisclosed cyber threats.[55]

The process also plays a vital role in value preservation. Intellectual property, proprietary databases, and trade secrets represent significant intangible assets in modern transactions. Cyber due diligence helps ensure that these assets are adequately protected and legally owned by the target. A lapse in verifying ownership or data integrity can devalue the acquisition. In DuPont v. Kolon Industries (2011), theft of trade secrets during corporate negotiations led to substantial financial loss and highlighted the value-preserving role of digital asset verification in due diligence.[56]

VIII. INTERNATIONAL PERSPECTIVES AND EMERGING JURISPRUDENCE

The global framework on cyber due diligence in mergers and acquisitions is evolving as nations recognize data as both an economic and strategic asset. Jurisdictions like the European Union, the United States, and the United Kingdom have institutionalized legal duties requiring acquirers to assess cybersecurity and data protection compliance prior to transactions. This transformation reflects a shift from voluntary best practices to enforceable regulatory obligations anchored in corporate accountability and consumer protection.[57]

Under the European Union's General Data Protection Regulation (GDPR), data controllers and processors are legally obligated to ensure data integrity, transparency, and accountability. Articles 24 and 32 impose explicit duties of due diligence by requiring entities to adopt "appropriate technical and organizational measures" to prevent data breaches. The GDPR's enforcement approach is strict, imposing fines up to 4% of global annual turnover for non-compliance. The Marriott International case illustrates this rigor. After acquiring Starwood Hotels, Marriott faced a

[55] The Companies Act, No. 18 of 2013, §166, India Code (2013).
[56] E.I. DuPont de Nemours & Co. v. Kolon Indus., 2011 WL 4625760 (E.D. Va. 2011).
[57] KPMG, Cyber Risk and Cross-Border M&A: Global Legal Trends (2023).

massive data breach originating in the acquired entity's system. The UK Information Commissioner's Office imposed a £99 million penalty for failing to detect the breach during the acquisition process, thereby solidifying cyber due diligence as an indispensable legal duty in M&A.[58]

The United Kingdom, through the Data Protection Act, 2018 and the UK GDPR, mandates pre-transaction risk assessments, data mapping, and privacy impact evaluations. The Information Commissioner's Office (ICO) actively enforces these standards. In the Ticketmaster UK Ltd. case (2020), the ICO fined the company £1.25 million for failing to monitor and assess third-party digital vulnerabilities, establishing that acquirers and controllers must conduct thorough cybersecurity vetting. The UK Companies Act, 2006 also extends directors' duties to exercise "reasonable care, skill, and diligence," encompassing oversight of cyber governance during acquisitions. This dual approach-combining statutory duties with fiduciary accountability-sets a governance benchmark for other jurisdictions.[59]

Australia and Singapore represent Asia-Pacific jurisdictions pioneering structured cyber due diligence. Australia's Privacy Act, 1988, as amended by the Privacy Amendment (Notifiable Data Breaches) Act, 2017, mandates notification and accountability for data breaches. The Office of the Australian Information Commissioner (OAIC) has directed companies to perform due diligence assessments before transferring ownership of personal data assets. Similarly, Singapore's Personal Data Protection Act (PDPA) requires acquiring companies to ensure continued compliance by verifying the target's data management frameworks. These jurisdictions demonstrate that cybersecurity diligence is an integral part of transaction structuring and legal compliance, not a post-closing exercise.[60]

International institutions also shape the jurisprudence of cyber due diligence. The Organisation for Economic Co-operation and Development (OECD) in its 2013 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data emphasized corporate responsibility for ensuring privacy continuity during restructuring or acquisition. The United Nations Conference on Trade

[58] In re Marriott International, Inc. Data Breach Litigation, 440 F. Supp. 3d 447 (D. Md. 2020); UK Information Commissioner's Office, Enforcement Notice, Marriott International (2020).
[59] Ticketmaster UK Ltd., ICO Enforcement Notice (2020); UK Companies Act, 2006, §172.
[60] Office of the Australian Information Commissioner, Guidelines on Notifiable Data Breaches (2018); Personal Data Protection Act, No. 26 of 2012 (Singapore).

and Development (UNCTAD), in its 2021 report on digital economy governance, recognized cyber diligence as essential for sustainable foreign direct investment, urging developing nations to embed such obligations in M&A frameworks. These instruments collectively reflect the global trend toward codifying cyber diligence as a component of responsible corporate conduct.[61]

IX. FINDINGS, SUGGESTIONS, AND CONCLUSION

The research establishes that cyber due diligence has emerged as a critical but often neglected component in mergers and acquisitions. Most acquiring firms prioritize financial, legal, and operational due diligence while underestimating the growing significance of cybersecurity assessment. This oversight results in post-acquisition liabilities, data breaches, and erosion of shareholder value. The study finds that despite the proliferation of digital assets and data-driven business models, India's legal framework lacks a dedicated statutory requirement for cyber due diligence in corporate transactions.[62]

The examination of the Indian regulatory ecosystem reveals that existing laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 only provide general obligations regarding data security and personal data protection. They do not impose specific duties on acquirers to conduct cybersecurity vetting before or after acquisitions. Consequently, acquirers often inherit undisclosed data breaches or non-compliance issues, resulting in successor liability and reputational harm. The absence of sector-specific enforcement guidelines exacerbates these vulnerabilities.[63]

Another key finding is that global jurisdictions, particularly the European Union, the United States, and the United Kingdom, have developed advanced regulatory mechanisms linking cybersecurity with corporate responsibility. The EU's General Data Protection Regulation (GDPR) imposes mandatory due diligence obligations, while the U.S. Securities and Exchange Commission (SEC) enforces disclosure-based accountability. These frameworks demonstrate that cyber diligence is

[61] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013); UNCTAD, Digital Economy Report (2021).
[62] Deloitte, Cyber Risk in M&A Transactions: Hidden Liabilities and Legal Exposure (2023).
[63] Information Technology Act, No. 21 of 2000, §43A, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, §33, India Code (2023).

no longer optional-it is a legal and fiduciary expectation tied to investor protection and consumer trust.[64]

Empirical findings show that companies that integrate cyber due diligence into M&A transactions not only mitigate post-acquisition risks but also achieve better integration outcomes. A 2023 PwC survey reported that nearly 60% of deals suffering valuation losses post-merger had overlooked cyber assessments. Cyber negligence during acquisition processes has been linked to valuation adjustments, legal disputes, and compliance penalties. The Verizon–Yahoo and Marriott–Starwood cases illustrate that failing to uncover pre-existing breaches before acquisition can lead to multi-million-dollar losses and regulatory sanctions.[65]

The research also reveals that data localization laws, cloud computing reliance, and cross-border data transfers complicate cyber due diligence. In India, acquirers often face challenges in verifying data storage locations and compliance with global privacy standards. This makes international transactions prone to jurisdictional conflicts, particularly when involving entities subject to GDPR, CCPA, or other foreign data protection regimes. As a result, Indian firms face potential dual liability across multiple jurisdictions.[66]

It is found that the current M&A contracts used in India inadequately address cyber risk. Representations and warranties are often drafted broadly without specific clauses on cybersecurity, data breaches, or regulatory compliance. This contractual vagueness limits acquirers' ability to claim indemnification when cyber incidents arise post-acquisition. Furthermore, the lack of standardized cyber diligence frameworks across industries leads to inconsistent practices and uneven risk exposure among acquirers.[67]

The study underscores that cyber risk is not only a technological issue but a legal and governance challenge. Effective due diligence requires interdisciplinary collaboration involving legal, technical, and compliance professionals. However, most M&A teams in India lack the integrated expertise necessary to evaluate cyber resilience. This professional gap contributes to superficial

[64] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), arts. 24, 32; U.S. Securities and Exchange Commission, Cybersecurity Disclosure Guidance, Release No. 33-10459 (2018).
[65] PwC, Global M&A Cyber Risk Report (2023); Verizon Communications Inc. v. Yahoo! Inc., 2017 M&A Dispute (Del. Ch. 2017).
[66] KPMG, Cross-Border Data Risk Management in M&A Transactions (2022).
[67] EY, Cyber Due Diligence and Contractual Risk Allocation (2023).

diligence processes that overlook structural vulnerabilities, outdated IT systems, or inadequate data protection policies in target entities.[68]

A structured and statutory framework for cyber due diligence in India is essential. The first recommendation is to amend the Information Technology Act, 2000 or the Digital Personal Data Protection Act, 2023 to explicitly mandate cyber risk assessments during mergers and acquisitions. This amendment should require entities to perform security audits, disclose prior data breaches, and certify compliance with prescribed security standards before completion of transactions.[69]

The second suggestion is for SEBI and the Ministry of Corporate Affairs to issue binding guidelines integrating cyber risk evaluation into corporate governance and disclosure obligations. SEBI's LODR framework should mandate listed companies to disclose their cybersecurity preparedness and incident history during acquisitions. The Companies Act can incorporate cyber diligence under directors' duties of care, ensuring that board members are legally accountable for verifying the digital resilience of both acquiring and target entities.[70]

Professional capacity building is also vital. The Institute of Chartered Accountants of India (ICAI) and the Institute of Company Secretaries of India (ICSI) should develop certification programs on cyber due diligence to enhance technical understanding among legal and financial professionals. Specialized training will enable M&A teams to assess cyber risk more effectively, integrating legal and technical perspectives into a unified due diligence model.[71]

Contractual practices in M&A transactions must evolve to include precise representations and warranties on cybersecurity. Agreements should incorporate clauses mandating disclosure of prior cyber incidents, data breach liabilities, and compliance with data protection laws. Indemnity provisions should be explicitly linked to cybersecurity obligations. This ensures equitable allocation of liability between acquirer and seller in the event of undisclosed cyber incidents discovered after deal closure.[72]

[68] IBM, Cost of a Data Breach Report (2023).
[69] Ministry of Electronics and Information Technology, Proposed Amendments to IT Act for Cyber Risk Governance (2024 Draft).
[70] SEBI Circular on Cybersecurity and Cyber Resilience Framework, June 2022.
[71] Institute of Chartered Accountants of India, Handbook on Cyber Risk and Compliance Audits (2023).
[72] Akorn Inc. v. Fresenius Kabi AG, 2018 WL 4719347 (Del. Ch. 2018).

Cyber insurance mechanisms must be encouraged to mitigate financial exposure arising from cyber incidents post-acquisition. Regulators should promote standardized cyber insurance policies that cover breach investigations, regulatory fines, and reputational damage. Making cyber insurance mandatory for high-value M&A transactions will ensure an additional layer of protection for investors and stakeholders.[73]

Finally, there is a pressing need for post-acquisition monitoring mechanisms. Regulators should require acquiring entities to file periodic cyber compliance reports for a defined period after merger completion. This will ensure continued vigilance, enabling early detection of vulnerabilities that may arise during IT system integration. A dedicated oversight mechanism, perhaps under the jurisdiction of CERT-In or the Data Protection Board, could be established to audit post-merger cybersecurity transitions.[74]

Cyber due diligence is now an indispensable component of modern corporate transactions. The increasing dependence on digital assets, data analytics, and networked operations means that a company's cyber health directly influences its valuation and sustainability. The research concludes that the absence of a comprehensive statutory framework in India has left a critical compliance vacuum that exposes acquirers to significant risks. While Indian laws address data protection in general terms, they do not yet impose targeted obligations on cyber due diligence during mergers and acquisitions, leaving enforcement fragmented and inconsistent.[75]

The comparative analysis of the U.S., EU, and UK frameworks demonstrates that effective cyber diligence is grounded in clear legal mandates, regulatory oversight, and board-level accountability. India must adopt similar measures, integrating cyber diligence within its corporate governance architecture. Doing so will align India with global best practices, enhance investor confidence, and protect stakeholders in an increasingly digital economy.

X. BIBLIOGRAPHY

Primary Sources

1. **Statutes and Legislations**

[73] IRDAI, Framework for Cyber Insurance in Corporate Transactions (2023).
[74] CERT-In, Post-Merger Cybersecurity Monitoring Framework (2023).
[75] PwC, Cyber Due Diligence as a Governance Imperative in India (2023).

- The Information Technology Act, No. 21 of 2000, India Code (2000).
- The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
- The Companies Act, No. 18 of 2013, India Code (2013).
- Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.
- SEBI (Prohibition of Insider Trading) Regulations, 2015.
- The General Data Protection Regulation (EU) 2016/679 (GDPR).
- UK Data Protection Act, 2018.
- U.S. Securities and Exchange Commission, *Cybersecurity Disclosure Guidance*, Release No. 33-10459 (2018).
- Cybersecurity Information Sharing Act, Pub. L. No. 114–113, 129 Stat. 2242 (2015) (U.S.).
- California Consumer Privacy Act, Cal. Civ. Code §1798.100 (2018).
- Network and Information Systems (NIS 2) Directive, European Union (2022).
- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).

2. **Cases**

- *Verizon Communications Inc. v. Yahoo! Inc.*, 2017 M&A Dispute (Del. Ch. 2017).
- *In re Marriott International, Inc. Data Breach Litigation*, 440 F. Supp. 3d 447 (D. Md. 2020).
- *Akorn Inc. v. Fresenius Kabi AG*, 2018 WL 4719347 (Del. Ch. 2018).
- *E.I. DuPont de Nemours & Co. v. Kolon Indus.*, 2011 WL 4625760 (E.D. Va. 2011).
- *In re Target Corp. Customer Data Security Breach Litigation*, 66 F. Supp. 3d 1154 (D. Minn. 2014).
- *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
- *Ticketmaster UK Ltd.*, ICO Enforcement Notice (2020).

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
- *Tata Consultancy Services Ltd. v. Cyrus Investments Pvt. Ltd.*, (2021) 9 SCC 449 (India).
- *In re SolarWinds Corp. Securities Litigation*, No. 1:21-cv-00138 (W.D. Tex. 2023).

Secondary Sources

1. Accenture, *Post-Merger Cyber Integration Strategy* (2023).
2. Bain & Co., *Due Diligence in the Digital Age: Redefining Risk Evaluation* (2022).
3. Deloitte, *Cyber Due Diligence Framework for M&A Transactions* (2023).
4. Deloitte, *Cybersecurity in M&A: Managing the Hidden Risk* (2022).
5. EY, *Valuing Cybersecurity: The Financial Dimension of Risk* (2022).
6. EY, *Cyber Due Diligence and Contractual Risk Allocation* (2023).
7. IBM, *Cost of a Data Breach Report* (2023).
8. Institute of Chartered Accountants of India, *Handbook on Cyber Risk and Compliance Audits* (2023).
9. KPMG, *Cyber Due Diligence in M&A Transactions* (2023).
10. KPMG, *Global Cyber Regulations and Cross-Border M&A Compliance* (2023).
11. Ministry of Electronics and Information Technology, *National Cyber Security Policy* (2013).
12. OECD, *Guidelines on Cross-Border Data Governance and Corporate Accountability* (2023).
13. PwC, *Cybersecurity in M&A: Redefining Transaction Value* (2020).
14. PwC, *Cyber Risk Management in Indian Corporate Transactions* (2023).
15. PwC, *Global M&A Cyber Risk Report* (2023).
16. Reserve Bank of India, *Cybersecurity Framework for Banks* (2016).

17. SEBI, *Circular on Cybersecurity and Cyber Resilience Framework for Intermediaries* (June 2022).

18. UNCTAD, *Digital Economy Report* (2021).

19. U.S. House of Representatives, *The Equifax Data Breach: Majority Staff Report* (2018).

20. World Bank, *Cyber Risk and Corporate Governance: Policy Implications for Emerging Economies* (2022).

Books and Journals

1. Solove, Daniel J., and Paul M. Schwartz, *Information Privacy Law* (7th ed., Wolters Kluwer 2023).

2. Bainbridge, Stephen, *Corporate Law and Governance in the Digital Age* (Oxford University Press, 2022).

3. Sharma, Ritu, "Cyber Governance and Corporate Accountability in Indian M&A," *Indian Journal of Law and Technology*, Vol. 19 (2023).

4. Rajan, Meenakshi, "The Legal Imperative of Cyber Due Diligence in M&A Transactions," *NLSIU Law Review*, Vol. 34 (2022).

5. Chawla, Aditya, "Digital Risks and Corporate Governance: Lessons from Global Jurisprudence," *International Journal of Cyber Law and Policy*, Vol. 11 (2023).

6. Kumar, Anant, "The Role of Data Protection in Cross-Border Mergers: A Comparative Analysis," *Journal of Business Law Studies*, Vol. 18 (2022).