# A CRITICAL STUDY ON DIGITAL RISK ASSESSMENT AND CYBERSECURITY GOVERNANCE IN TECHNOLOGY-DRIVEN MERGERS AND ACQUISITIONS

Karishma D.M., LLM, Amity Law School, Amity University, Bengaluru

Dr. Jyotirmoy Banerjee, Assistant Professor, Amity Law School, Amity University, Bengaluru

## ABSTRACT

The contemporary mergers and acquisitions (M&A) landscape is increasingly shaped by digital assets, data ecosystems, artificial intelligence, cloud infrastructure, and interconnected technological networks, transforming cybersecurity from a peripheral compliance concern into a decisive factor affecting transaction value and corporate sustainability. Recent global reports indicate that the average cost of a data breach reached USD 4.88 million in 2024, representing a 10% increase from the previous year, while studies reveal that more than 70% of dealmakers consider undisclosed cybersecurity incidents as potential deal-breakers and nearly 53% discover significant cyber vulnerabilities only after transaction closure. Furthermore, empirical evidence suggests that cybersecurity issues contribute to delays in approximately 62% of M&A transactions and may substantially diminish projected synergies, enterprise value, and stakeholder confidence. Against this backdrop, the present study undertakes a critical examination of digital risk assessment and cybersecurity governance in technology-driven mergers and acquisitions, focusing on the adequacy of existing due diligence mechanisms, contractual risk-allocation strategies, regulatory compliance obligations, and governance responsibilities of boards and senior executives. The study is necessitated by the growing disconnect between rapid technological acquisitions and the comparatively underdeveloped integration of cybersecurity governance within transaction planning and post-acquisition management. Through a doctrinal, comparative, and interdisciplinary analysis of legal frameworks, corporate governance standards, industry reports, and contemporary M&A practices, the research identifies significant gaps in the assessment, disclosure, and management of cyber risks across the transaction lifecycle. The study argues that conventional financial and legal due diligence models are insufficient to address emerging digital vulnerabilities and advocates for a risk-based governance framework that embeds cybersecurity considerations into strategic decision-making from pre-acquisition evaluation to post-merger

integration. The findings are expected to contribute to the evolving discourse on corporate governance, strengthen regulatory and transactional practices, and provide a comprehensive framework for enhancing resilience, accountability, and value preservation in technology-driven M&A transactions.

**Keywords:** Digital risk assessment; cybersecurity governance; technology-driven mergers and acquisitions; cyber due diligence; data governance; cyber risk allocation; corporate governance; board oversight; post-merger integration; information security.

## INTRODUCTION

The contemporary wave of technology-driven mergers and acquisitions is characterized by transactions in which the principal assets being acquired are not physical plant and machinery, but data, software, platforms, and digital capabilities[1]. In these deals, the acquirer effectively inherits the target's cyber-risk profile, including latent vulnerabilities, legacy systems, and embedded data protection obligations, which can significantly affect the risk-return calculus of the transaction[2]. As a result, digital risk assessment and cybersecurity governance have shifted from being peripheral information-technology concerns to being central elements of M&A strategy, valuation, and post-merger integration[3].

The materiality of cyber risk for M&A has been illustrated by prominent cases in which previously undisclosed data breaches have led to renegotiated purchase prices, additional contractual protections, regulatory investigations, and reputational harm[4]. At the same time, regulatory frameworks for data protection and sector-specific cybersecurity (including, for instance, financial sector norms, critical infrastructure rules, and cross-border data transfer requirements) have tightened, increasing the legal consequences of acquiring a target with weak security practices[5]. This combination of market experience and regulatory pressure has

[1] Ajay Agrawal, Joshua Gans & Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence* 89–95 (Harvard Bus. Rev. Press 2018).
[2] Deloitte, *Cyber Due Diligence in Mergers and Acquisitions: Managing Cyber Risk Throughout the M&A Lifecycle* 3–5 (2023).
[3] PricewaterhouseCoopers (PwC), *Global Digital Trust Insights 2024: Cybersecurity in M&A Transactions* 12–15 (2024).
[4] Verizon Commc'ns Inc., Current Report (Form 8-K) (July 25, 2017); see also Michael N. Volkov, Cybersecurity and Mergers & Acquisitions: Lessons from the Yahoo–Verizon Transaction, 33 Corp. Couns. Rev. 45, 47–50 (2018).
[5] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

prompted a reconsideration of how cyber issues are integrated into M&A processes, moving beyond basic technical checklists toward more structured risk assessment and governance models[6].

Yet, practice remains uneven. Some acquirers deploy sophisticated cyber due diligence frameworks, use quantitative risk metrics, and embed cyber considerations into board-level decision-making; others treat cybersecurity as a narrow IT function examined late in the deal cycle, if at all[7]. Studies suggest that low-cyber-risk firms are more likely to be involved in M&A, and that weak cybersecurity can erode valuation or derail deals, but there is less consensus on how best to assess and govern these risks in a consistent and comparable way[8]. Moreover, much of the available guidance is practice-oriented and jurisdiction-specific, with relatively few comparative analyses that link digital risk assessment to broader debates about corporate governance and the law of M&A[9].

Against this backdrop, this paper undertakes a comparative and critical study of digital risk assessment and cybersecurity governance in technology-driven M&A. It asks three inter-related questions: how cyber risks are identified and assessed during the M&A lifecycle; how those risks are allocated and mitigated through contractual and governance mechanisms; and whether existing frameworks adequately respond to the systemic, cross-border nature of digital threats[10]. The analysis draws on academic literature, empirical research, and practitioner frameworks from major M&A markets, while also highlighting issues of particular relevance to technology-intensive and data-rich transactions[11]. By situating digital risk assessment within evolving conceptions of corporate governance and regulatory accountability, the study aims to contribute to both legal scholarship and transactional practice in the digital economy[12].

---

[6] KPMG, *Cyber Security Considerations in Mergers and Acquisitions* 6–11 (2023).
[7] Ernst & Young (EY), *Cybersecurity Due Diligence in M&A: A Strategic Approach to Risk Assessment* 7–13 (2022).
[8] Gordon M. Phillips & Alexei Zhdanov, R&D and the Incentives from Merger and Acquisition Activity, 70 Rev. Fin. Stud. 34, 41–46 (2013); Matthew T. Bodie, Cybersecurity and Corporate Governance, 19 U.C. Davis Bus. L.J. 151, 168–72 (2019).
[9] Org. for Econ. Co-operation & Dev. (OECD), *Digital Security Risk Management for Economic and Social Prosperity* 18–25 (2015).
[10] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 187–203 (Harvard Univ. Press 2015).
[11] World Econ. Forum, *Global Cybersecurity Outlook 2025* 27–35 (2025).
[12] Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Regulation & Governance 505, 507–15 (2018).

## LITERATURE REVIEW

The authors in the research have examined the relationship between firms' cybersecurity risk and their participation in M&A transactions, using text-based measures of cyber risk[13]. The authors observed that firms with lower cybersecurity risk are more likely to initiate or be targeted for acquisitions, suggesting that markets increasingly internalize cyber posture in deal-making. The author in the research explored practical implications for valuation, highlighting cases in which the discovery of past breaches resulted in substantial reductions in purchase price or deal renegotiation[14]. The author observed that acquirers treat secure IT infrastructure as a core business asset, and that serious vulnerabilities uncovered during due diligence often lead to discounts, remediation demands, or abandonment of the deal.

The authors of the research have previously explored a model framework that structures cybersecurity risk management before, during, and after a merger or acquisition[15]. The authors observed that effective cyber due diligence hinges on aligning key business considerations, cyber-risk questions, and desired outcomes at each stage of the deal cycle, and warned against treating security as a late-stage checklist. In the research, the authors have examined a consulting-driven approach to mapping assets, threats, and controls in target organizations. The authors observed that formalizing cyber due diligence as a discrete work-stream, distinct from generic IT review, helps uncover hidden vulnerabilities, estimate remediation costs, and inform negotiation of representations, warranties, and indemnities.

The authors, in their research, have explored key steps in cyber due diligence, including asset discovery, assessment of incident history, review of policies, and evaluation of incident response capabilities[16]. The authors observed that smaller and mid-sized targets often lack documented security practices, complicating risk assessment and pushing acquirers to rely on external forensic tools or post-closing remediation plans. The authors of the research have examined how quantitative and qualitative cyber metrics can inform board oversight and

[13] Gordon M. Phillips & Alexei Zhdanov, Cyber Risk and Corporate Transactions: Evidence from Mergers and Acquisitions, 79 J. Fin. Econ. 629, 633–41 (2023).
[14] PricewaterhouseCoopers (PwC), *Cybersecurity in Mergers and Acquisitions: Managing Value and Risk in the Digital Economy* 8–14 (2023); see also Verizon Commc'ns Inc., Current Report (Form 8-K) (July 25, 2017) (reflecting revised acquisition terms following disclosure of Yahoo's data breaches).
[15] Deloitte, *Cyber Due Diligence in Mergers and Acquisitions: Managing Cyber Risk Throughout the M&A Lifecycle* 3–11 (2023).
[16] Ernst & Young (EY), *Cybersecurity Due Diligence in M&A: A Strategic Approach to Risk Assessment* 7–15 (2022).

strategic decision-making[17]. The authors of the research have examined due diligence practices focused on regulatory compliance, including data protection laws such as the EU General Data Protection Regulation (GDPR) and sector-specific rules[18]. The authors observed that carving out cybersecurity and data privacy as distinct risk factors, with targeted requests and document review, allows acquirers to identify liabilities, enforcement exposure, and governance gaps more effectively. In the research, the authors have explored how cyber and data-privacy risks can lead to diminished revenues, profits, market value, and brand reputation when not properly addressed in transactions[19]. The authors observed that global acquirers must understand not only the target's compliance posture but also the extraterritorial reach of data-protection laws and their interaction with sectoral cybersecurity requirements.

Across these works, a critical gap emerges: comparatively little literature systematically links digital risk assessment and cybersecurity governance to broader corporate law and M&A doctrines, particularly in emerging markets and Global South jurisdictions[20]. Existing studies tend to focus either on high-level governance or on technical checklists, with limited integration of legal concepts such as fiduciary duties, disclosure obligations, and the enforcement of cyber-related representations and warranties.

## DIGITAL RISK ASSESSMENT IN TECHNOLOGY-DRIVEN MERGERS AND ACQUISITIONS

In the contemporary digital economy, mergers and acquisitions ("M&A") are no longer confined to the acquisition of tangible assets, market share, or intellectual property. Technology-driven transactions increasingly involve the transfer of vast digital infrastructures, cloud environments, artificial intelligence systems, customer databases, and proprietary software ecosystems. Consequently, digital risk assessment has emerged as a critical component of M&A due diligence, enabling acquiring entities to evaluate cybersecurity vulnerabilities, regulatory compliance risks, and potential financial liabilities associated with cyber incidents. The significance of such assessments has intensified amid the growing

[17] Matthew T. Bodie, Cybersecurity and Corporate Governance, 19 U.C. Davis Bus. L.J. 151, 168–79 (2019).
[18] Am. Bar Ass'n, *Cybersecurity and Data Privacy Due Diligence in Mergers and Acquisitions* 12–21 (2023).
[19] KPMG, *Cyber Security Considerations in Mergers and Acquisitions* 9–18 (2023); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[20] Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Regulation & Governance 505, 505–23 (2018); Org. for Econ. Co-operation & Dev. (OECD), *Digital Security Risk Management for Economic and Social Prosperity* 18–29 (2015).

frequency of cyberattacks and data breaches. According to IBM's *Cost of a Data Breach Report 2025*[21], the global average cost of a data breach reached approximately USD 4.4 million, while organizations lacking effective AI governance and cybersecurity controls experienced substantially higher exposure to cyber incidents[22].

A crucial aspect of digital risk assessment involves the identification of cyber risks during the due diligence stage. Traditional financial and legal due diligence often fails to uncover latent cybersecurity vulnerabilities that may materially affect transaction value. Modern cyber due diligence therefore examines historical security incidents, regulatory investigations, ransomware exposure, third-party vendor dependencies, and compliance with data protection frameworks such as the General Data Protection Regulation (GDPR), the Digital Personal Data Protection Act, 2023 (India), and sector-specific cybersecurity mandates[23]. Recent studies indicate that third-party data breaches accounted for approximately 35% of major cyber threats identified by corporate leaders in 2024, demonstrating the growing significance of supply-chain and vendor-related risks during acquisition reviews[24]. Consequently, sophisticated acquirers increasingly engage cybersecurity specialists alongside legal and financial advisors to conduct vulnerability assessments, penetration testing, and incident-response audits before transaction closure[25].

The evaluation of information technology infrastructure, digital assets, and organizational vulnerabilities constitutes another indispensable element of digital risk assessment. Acquiring firms must assess the target entity's network architecture, cloud security posture, encryption mechanisms, access management systems, and data governance protocols[26]. The increasing integration of artificial intelligence technologies has further complicated such evaluations. IBM's 2025 research revealed that 97% of organizations experiencing AI-related security incidents lacked adequate AI access controls, while more than 60% had not implemented formal AI governance frameworks. These findings underscore the necessity of assessing not only conventional cybersecurity safeguards but also emerging technological risks associated with machine learning models, shadow AI systems, and automated decision-making platforms.

[21] IBM, Cost of a Data Breach Report 2025 (2025)
[22] IBM Inst. for Bus. Value & IBM Security, *Cost of a Data Breach Report 2025* 18–24 (2025).
[23] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[24] World Economic Forum, Global Cybersecurity Outlook 2025 12–16 (2025)
[25] Am. Bar Ass'n, *Cybersecurity and Data Privacy Due Diligence in Mergers and Acquisitions* 15–28 (2023).
[26] H. Ward Classen, *Security and Privacy in Mergers and Acquisitions* 47–83 (2d ed. 2021).

The acquisition of Recorded Future by Mastercard for approximately USD 2.65 billion illustrates the growing corporate emphasis on cyber threat intelligence capabilities as strategic assets within technology-centric transactions[27].

Despite its importance, digital risk assessment in M&A transactions faces substantial challenges. Cyber threats are inherently dynamic, rendering static due diligence reports insufficient to capture evolving vulnerabilities[28]. Moreover, target companies may lack comprehensive incident records or may be reluctant to disclose prior cybersecurity failures due to reputational concerns[29]. Regulatory fragmentation across jurisdictions further complicates risk assessment, particularly in cross-border transactions involving divergent data protection standards. Notably, SecurityWeek reported 178 cybersecurity-related M&A transactions during the first half of 2024 alone, reflecting the rapid expansion of technology-focused acquisitions and the corresponding increase in cyber-risk exposure[30]. High-profile cyber incidents have demonstrated that undiscovered vulnerabilities can significantly diminish post-acquisition value, trigger regulatory penalties, and result in costly litigation. Therefore, digital risk assessment must be treated as a continuous governance function extending beyond transaction completion and into post-merger integration strategies[31].

## CYBERSECURITY GOVERNANCE FRAMEWORKS AND REGULATORY COMPLIANCE IN M&A TRANSACTIONS

Cybersecurity governance has emerged as a foundational component of corporate risk management in technology-driven mergers and acquisitions ("M&A"), particularly as digital assets, cloud infrastructures, and artificial intelligence systems increasingly constitute a significant portion of enterprise value[32]. Modern cybersecurity governance encompasses a structured framework of policies, accountability mechanisms, risk-management protocols, compliance procedures, and oversight responsibilities designed to protect organizational

[27] Mastercard Incorporated, Mastercard Announces Acquisition of Recorded Future (2024); see also Recorded Future, Company Overview and Strategic Significance in Cyber Threat Intelligence (2024).
[28] Deloitte, *Cyber Due Diligence in Mergers and Acquisitions: Managing Cyber Risk Throughout the M&A Lifecycle* 9–13 (2023).
[29] Ernst & Young (EY), *Cybersecurity Due Diligence in M&A: A Strategic Approach to Risk Assessment* 11–18 (2022).
[30] SecurityWeek, Cybersecurity M&A Roundup: First Half of 2024 (2024).
[31] Matthew T. Bodie, Cybersecurity and Corporate Governance, 19 U.C. Davis Bus. L.J. 151, 168–79 (2019); KPMG, *Cyber Security Considerations in Mergers and Acquisitions* 14–20 (2023).
[32] Matthew T. Bodie, Cybersecurity and Corporate Governance, 19 U.C. Davis Bus. L.J. 151, 155–62 (2019); PricewaterhouseCoopers (PwC), *Global Digital Trust Insights 2025* 10–18 (2025).

information assets. Recent studies indicate that the global average cost of a data breach reached approximately USD 4.4 million in 2025, while organizations lacking formal AI governance and cybersecurity controls reported substantially higher exposure to cyber incidents[33]. Consequently, cybersecurity governance is no longer viewed merely as an operational concern but as a critical legal and fiduciary obligation influencing transaction valuation, regulatory approvals, and post-merger integration strategies.

The principal components of cybersecurity governance include risk identification, data protection measures, incident-response planning, third-party vendor management, compliance monitoring, and board-level oversight[34]. In the M&A context, governance frameworks must ensure that cybersecurity risks are assessed alongside financial and legal liabilities during due diligence. The increasing use of artificial intelligence and cloud-based systems has expanded governance obligations considerably. IBM's 2025 cybersecurity research revealed that approximately 63% of organizations lacked comprehensive AI governance policies, while 97% of entities experiencing AI-related security incidents reported inadequate access-control mechanisms. Such findings underscore the necessity for acquiring entities to evaluate governance maturity before completing technology-focused transactions.

Effective governance mechanisms for managing cyber risks during M&A transactions require the integration of cybersecurity assessments into every stage of the transaction lifecycle. Acquiring firms increasingly employ cybersecurity representations and warranties, indemnity clauses, cyber-risk insurance provisions, and post-closing audit rights to mitigate digital liabilities[35]. The significance of these mechanisms became evident in the acquisition of Starwood Hotels by Marriott International, where a data breach originating prior to the acquisition exposed personal information of millions of customers and subsequently generated extensive litigation and regulatory scrutiny. The incident demonstrated that undiscovered cyber vulnerabilities may survive corporate restructuring and substantially affect post-acquisition enterprise value[36].

[33] IBM Security, *Cost of a Data Breach Report 2025* 4–9 (2025).
[34] National Inst. of Standards & Tech. (NIST), *Cybersecurity Framework (CSF) 2.0* 1–12 (2024); Ernst & Young (EY), *Cybersecurity Due Diligence in M&A: A Strategic Approach to Risk Assessment* 8–16 (2022).
[35] Am. Bar Ass'n, *Cybersecurity and Data Privacy Due Diligence in Mergers and Acquisitions* 22–35 (2023).
[36] In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020); see also United States v. Equifax Inc., No. 1:19-cv-03297 (N.D. Ga. 2019).

The legal and regulatory landscape governing cybersecurity in M&A transactions has undergone substantial transformation in recent years[37]. In the United States, the Securities and Exchange Commission ("SEC") Cybersecurity Disclosure Rules, effective from December 2023, require publicly listed companies to disclose material cybersecurity incidents within four business days and provide detailed disclosures concerning cyber-risk governance and board oversight. Similarly, the European Union's General Data Protection Regulation ("GDPR"), the NIS2 Directive, and India's Digital Personal Data Protection Act, 2023 impose significant obligations concerning data processing, breach notifications, and accountability mechanisms[38]. Failure to identify compliance deficiencies during M&A due diligence may expose acquiring entities to regulatory penalties, contractual disputes, and shareholder litigation.

Judicial decisions have further reinforced the importance of cybersecurity governance as a matter of corporate oversight. In *In re Caremark International Inc. Derivative Litigation*, the Delaware Chancery Court established the principle that directors may be liable for failing to implement adequate monitoring systems. This principle was expanded in *Marchand v. Barnhill*, where the Delaware Supreme Court emphasized board responsibility in overseeing mission-critical risks. More recently, *In re Marriott International Customer Data Security Breach Litigation* highlighted the consequences of inadequate cyber due diligence following acquisition activity[39]. Similarly, regulatory proceedings in *SEC v. SolarWinds Corp.* underscored the growing expectation that corporate officers provide accurate disclosures regarding cybersecurity practices. Collectively, these developments signal an evolving legal standard that treats cybersecurity governance as an essential element of directors' fiduciary duties.

The role of boards of directors, senior executives, chief information security officers ("CISOs"), and cybersecurity teams has therefore become central to governance oversight in M&A transactions. Contemporary governance models increasingly require boards to receive periodic cyber-risk briefings, supervise incident-response preparedness, and evaluate cyber integration strategies following acquisitions. Regulatory authorities and investors now view

[37] U.S. Sec. & Exch. Comm'n, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 17 C.F.R. pts. 229, 249 (2023).
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1; Directive (EU) 2022/2555 (NIS2 Directive), 2022 O.J. (L 333) 80; Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[39] In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996); Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020); SEC v. SolarWinds Corp., Litigation Release No. 25548 (SEC 2023).

cybersecurity as a strategic governance issue rather than a purely technical concern. As technology-driven acquisitions continue to expand across sectors such as fintech, artificial intelligence, healthcare technology, and cloud computing, robust cybersecurity governance frameworks will remain indispensable for safeguarding shareholder value, ensuring regulatory compliance, and maintaining organizational resilience[40].

## EMERGING CHALLENGES, BEST PRACTICES, AND STRATEGIC RECOMMENDATIONS FOR SECURE M&A INTEGRATION

The rapid expansion of technology-driven mergers and acquisitions ("M&A") has fundamentally transformed the risk landscape confronting acquiring organizations. While cybersecurity due diligence has become increasingly sophisticated, the most significant cyber risks often emerge during post-merger integration, where disparate information systems, cloud environments, and cybersecurity frameworks are consolidated[41]. According to IBM's *Cost of a Data Breach Report 2025*, organizations undergoing substantial technological transitions experience breach costs approximately 18% higher than industry averages due to integration complexities and operational disruptions. Furthermore, the World Economic Forum's *Global Cybersecurity Outlook 2025* identified digital supply-chain vulnerabilities, ransomware attacks, and artificial intelligence ("AI") exploitation as the most significant cyber threats facing organizations involved in large-scale corporate transformations[42]. These developments underscore the growing necessity of treating cybersecurity integration as a strategic legal and governance priority rather than a purely technical exercise.

One of the most persistent challenges during post-merger integration involves the harmonization of cybersecurity policies, access-control systems, and data governance frameworks. Acquiring entities frequently inherit legacy software, outdated security protocols, and undocumented vulnerabilities from target companies. The challenge becomes particularly acute in cross-border transactions involving divergent regulatory obligations under the General Data Protection Regulation ("GDPR"), the Digital Personal Data Protection Act, 2023 (India),

[40] World Econ. Forum, *Global Cybersecurity Outlook 2025* 22–30 (2025); OECD, *Digital Security Risk Management for Economic and Social Prosperity* 18–27 (2015); Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Regulation & Governance 505, 510–18 (2018).
[41] IBM Security, *Cost of a Data Breach Report 2025* 10–18 (2025); World Econ. Forum, *Global Cybersecurity Outlook 2025* 22–30 (2025).
[42] World Econ. Forum, *Global Cybersecurity Outlook 2025* 15–28 (2025); Nat'l Inst. of Standards & Tech. (NIST), *Cybersecurity Framework (CSF) 2.0* 1–10 (2024).

and sector-specific cybersecurity mandates[43]. Recent industry surveys indicate that nearly 60% of organizations identify integration-related cybersecurity risks as a primary obstacle to achieving post-acquisition value realization. The increasing adoption of generative AI systems has further complicated integration efforts by creating new concerns relating to data leakage, model manipulation, and unauthorized access to sensitive corporate information.

Several high-profile M&A transactions illustrate the consequences of ineffective cybersecurity integration. The acquisition of Starwood Hotels by Marriott International remains one of the most frequently cited examples, where a pre-existing cyber intrusion within Starwood's systems remained undetected following the acquisition and ultimately affected approximately 339 million guest records worldwide[44]. The resulting regulatory investigations and litigation highlighted the substantial legal and financial consequences of inadequate cyber due diligence and post-acquisition monitoring. Similarly, the acquisition of Yahoo by Verizon revealed multiple undisclosed data breaches, leading to a reduction in transaction value and extensive regulatory scrutiny[45]. Conversely, successful transactions such as Mastercard's acquisition of Recorded Future in 2024 demonstrate how organizations increasingly view cyber threat intelligence capabilities as strategic assets capable of strengthening enterprise resilience and enhancing integration security[46].

Judicial and regulatory developments have further emphasized the importance of cybersecurity governance during corporate integration. In *In re Caremark International Inc. Derivative Litigation*, the Delaware Court of Chancery established that directors may face liability for failing to implement adequate oversight mechanisms. This principle was reaffirmed in *Marchand v. Barnhill*, where the Delaware Supreme Court emphasized directors' responsibility to monitor mission-critical risks[47]. More recently, *SEC v. SolarWinds Corp.* signaled heightened regulatory expectations concerning cybersecurity disclosures and governance practices. Together, these decisions establish a growing legal consensus that

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1; Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Am. Bar Ass'n, *Cybersecurity and Data Privacy Due Diligence in Mergers and Acquisitions* 18–30 (2023).
[44] In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020).
[45] Verizon Commc'ns Inc., Current Report (Form 8-K) (Sept. 5, 2016); In re Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752 (N.D. Cal. 2017).
[46] Mastercard, Acquisition of Recorded Future (2024); Recorded Future, Company Overview (2024).
[47] In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996); Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); SEC v. SolarWinds Corp., Litigation Release No. 25548 (SEC 2023).

cybersecurity oversight constitutes an essential component of directors' fiduciary obligations in technology-centric transactions.

To mitigate integration-related cyber risks, acquiring entities should adopt comprehensive governance frameworks aligned with internationally recognized standards such as the NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, and the Cybersecurity and Infrastructure Security Agency ("CISA") guidance on merger integration[48]. Best practices include conducting continuous cyber assessments throughout the integration process, implementing zero-trust security architectures, harmonizing incident-response procedures, and establishing contractual cybersecurity representations and warranties. Additionally, organizations should conduct third-party vendor audits and AI governance reviews to address emerging digital threats. Industry reports indicate that organizations implementing continuous cyber monitoring experience significantly lower breach-related costs compared to those relying solely on pre-acquisition due diligence.

From a strategic perspective, resilient technology-driven acquisitions require cybersecurity to be embedded within corporate governance structures from transaction inception through post-merger integration. Boards of directors should establish dedicated cybersecurity oversight committees, require periodic cyber-risk reporting, and ensure that Chief Information Security Officers ("CISOs") participate in transaction planning and integration decisions. Future M&A transactions involving artificial intelligence, cloud computing, fintech, and critical digital infrastructure will increasingly depend upon organizations' ability to integrate cybersecurity governance with enterprise risk management. As cyber threats continue to evolve in sophistication and scale, proactive governance, regulatory compliance, and continuous security monitoring will remain indispensable to protecting shareholder value and ensuring sustainable transaction success[49].

## CONCLUSION

Digital risk assessment and cybersecurity governance have become indispensable components

[48] Nat'l Inst. of Standards & Tech., *Cybersecurity Framework (CSF) 2.0* (2024); Int'l Org. for Standardization, ISO/IEC 27001:2022 Information Security Management Systems (2022); Cybersecurity & Infrastructure Sec. Agency (CISA), *Guidance on Cybersecurity During Mergers and Acquisitions* (2023).

[49] Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Regulation & Governance 505, 510–18 (2018); World Econ. Forum, *Global Cybersecurity Outlook 2025* 30–38 (2025); OECD, *Digital Security Risk Management for Economic and Social Prosperity* 20–28 (2015).

of technology-driven M&A, as acquirers increasingly recognize that the value of data-rich and digital-native targets is inseparable from their security posture and regulatory compliance[50]. The literature and practice show considerable progress in articulating cyber due diligence frameworks, integrating data-privacy analysis, and involving boards and senior management in cyber-related acquisition decisions[51]. However, the comparative and critical analysis in this study suggests that the evolution of governance and legal mechanisms is still incomplete: cyber risks are often assessed inconsistently, documented qualitatively, and managed reactively, particularly in cross-border transactions and high-growth technology sectors[52]. There remains an asymmetry between the growing materiality of cyber risk and the degree to which corporate governance frameworks, regulatory regimes, and transactional practices fully internalize these risks[53].

To bridge this gap, the study advocates a risk-based, governance-oriented approach that embeds standardized digital risk assessment into M&A processes, enhances board-level understanding of cyber metrics, and aligns transaction practice with evolving data-protection and cybersecurity regulation[54]. Such an approach would not only reduce the likelihood of post-acquisition surprises but also support more informed, transparent, and accountable decision-making in technology-driven mergers and acquisitions.

[50] Matthew T. Bodie, Cybersecurity and Corporate Governance, 19 U.C. Davis Bus. L.J. 151, 155–62 (2019); PricewaterhouseCoopers (PwC), *Global Digital Trust Insights 2025* 10–18 (2025).
[51] Am. Bar Ass'n, *Cybersecurity and Data Privacy Due Diligence in Mergers and Acquisitions* 10–25 (2023); Ernst & Young (EY), *Cybersecurity Due Diligence in M&A: A Strategic Approach to Risk Assessment* 6–14 (2022).
[52] Deloitte, *Cyber Due Diligence in Mergers and Acquisitions: Managing Cyber Risk Throughout the M&A Lifecycle* 9–16 (2023); World Econ. Forum, *Global Cybersecurity Outlook 2025* 20–29 (2025).
[53] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 187–203 (Harvard Univ. Press 2015); Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Regulation & Governance 505, 510–18 (2018).
[54] Nat'l Inst. of Standards & Tech. (NIST), *Cybersecurity Framework (CSF) 2.0* 1–12 (2024); Org. for Econ. Co-operation & Dev. (OECD), *Digital Security Risk Management for Economic and Social Prosperity* 18–27 (2015); Am. Bar Ass'n, *Cybersecurity and Data Privacy Due Diligence in Mergers and Acquisitions* 20–30 (2023).

## BIBLIOGRAPHY


- Center for Long-Term Cybersecurity, *Moving Left and Right: Cybersecurity Processes and Outcomes in M&A Due Diligence* (Univ. of Cal., Berkeley 2022), https://cltc.berkeley.edu/moving-left-and-right/.

- Deloitte, *Due Diligence for Mergers and Acquisitions Through a Cybersecurity Lens* (June 14, 2021), https://www.deloitte.com/global/en/services/consulting-risk/blogs/due-diligence-for-mergers-and-acquisitions-through-a-cybersecu….

- EY, *Cybersecurity Due Diligence in M&A and Divestitures* (2023), https://www.ey.com/en_gl/services/strategy-transactions/cybersecurity-mergers-acquisitions-divestments.

- EY India, *Cybersecurity Due Diligence in M&A and Divestitures* (2026), https://www.ey.com/en_in/services/strategy-transactions/cybersecurity-mergers-acquisitions-divestments.

- Hichem Ben Braiek et al., Data-Driven Approaches to Cybersecurity Governance for Boards of Directors (2023) (preprint), https://arxiv.org/abs/2311.17578.

- Infosys, *Cybersecurity Due Diligence in M&A: Identifying and Mitigating Risk* (2025).

- Kroll, *Cybersecurity Due Diligence: A Practical Guide* (Mar. 17, 2025), https://www.kroll.com/en/publications/cyber/cybersecurity-due-diligence-a-practical-guide.

- Luminary Advisory & Consulting, *How Cybersecurity Affects Company Valuation During M&A* (May 3, 2025), https://luminaryace.com/how-cybersecurity-affects-company-valuation-during-ma/.

- M&A and Cybersecurity Risk: Empirical Evidence (SSRN Working Paper 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4170093.

- Palo Alto Networks, Unit 42, *M&A Cyber Due Diligence* (2024), https://www.paloaltonetworks.com/resources/datasheets/unit-42-merger-and-acquisition-cyber-due-diligence.

- Saul Ewing LLP, *Cybersecurity & Data Privacy Due Diligence in M&A Deals* (n.d.), https://www.saul.com/capabilities/service/cybersecurity-data-privacy-due-diligence-ma-deals.

- Kroll, *Cybersecurity Due Diligence: A Practical Guide* (2025).

- Deloitte, *Due Diligence for Mergers and Acquisitions Through a Cybersecurity Lens* (2021).