INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 3 | 2025 Art. 66

Critical Study on Strengthening Corporate Governance to Combat Insider Trading and Cyber Crime in Digital Finance Era

Sreelakshmi PR
LLM Student,
Amity Law School, Amity University, Bengaluru

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

Recommended Citation
Sreelakshmi PR and Jyotirmoy Banerjee, *Critical Study on Strengthening Corporate Governance to Combat Insider Trading and Cyber Crime in Digital Finance Era*, 4 IJHRLR 929-940 (2025).
Available at www.humanrightlawreview.in/archives/.

Critical Study on Strengthening Corporate Governance to Combat Insider Trading and Cyber Crime in Digital Finance Era

Sreelakshmi PR
LLM Student,
Amity Law School, Amity University, Bengaluru

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

Manuscript Received	Manuscript Accepted	Manuscript Published
04 June 2025	06 June 2025	08 June 2025

ABSTRACT

In the rapidly evolving digital finance era, the convergence of technology and financial markets has brought unprecedented opportunities as well as critical vulnerabilities. Among the most pressing threats are insider trading and cybercrime, both of which undermine market integrity, erode investor confidence, and compromise regulatory effectiveness. This study undertakes a critical analysis of corporate governance mechanisms to evaluate and enhance their capacity to prevent and respond to these challenges in a technologically driven financial ecosystem. Insider trading, characterized by the misuse of privileged information, continues to plague securities markets, despite existing legal frameworks. Meanwhile, the surge in digital transactions, cloud-based financial operations, and algorithmic trading has exposed organizations to sophisticated cyberattacks, including data breaches, ransomware, and financial fraud. These crimes often intersect, with cyber intrusions facilitating unauthorized access to sensitive market data. The study explores the regulatory responses in India and compares them with global best practices to identify gaps and recommend reforms. Emphasis is placed on the role of board oversight, the effectiveness of internal compliance systems, cybersecurity governance, and the integration of emerging technologies such as artificial intelligence, blockchain, and smart contracts for real-time monitoring and auditability. The research adopts a multidisciplinary approach, blending doctrinal analysis

with empirical insights drawn from recent cases, regulatory reports, and expert interviews. It argues for a paradigm shift in corporate governance—moving from a reactive compliance model to a proactive, tech-enabled risk management framework. Key recommendations include mandatory cybersecurity audits, enhanced whistleblower protections, cross-border regulatory collaboration, and the institutionalization of ethical corporate cultures. By critically examining the interplay between governance, insider threats, and cyber risks, the study seeks to contribute to the development of a resilient, transparent, and secure digital financial environment in India, aligning it with international standards and investor expectations.

KEYWORDS

Corporate Governance, Insider Trading, Cyber Crimes, Digital Finance, Fintech, Regulatory Framework

INTRODUCTION

The digital transformation of the financial sector has fundamentally reshaped the global economic landscape, introducing both significant efficiencies and unprecedented risks. In India, the rise of digital finance—spurred by innovations such as online banking, mobile wallets, cryptocurrency platforms, and algorithmic trading—has increased the complexity and scale of financial operations. However, this shift has also magnified two persistent threats to financial market integrity: insider trading and cybercrime. These dual challenges demand a robust and adaptive corporate governance framework that can effectively mitigate emerging risks while promoting ethical, transparent, and accountable financial practices.

Insider trading, defined as the illicit use of unpublished price-sensitive information (UPSI) for personal gain, continues to undermine investor confidence and market fairness. Despite regulatory mechanisms such as the SEBI (Prohibition of Insider Trading) Regulations, 2015, enforcement challenges persist, particularly in the face of rapidly evolving digital communication channels (SEBI, 2015).[1]

[1] Mandavi Jayakar, *SEBI's authority to regulate Global Depository Receipts, traded on overseas exchange: Supreme Court's analysis in Securities and Exchange Board of India versus Pan Asia Advisors Ltd. and Ors.*, 6 JINDAL GLOBAL LAW REVIEW 255–263 (2015), http://link.springer.com/10.1007/s41020-015-0012-5.

Simultaneously, cybercrime in the financial sector has seen a dramatic escalation. According to the Reserve Bank of India (RBI, 2020), financial institutions reported a steep rise in cyber incidents, including phishing, identity theft, ransomware attacks, and unauthorized data access. These not only result in direct financial losses but also pose reputational and systemic risks to financial markets.[2]

Corporate governance serves as the first line of defense against these threats by promoting sound risk management, ethical decision-making, and accountability. However, traditional governance structures—often reactive and compliance-driven—may no longer suffice in the digital era. Scholars like Solomon (2020) argue for a shift toward strategic governance, integrating technology, predictive analytics, and real-time surveillance into corporate oversight functions.[3]

This study critically examines how corporate governance frameworks in India can be strengthened to combat insider trading and cybercrime in the digital finance era. It draws from national and international best practices, regulatory policies, and technological advancements to propose a forward-looking governance model aligned with the realities of a digital economy.

CONCEPTUAL FRAMEWORK AND LEGAL FOUNDATIONS

This article establishes the conceptual underpinnings of the research by defining the primary constructs—corporate governance, insider trading, and cybercrime—and contextualizing their interrelationship within the digital finance ecosystem. As financial markets become increasingly reliant on technology, these concepts have grown more interconnected and complex, necessitating a comprehensive theoretical and legal examination.

Corporate Governance refers to the system of rules, practices, and processes through which companies are directed and controlled. It embodies the mechanisms by which corporations balance the interests of a diverse range of stakeholders, including shareholders, management, customers, suppliers, financiers, government, and the community. The fundamental principles of corporate governance—accountability, transparency, responsibility, and fairness—are essential to maintaining the

[2] Ashishbhai Chitranjan Mehta, *Indian banking and role of Reserve Bank of India*, 9 SAARJ JOURNAL ON BANKING & INSURANCE RESEARCH 5 (2020), http://www.indianjournals.com/ijor.aspx?target=ijor:sjbir&volume=9&issue=4&article=001 (last visited Jun 4, 2025).

[3] JILL ATKINS, CORPORATE GOVERNANCE AND ACCOUNTABILITY (Wiley Fifth Edition) (2021).

integrity of financial systems and ensuring sustainable business practices. As the Organisation for Economic Co-operation and Development (OECD) notes, sound corporate governance is critical to market confidence, capital formation, and economic growth.[4]

In the traditional context, corporate governance focused primarily on financial disclosures, board structures, and shareholder rights. However, the rise of digital finance—characterized by online trading platforms, algorithmic investment tools, digital payment systems, and the proliferation of cryptocurrencies—has significantly broadened the scope of governance responsibilities. These developments have introduced new vectors for financial misconduct, including insider trading and cybercrime, that challenge existing regulatory frameworks.

Insider Trading involves the illegal practice of trading on the stock exchange to one's own advantage through access to confidential, non-public information. It distorts market fairness and violates fiduciary duties. In India, the SEBI (Prohibition of Insider Trading) Regulations, 2015, lay down the regulatory framework for curbing this offense.[5] However, in the digital era, identifying and prosecuting insider trading has become more difficult, with the use of encrypted communication channels, decentralized platforms, and sophisticated data mining techniques.

Cybercrime, in the context of digital finance, refers to illegal activities that exploit information and communication technologies to compromise financial systems. These include hacking, phishing, data breaches, ransomware attacks, and identity theft. According to the Reserve Bank of India (RBI), the banking and financial sector has witnessed a sharp increase in reported cyber incidents, which not only cause financial losses but also disrupt market operations and damage public confidence.[6]

Given the convergence of these risks, corporate governance must evolve to include robust digital risk management strategies. This involves integrating cybersecurity policies, real-time compliance monitoring, AI-based surveillance systems, and internal controls that can detect and prevent both insider and external threats. It also necessitates a shift in corporate culture, emphasizing ethical

[4] G20/OECD PRINCIPLES OF CORPORATE GOVERNANCE (OECD ed., OECD) (2015).
[5] Sankalp Jain, *Sahara India Real Estate Corp. Ltd. vs. Securities and Exchange Board of India: A Case Study*, SSRN ELECTRONIC JOURNAL (2015), https://www.ssrn.com/abstract=2799913.
[6] Reserve Bank of India, *Report on Trends and Progress of Banking in India 2020–21* (Dec. 28, 2021).

behavior and technological accountability.

The legal foundation for such transformation lies in the interplay of multiple regulatory instruments, including the Companies Act, 2013,[7]SEBI regulations,[8]and the Information Technology Act, 2000.[9]These frameworks must now be interpreted and applied through the lens of digital resilience and financial innovation.

REGULATORY LANDSCAPE AND LEGAL FRAMEWORKS

The regulatory architecture of corporate governance, insider trading, and cybercrime in the digital finance era is multifaceted and continuously evolving. In India, this landscape is primarily governed by statutory enactments, regulatory guidelines, and sectoral oversight mechanisms, while international practices further inform policy development and harmonization.

- ***Corporate Governance in India***

  Corporate governance in India is chiefly regulated by the Companies Act, 2013, which provides the statutory foundation for board composition, audit committees, director responsibilities, and internal financial controls.[10] The Act emphasizes transparency, accountability, and equitable treatment of stakeholders. It mandates key governance practices such as the constitution of independent directors, vigil mechanisms, and financial disclosures.

  The SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (LODR Regulations) supplement the Companies Act by imposing specific obligations on listed entities.[11]These include norms for board independence, regular disclosure of financial information, related-party transactions, and adherence to the code of conduct. SEBI, in its capacity as the capital markets regulator, also issues periodic circulars to promote ethical corporate behavior and market integrity.

  Furthermore, the Ministry of Corporate Affairs (MCA) plays a pivotal role in issuing guidelines and amending rules to reflect best governance practices. These institutional frameworks

[7] Companies Act, No. 18 of 2013, INDIA CODE (Ministry of Law and Justice, India).
[8] Securities and Exchange Board of India Act, No. 15 of 1992, INDIA CODE.
[9] Information Technology Act, No. 21 of 2000, INDIA CODE.
[10] Companies Act, No. 18 of 2013, § 149–177, INDIA CODE (Ministry of Law and Justice, India).
[11] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, Gazette Notification No. SEBI/LAD-NRO/GN/2015-16/013.

collectively aim to foster investor protection, fair conduct, and sound financial stewardship.

- ***International Regulatory Frameworks***

Globally, corporate governance is shaped by several legislative and normative frameworks. The Sarbanes-Oxley Act, 2002 (SOX) in the United States was enacted in response to corporate fraud and mandates rigorous internal controls, board accountability, and auditor independence.[12]The Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010 introduced stronger whistleblower protections and systemic risk oversight.[13]

In the United Kingdom, the UK Corporate Governance Code sets high standards for leadership, board effectiveness, risk management, and remuneration policies.[14]The OECD Principles of Corporate Governance (2015) are widely regarded as a global benchmark, promoting transparency, stakeholder engagement, and investor rights.[15]These instruments influence domestic laws and set expectations for multinational corporations operating across jurisdictions.

- ***Insider Trading Regulations***

In India, insider trading is governed by the SEBI (Prohibition of Insider Trading) Regulations, 2015. These regulations prohibit the trading of securities on the basis of unpublished price-sensitive information (UPSI) and enforce disclosure obligations for insiders.[16]They also require listed entities to formulate a Code of Conduct to regulate, monitor, and report trading by designated persons.

---

[12] *Corporate Law. Congress Passes Corporate and Accounting Fraud Legislation. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (Codified in Scattered Sections of 11, 15, 18, 28, and 29 U. S. C.)*, 116 HARVARD LAW REVIEW 728 (2002), https://www.jstor.org/stable/1342618?origin=crossref.

[13] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

[14] Mohamed Khaled Eldaly & Magdy Abdel-Kader, *How to regain public trust in audit firms? The case of the Financial Reporting Council*, 31 ACCOUNTING RESEARCH JOURNAL 343–359 (2018), https://www.emerald.com/insight/content/doi/10.1108/ARJ-11-2015-0134/full/html (last visited Jun 4, 2025).

[15] OECD, *G20/OECD Principles of Corporate Governance* (2015).

[16] H Chitimira, *An overview analysis of selected challenges in the enforcement of the prohibition of insider trading and market manipulation in the European Union and South African regulatory frameworks*, 19 LAW, DEMOCRACY & DEVELOPMENT 94 (2015), http://www.ajol.info/index.php/ldd/article/view/122595 (last visited Jun 4, 2025).

In the United States, Rule 10b-5 under the Securities Exchange Act of 1934 criminalizes fraud or deceit in connection with the purchase or sale of securities, forming the cornerstone of insider trading enforcement.[17]The United Kingdom addresses insider trading through the Market Abuse Regulation (MAR), which imposes civil and criminal liabilities for unlawful disclosure and market manipulation.[18]

- ***Cybercrime Regulation***

Cybersecurity and digital finance crimes in India fall under the Information Technology Act, 2000, which addresses hacking, data theft, identity fraud, and unauthorized access.[19]The Reserve Bank of India (RBI) issues cybersecurity guidelines applicable to financial institutions, focusing on risk assessment, incident response, and secure IT governance.[20]Additionally, the Indian Computer Emergency Response Team (CERT-In) operates under the Ministry of Electronics and Information Technology (MeitY) and provides national-level oversight for cyber incidents.

Internationally, the Computer Fraud and Abuse Act (CFAA) in the U.S. criminalizes unauthorized access to computer systems.[21]The Federal Financial Institutions Examination Council (FFIEC) offers guidelines for cybersecurity resilience in financial entities. In the European Union, the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) Directive ensure data privacy and cybersecurity readiness.[22]

REGULATORY CHALLENGES IN THE DIGITAL FINANCE ERA

[17] 17 C.F.R. § 240.10b-5 (2023).
[18] Carmine Di Noia et al., *Issuers obligations under the new Market Abuse Regulation and the proposed ESMA guideline regime: a brief overview*, 26 ZEITSCHRIFT FÜR BANKRECHT UND BANKWIRTSCHAFT 96–107 (2014), https://www.degruyter.com/document/doi/10.15375/zbb-2014-0202/html.
[19] LAW RELATING TO COMPUTERS, INTERNET AND E-COMMERCE: A GUIDE TO CYBERLAWS AND THE INFORMATION TECHNOLOGY ACT, 2000 WITH RULES, REGULATIONS AND NOTIFICATIONS (N. Kamath ed., Universal Law Publ 2. ed., updated repr) (2005)
[20] LAW RELATING TO COMPUTERS, INTERNET AND E-COMMERCE: A GUIDE TO CYBERLAWS AND THE INFORMATION TECHNOLOGY ACT, 2000 WITH RULES, REGULATIONS AND NOTIFICATIONS (N. Kamath ed., Universal Law Publ 2. ed., updated repr) (2005)
[21] *USA: Preliminary Injunction on basis of Computer Fraud and Abuse Act*, 23 COMPUTER LAW REVIEW INTERNATIONAL 75–82 (2022), https://www.degruyter.com/document/doi/10.9785/cri-2022-230304/html
[22] General Data Protection Regulation, Regulation (EU) 2016/679; Directive (EU) 2016/1148 on security of network and information systems.

Emerging digital technologies such as blockchain, fintech platforms, and cryptocurrencies present novel regulatory dilemmas. In India, regulatory jurisdiction is fragmented—RBI supervises digital payments and stablecoins, SEBI monitors securities-related crypto-assets, and MeitY handles digital infrastructure. However, the lack of a unified legal framework complicates effective governance. Globally, the Financial Action Task Force (FATF) provides guidance on combating the misuse of virtual assets for money laundering and terrorist financing.[23] Emerging digital technologies—particularly blockchain, fintech platforms, and cryptocurrencies—have transformed the global financial ecosystem, offering enhanced speed, transparency, and efficiency. However, they also present complex regulatory challenges, especially in jurisdictions like India where institutional oversight is fragmented. The Reserve Bank of India (RBI) governs digital payments and has expressed concerns about private cryptocurrencies and their potential impact on monetary stability. Simultaneously, the Securities and Exchange Board of India (SEBI) oversees crypto-assets deemed securities, while the Ministry of Electronics and Information Technology (MeitY) is tasked with managing the underlying digital infrastructure and cybersecurity concerns. This division of authority leads to overlapping mandates, regulatory arbitrage, and gaps in enforcement—ultimately undermining coherent governance of digital financial systems.

On the international front, organizations such as the Financial Action Task Force (FATF) have stepped in to provide soft-law norms and guidelines aimed at preventing the misuse of virtual assets for money laundering and terrorist financing. However, global enforcement remains a significant challenge due to disparate national legal standards, the borderless nature of blockchain technologies, and the pseudonymous identities of users. Countries vary in their definitions, classifications, and legal treatment of crypto-assets, which complicates mutual legal assistance, data sharing, and extradition procedures.

Given the rapid evolution of digital financial innovations, India and other nations must prioritize inter-agency collaboration, regulatory harmonization, and the development of adaptive legal frameworks. Key measures should include establishing a centralized digital regulatory authority, creating risk-based licensing regimes, and engaging in bilateral and multilateral

[23] *Estimating Fair Market Value of Petroleum Assets in Nigeria: A Risk-Based Approach*, *in* SPE NIGERIA ANNUAL INTERNATIONAL CONFERENCE AND EXHIBITION D031S022R001, https://onepetro.org/SPENAIC/proceedings/21NAIC/21NAIC/D031S022R001/465527.

agreements for data exchange and legal enforcement. Furthermore, capacity building within enforcement and judicial agencies is essential to ensure technological literacy. The future of digital finance governance depends on the ability of regulators to balance innovation with consumer protection, financial stability, and national security, while participating in a globally synchronized effort to manage digital financial ecosystems.

STRENGTHENING GOVERNANCE AGAINST CYBER CRIMES IN DIGITAL FINANCE

The increasing reliance on digital platforms in financial services has fundamentally reshaped the operational and regulatory landscape. Innovations such as cryptocurrencies, fintech platforms, online trading, and digital payment systems offer greater speed and accessibility but have simultaneously increased exposure to cyber threats such as phishing, ransomware, and data breaches.[24]These threats pose serious risks to financial integrity, consumer trust, and legal compliance, thereby elevating cybersecurity to a critical component of corporate governance.

Cybersecurity is no longer a back-end technical issue but a strategic governance matter. Boards of directors must incorporate cyber risk oversight as part of enterprise-wide risk management.[25] Regular updates on cyber posture, threat intelligence, and incident response must be discussed at the board level. A strong internal control system—including firewalls, encryption, secure authentication, and employee awareness training—is essential to defend against increasingly sophisticated attacks.[26]

In the Indian context, the Information Technology Act, 2000 criminalizes unauthorized access, data theft, and cyber fraud, forming the legal backbone of cybersecurity regulation.[27]The RBI Cybersecurity Framework (2016) requires banks to conduct periodic risk assessments, implement robust IT controls, and report cyber incidents promptly.[28] The CERT-In (Indian Computer Emergency Response Team) provides national-level threat monitoring and response support. Additionally, companies must align with international norms such as the General Data Protection Regulation (GDPR), especially when dealing with cross-

[24] Ioannis Zografopoulos et al., *Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations*, 17 IEEE SYSTEMS JOURNAL 6695–6709 (2023), ttps://ieeexplore.ieee.org/document/10238347/.
[25] Solomon, J., *Corporate Governance and Accountability* (5th ed. 2020).
[26] ISO/IEC 27001:2022, *Information Security Management Systems.*
[27] Information Technology Act, No. 21 of 2000, INDIA CODE.
[28] RBI, *Cyber Security Framework in Banks* (2016).

border data or global partners.[29]

Technological safeguards must complement legal compliance. Measures such as multi-factor authentication, blockchain for transaction integrity, and penetration testing are vital. Cyber due diligence should be embedded in mergers, acquisitions, and vendor assessments to prevent inherited vulnerabilities.[30] Companies should also maintain a Cyber Incident Response Plan (CIRP) that outlines steps for detection, containment, and recovery—minimizing damage and ensuring business continuity. The cybersecurity governance also demands ethical leadership. Boards must foster a culture of transparency, accountability, and awareness. Appointing a Chief Information Security Officer (CISO) and ensuring board access to cybersecurity expertise can significantly enhance oversight and readiness.

CONCLUSION

This article synthesizes the key insights from the study on strengthening corporate governance to combat insider trading and cyber crimes in the digital finance era. As financial markets evolve with the proliferation of fintech innovations, cryptocurrencies, and digital trading platforms, corporate governance must adapt to address the sophisticated risks emerging in this dynamic environment.The findings reveal that, although legal and regulatory frameworks—such as India's *Companies Act, 2013*, *SEBI (Prohibition of Insider Trading) Regulations, 2015*, the *Information Technology Act, 2000*, and global instruments like the *Sarbanes-Oxley Act* or *GDPR*—have made substantial progress, enforcement challenges persist. These include delays in surveillance mechanisms, fragmented regulatory jurisdictions, and technological gaps that cybercriminals and market manipulators continue to exploit. Insider trading remains difficult to detect and prosecute, while cyber crimes have escalated in frequency and impact due to the vulnerabilities introduced by digital financial systems.

The study underscores the imperative for integrated governance models that align legal compliance with technological resilience and ethical oversight. A proactive approach involves embedding cybersecurity into corporate governance frameworks, enhancing board-level awareness, and implementing real-time surveillance systems powered by emerging technologies such as AI and blockchain. Moreover, cross-sector collaboration among financial institutions, regulators, law enforcement agencies, and cybersecurity experts is crucial to ensuring responsive and

[29] General Data Protection Regulation, Regulation (EU) 2016/679.
[30] EY, *Cybersecurity Due Diligence in M&A* (2020)

holistic risk mitigation.A central takeaway is the need for interdisciplinary engagement—blending legal analysis, financial risk assessment, and technological innovation—to design agile, forward-looking governance systems. Such collaboration can bolster transparency, foster investor confidence, and reinforce the credibility of capital markets in the digital age. A central takeaway is the need for interdisciplinary engagement blending legal analysis, financial risk assessment, and technological innovation—to design agile, forward-looking governance systems. Such collaboration can bolster transparency, foster investor confidence, and reinforce the credibility of capital markets in the digital age. This research contributes to the academic and policy discourse by critically exploring how corporate governance can evolve in response to insider trading and cyber threats in digital finance. It offers actionable insights for regulators, policymakers, and corporate leaders aiming to build robust institutional frameworks that uphold market integrity, ensure stakeholder protection, and sustain public trust in a rapidly digitizing global economy.