ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

Cyber Governance and Financial Responsibility in Digital Organizations: Developing an Integrated Cyber-Risk Governance Framework for Indian Listed Companies

Dr. Santanu Kumar Das
P.G. Department of Management Studies, Roland Institute of Technology, Affiliated to BPUT, Surya Vihar, Golanthara; Berhampur; Odisha

Prof. (Dr.) Manas Pandey
Professor& Head,Department of Business Economics, Faculty of Management Studies; Veer Bahadur Singh Purvanchal University, Jaunpur, Uttar Pradesh

Abstract
The swift digitization of businesses has revolutionized how Indian publicly listed firms utilize their financial resources, engage with stakeholders, and generate value in an organizational context. The increased reliance on digital facilities has exposed corporations to cyber-attacks, data thefts, ransomware, and financial scams. Henceforth, cybersecurity is no longer just an issue for IT but has turned into a significant part of corporate governance and financial accountability. The research work aims to explore the relationship between cyber governance and financial accountability in Indian listed firms, covering board supervision, cyber-risk, internal control issues, governance of cybersecurity investment, and compliance and reporting. It proposes an Integrated Cyber Risk Governance Framework to help firms align cybersecurity decisions with financial governance.
In this study, a quantitative and cross-sectional research design is recommended. The research uses responses from the directors, CFOs, CISOs, risk managers, internal auditors and compliance officers of the listed firms in India, followed by analysis through SEM. A representative dataset is used for this, which shows that all of the five dimensions of cyber-governance are good predictors of financial accountability. In this regard, the dataset shows that the cyber-risk management proves to be the strongest set of predictors of financial responsibility. Thus, the contribution of this research is both the theoretical and practical insertion of cyber governance into the framework of financial responsibility, thereby building the governing framework suitable for digitally dependent listed companies.

Keywords:
Cyber Governance, Cyber Risk, Financial Responsibility, Corporate Governance, Cybersecurity, Listed Companies, Risk Management, Governance Framework

1. Introduction

Digital changeover currently plays a crucial role in the business approaches of today. Indian businesses are using cloud-based systems, cashless payments, enterprise solutions, artificial intelligence, data analysis, and sophisticated online finance solution technologies more often. In addition to enhancing efficiency and providing opportunities for growth, digitalization has become the factor increasing organizational risk.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

Cyber crimes have important outcomes far beyond the scope of the technical sphere. A successful cyber attack may result in interruptions to operations, compromises in confidentiality, direct losses, increased regulatory expenditure, harm to reputation, and reduced confidence of investors. Cyber risk has thus become a topic for governance discussion for boards of directors, executive management, audits and risk committees, and finance offices.

Financial responsibility goes far beyond traditional financial reporting, as it involves rational use of organizational resources, asset protection, transparency, internal accountability, compliance with regulations, and value creation for stakeholders. In organizations characterized by heavy digitalization, cyber security and financial responsibility cannot be separated, since cyber security deficiency influences revenues, expenses, assets, liabilities, and sustainability in the long-run.

Despite growing importance of cyber threats, many companies still view cybersecurity mainly as a technical issue and do not connect cyber-risks to financial ones. This research suggests that cyber governance should be included in corporate governance systems used by Indian publicly traded companies and creates a system linking cyber oversight at the board level, cyber-risk management, internal controls, cybersecurity investments, compliance, and reporting, with financial responsibility.

2. Background information

The development of e-companies changed the nature of corporate risks. Traditional risks received new facets gaining their development through cyber risks — it makes cyber incidents a simultaneous operational, financial, legal, reputational, and strategic risk.

The impact on public companies is particularly strong because the performance is monitored by various stakeholders including shareholders, institutional investors, regulators, creditors, and analysts all the time. Week cyber governance can therefore have an impact on information assets, as well as on the credibility and financial standing of the company. Proper cyber governance implies that responsibilities are defined: the board receives information about the main cyber risks; the management carries out cyber risk management; internal control explores threats; and financial decision makers do not forget about the cyber risks while making decisions on allocating resources.

This study argues that financial responsibility in the digital organization means proper governance of cyber risks. Cybersecurity expenditures, internal controls, risk management, compliance, and disclosure should be regarded not only as technological solutions but also as the elements of financial responsibility.

3. Statement of the Research Problem

The rise in digitalization has posed not only numerous opportunities for Indian public firms but also has resulted in risks coming due to cyber activities, like financial losses, interference in business activity, fines imposed by regulatory bodies, costs of litigation, and damage to reputation. It should be noted that although important outcomes can occur due to cyber risk, the issue of governance is treated separately from the issue of financial accountability. A serious issue of governance is that there is not enough integration between cyber security governance at the level of the board and making financial decisions. In many companies, making investments in cyber security is driven mainly by technical needs, with not enough attention paid to financial risk, whereas finance departments usually do not have enough knowledge of the cyber threats, and keeping in mind that internal control systems and reporting systems do not focus on the financial aspects of cyber incidents.

4. Review of Literature

Today’s research looks at cyber security as a problem of corporate governance rather than an isolated IT problem, noting the roles of board supervision, cyber security information disclosure, cyber risk management, and the implications of cyber governance.

The study done by Modi, Kuzminykh and Ghita (2023): shows that most boards do not have the right type of metrics and information regarding cybersecurity, which renders their decision lacking. According to the findings of Hydari, Liang and Telang (2024), there is no uniform revenue drop after breach disclosure which raises questions about the assumption that such cases automatically result in financial losses. Akhtar and Akhtar (2024) said that the area of cyber governance is becoming more important but still lacks theoretical development. The study undertaken by Oktavendi and Kholmi (2024) mentions that cybersecurity disclosure has implications for stakeholders and investors whereas

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

the findings of the research conducted by Dinkova et al. (2024): indicate that there is a positive correlation between investment into cybersecurity and financial performance. Al-Somali et al. (2024) linked the notion of cybersecurity systems to sustainability in business due to the concept of resilience.

Tan, Guo, and Zhang (2025) showed that cybersecurity governance contributes to increase in market value through the increase in confidence of investors and supply chain partners, while Barsky and Pearlson (2025) pointed to a mismatch between the amount of money allocated to cybersecurity and the knowledge of the board. The study conducted in 2025 demonstrated that better governance and knowledge in cybersecurity are related to better disclosure, but symbolic governance significantly reduces efficiency. Mansour et al. (2026) studied the effect of cybersecurity disclosure and governance on the performance of the company, while Bello and Yahaya (2026) created the Cybersecurity Governance Index, which is based on such financial indicators as ROA, ROE, and Tobin´s Q.

4.1 Synthesis. Various publications indicate a shift in viewpoint from considering cybersecurity as merely a technical task to realizing it as strategic governance accountability due to the emergence of various themes such as oversight by the Board of Directors, disclosure/transparency, cyber awareness/acumen of (a) Board of Directors and the linkage between cyber governance and financial/market outcomes. Nevertheless, there is no synergy between these themes, and they are studied independently or as separate issues rather than a holistic model.

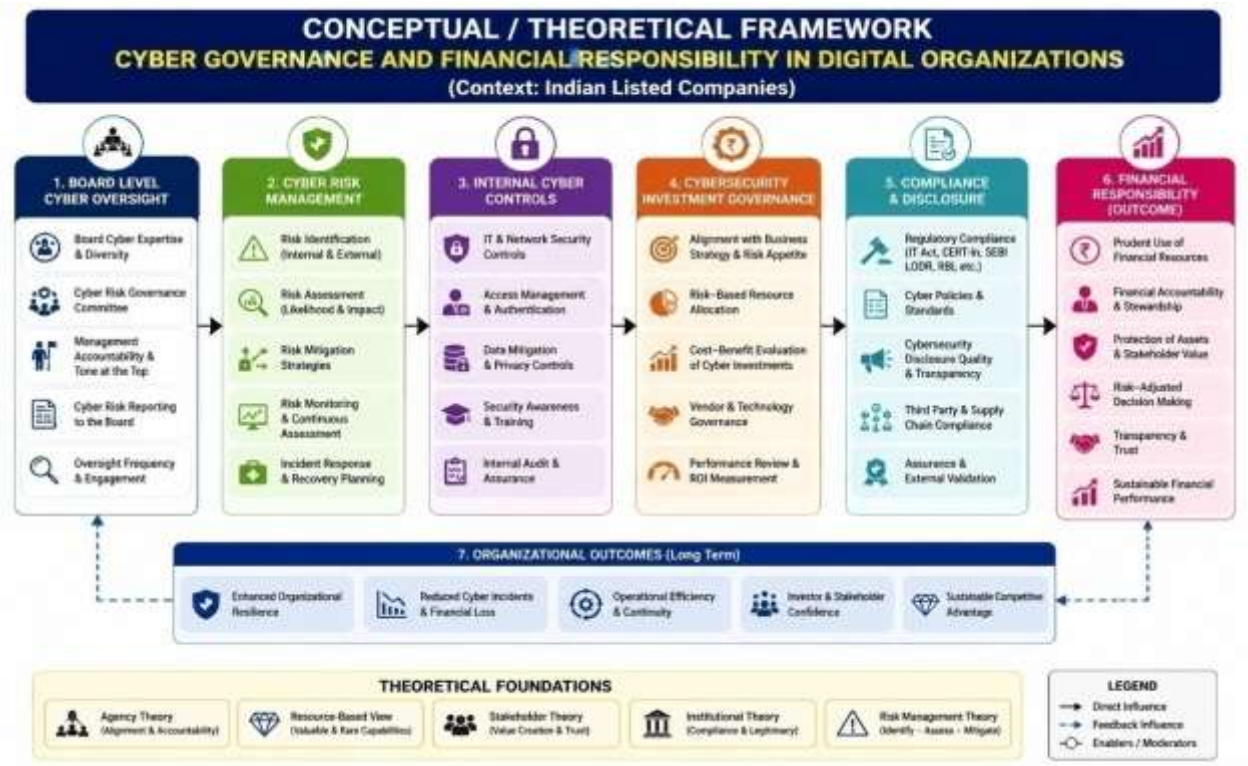
4.2 Research Gap. Although cybersecurity has started to be understood as a governance matter, the current literature remains fragmented, relating to oversight by the Board of Directors, disclosure, investment, risk management, and organizations' performance but often based on only financial performance/firm value as an outcome variable. The overall concept of financial accountability—consisting of accountability, being transparent, resource-efficient, asset-protecting, risk-adjusted decision-making, and safeguarding value of stakeholders—has been much less analyzed, and the empirical evidence regarding listed companies in India is underdeveloped. Thus, there is a significant gap in the development and empirical assessment of an integrated cyber-risk governance model, connecting these aspects to the financial accountability.

4.3 Contribution. The essential contribution of the research is in creating and testing the Integrated Cyber-Risk Governance Framework, which explains how board control, management of cyber risks, internal control, governance of the investments in cybersecurity, as well as compliance/disclosure work in combination in strengthening financial accountability of the Indian listed companies. This brings the contribution of the research to a higher level, beyond just being able to determine the influence of cybersecurity on financial performance.

4.4 Positioning in Comparison to Past Studies. Earlier studies have typically analyzed individual factors independently—for example, one study examined board features, another one looked into quality of disclosures, and a third addressed investment amounts—employing outcome indicators like corporate wealth, stock prices, or accounting profitability. Very few studies capture board supervision, risk control, internal control, investment governance, and disclosure at the same time and even fewer ones do it in the context of publicly listed companies in India, where the introduction of rules of the Securities Exchange Board of India (SEBI) regarding the Cybersecurity and Cyber Resilience Framework (CSCRF) made cyber governance essential. In this research, different dimensions are put in one single metric and structural model, providing methodological and theoretical contribution to the literature by creating a guide for future researchers focusing on corporate governance in less developed countries.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

5. Conceptual and Theoretical Framework



The framework clarifies the significance of cyber governance in ensuring accountability for financial operations of the Indian companies listed on stock exchanges by incorporating cyber security into corporate governance, enterprise risk management and stakeholder accountability. The five dimensions of cyber governance are merged into one, and effects of such merger are discussed.

Board-Level Cyber Oversight denotes the contribution of the board of directors in defining strategic direction in respect of cyber risk management, provided that it involves relevant cyber competences, establishing the oversight mechanisms, holding management accountable, and fixing the schedule for reporting. Agency theory presumes that effective cyber risk oversight helps eliminate asymmetry in information between the management and shareholders and ensures accountability.

Cyber Risk Management involves any systematic methodology in terms of identifying, assessing, mitigating, monitoring and responding to the cyber threats. This transforms cyber security from pure technical activity into enterprise risk management method, aimed at minimizing unexpected financial losses.

Internal Cyber Controls consist of IT security systems, ensuring access management, authentication, protection of information, employee training and internal audit. Internal controls ensure unsafe access, cyber fraud or information loss.

Cybersecurity Investment Governance stresses the importance of managing cybersecurity expenditures in terms of the associated risks, strategies, and benefits, borrowing from the Resource-Based Theory, which posits that governance capability is a sustainable source of benefits.

Compliance and Disclosure concerns compliance with legislation and the degree of cybersecurity transparency. Institutional Theory portrays organizational responses to legislative, industry, and investor demands, with compliance being an important contributor to legitimacy and credibility.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

Financial Responsibility, which is the main independent construct, can be defined broadly in terms of the efficient use of resources, responsibility for resource management, risk-adjusted decision-making, transparency, and responsibility for stakeholder value creation. According to the main premise of the study, improved cyber governance situates responsible financial decisions through uncovering cyber-related risks before those risks turn into real losses.

Additionally, it is important to note that the framework identifies long-term organizational outcomes that are: resilience, continuity of operations, trust of stakeholders, and sustainable competitive advantage, which is being backed jointly by five theories, namely Agency Theory, Stakeholder Theory, Resource-Based View, Institutional Theory, and Risk Management Theory.

The proposed relationship can be summarized as follows:
Cyber Oversight by Board Level → Cyber Risk Management → Internal Controls Related to Cybersecurity → Governance of Cybersecurity Investments → Compliance and Disclosure → Financial Accountability → Organizational Resilience and Sustainable Value

6: Research Questions

RQ1: What is the impact of board-level oversight in the field of cybersecurity on financial accountability within companies listed in India?
RQ2: To what extent is the practice of managing cyber risks helpful in obtaining financial responsibility in companies that rely heavily on electronic devices?
RQ3: What is the effect of internal controls in the area of cybersecurity in securing the financial resources and the assets of the organization?
RQ4: What is the significance of governance, compliance, and disclosure in the field of investments into cybersecurity in promoting financial accountability?
RQ5: What measures could be put in place while developing an effective model of governance in the field of cyber risk management for companies listed in India?

7. Research Objectives

RO1: To explore how board-level cyber oversight affects financial responsibility of publicly-listed firms in India.
RO2: To investigate the role of cyber risk management on financial accountability of Indian listed firms that use the internet.
RO3: To assess the effect of internal cyber controls on safeguarding corporate finances and assets.
RO4: To scrutinize how governance of cybersecurity investments, compliance, and disclosure contributes to financial responsibility.
RO5: To create a framework for cyber risk management and test it statistically in terms of its ability to improve financial responsibility among listed firms in India.

8. Research Methodology

8.1 Methodology of the Research Study

The quantitative, descriptive and explanatory research design has been selected for this investigation in order to find the link between cyber governance and financial responsibility of listed firms in India. As for the descriptive part of the research, it will describe the current practices regarding cyber-risk governance, and the explanatory part will find out whether different dimensions of cyber governance really impact financial responsibility significantly.
The research will be based on the assumption that cyber governance is a multidimensional capability of the organization which consists of such elements as cyber oversight of the board, cyber-risk management, internal cyber controls, governance of cybersecurity investments and compliance and disclosures. All of these elements are supposed to play a significant role in responsible financial management.
The adoption of a cross-sectional research design in this investigation will find its justification in the fact that the primary data will be gathered during a certain time period from professionals of organizations.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

8.2 Research Approach

For the purpose of this study, a deductive research approach will be adopted. The theoretical foundations for the research will be formulated from theories such as Agency theory, Stakeholder theory, Resource-based view, Institutional theory, and Risk management theory. The theoretical foundations will be developed into a conceptual framework and research hypotheses that can be tested.

The hypotheses formulated would be tested empirically through data that would be collected from professional workers in the Indian listed companies. This method helps to move from the theoretical foundation to empirical tests.

8.3 Research Context

The research is centered around the Indian listed companies working in a digital environment. Listed companies are selected as their governance structures contain higher expectations regarding transparency, accountability, risk management, internal control, and protection of stakeholders.

The study will examine the companies from various sectors instead of restricting the study to one industry. This method can help the research capture the variety in cyber governance practices because of differences in business models, digitalization, organization size and risk.

8.4 Target Population: The sample consists of the members of the board and senior employees including CIOs, CISOs, CFOs, finance managers, risk specialists, internal auditors, specialists in the sphere of information security, compliance officers, and senior managers.

8.5 Sampling:A purposeful sampling approach will be applied, choosing respondents with cyber governance knowledge and skills in decision-making for finances. The target sample should have 350–500 valid answers, starting from 300 at least for SEM analysis.

8.6 Data Sources: For primary data, a structured questionnaire will be used, while for secondary one – annual reports, corporate governance disclosure reports, ESG reports, regulatory documents, and investors' presentations will be used for further context provision of the primary data.

8.7 Instrument: The structured questionnaire will consist of two parts: (A) the profile of respondent and organization (age, qualifications, experience, role in organization, industry of organization, its size, and participation in decision-making process) and (B) the measurement of constructs with help of five-point Likert Scale (from 1 – Strongly Disagree to 5 – Strongly Agree).

8.8 Pilot Study: About 30–50 respondents will take part in pilot research, and item clarity and relevance will be checked. Ambiguous and poorly loaded items will be improved or deleted, and preliminary reliability will be assessed.

8.9: Validity & Reliability: Content validity will be determined by an expert review; construct validity by EFA and CFA; convergent validity by factor loadings, Composite Reliability (CR) and Average Variance Extracted (AVE); and discriminant validity by Fornell-Larcker Criterion, HTMT ratio and cross-loadings. The internal consistency will be determined by Cronbach's Alpha (acceptable > 0.70) and Composite Reliability, both at pilot and final stages.

8.10: Data Collection and Screening: The data will be gathered via online/structured questionnaire, where participation is voluntary and confidential. Prior to analysis, the data will be screened for missing values, duplicates, non-respondents, outliers, and common-method variance.

8.11: Data Analysis Approach: The analysis will be conducted in the order of descriptive statistics; EFA (KMO, Bartlett's Test, eigenvalues, variance explained, rotated component matrix); CFA (factor loadings, CR, AVE, convergent/discriminant validity, model fit); and Structural Equation Modeling (SEM), which will be the core method, and testing of the five direct relationships between cyber governance variables and financial responsibility, and the second-order model (Cyber Governance ->

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

Financial Responsibility). The model fit will be determined by χ^2/df, CFI, TLI, RMSEA, SRMR, and GFI. Hypotheses will be tested with standardized path coefficients, t-values and p-values (α=.05).

8.12: Further Analysis and Ethics: Mediation analysis through bootstrapping could analyze the organization's resilience as a mediator variable, while multigroup analysis could analyze variations based on the size, industry, and maturity of governance in the organizations. Method commonality will be handled using both procedures (anonymity, use of neutral language, and separate sections) and statistical methods (Harman's one factor test and latent method factor analysis). The study will conduct research in compliance with research ethics (voluntary participation and confidentiality).

9. Data Analysis and Interpretation

To illustrate the suggested analytical approach, we are utilizing a descriptive data set consisting of 400 authentic responses measuring five dimensions of cyber governance—Board-Level Cyber Oversight, Cyber-Risk Management, Internal Cyber Controls, Cybersecurity Investment Governance, and Compliance & Disclosure—and Financial Responsibility being the dependent variable.

Table 1: Demographic Profile (N = 400, selected)

Variable	Category	Frequency	Percentage
Gender	Male	276	69.0
	Female	124	31.1
Age	Below 30 years	58	14.5
	30–40 years	126	31.5
	41–50 years	137	34.5
	Above 50 years	79	19.7
Professional Experience	Below 5 years	46	11.5
	5–10 years	103	25.8
	11-15 years	132	33.0
	Above 15 years	119	29.7
Functional Area	Finance/Accounts	104	26.0
	IT/Cybersecurity	91	22.8
	Risk/Compliance	73	18.3
	Audit/Governance	68	17.0
	Senior Management/Other	64	16.0

As many as 63% of the participants report over ten years in the profession, and the population is broad, including realms like finance, cybersecurity, risk, compliance, audit, as well as senior management, meaning there is a multidisciplinary representation.

Table 2: Descriptive Statistics

Construct	Mean	SD
Board-Level Cyber Oversight	3.84	0.71
Cyber-Risk Management	3.91	0.70
Internal Cyber Controls	3.88	0.69
Cybersecurity Investment Governance	3.72	0.76
Compliance & Disclosure	3.79	0.73
Financial Responsibility	3.86	0.68

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

The results show that all variables score more than the midpoint on the scale. The variable 'Cyber-Risk Management' has the highest average, indicating that there are already established risk practices. Meanwhile, the variable 'Cybersecurity Investment Governance' is lower than its counterpart.

Table 3: Reliability

Construct	Cronbach's α	CR
Board-Level Cyber Oversight (BCO)	0.891	0.916
Cyber-Risk Management (CRM)	0.904	0.928
Internal Cyber Controls (ICC)	0.912	0.934
Cybersecurity Investment Governance (CIG)	0.883	0.909
Compliance & Disclosure (CD)	0.896	0.919
Financial Responsibility (FR)	0.918	0.938

The ratio of α and CR variables exceeds the accepted limit of internal consistency.
9.2 KMO & Bartlett's Test. KMO = 0.934; Bartlett's $\chi^2 = 4862.42$, df = 435, $p < .001$, meaning that the data is appropriate for conducting factor analysis.

9.3 Exploratory Factor Analysis (EFA) / Confirmatory Factor Analysis (CFA) / Discriminant Validity. EFA has produced six factors which comply with the theoretical model and have accounted for 71.46% of variance in data. Lastly, results of CFA prove that the standardized loadings of the factors range from 0.71 to 0.91, while the CR exceeds 0.90 and AVE is higher than 0.66 for all constructs which indicates the satisfactory level of convergent validity.
The square root of Average Variance Extracted (AVE) for every construct is greater than the correlations for the other constructs according to Fornell and Larcker's criteria thus confirming discriminant validity.

9.4: Correlation Analysis: All indicators of cyber-governance have a positive and statistically significant relationship with financial responsibility with the range of r= 0,62-0,71, p=0,01. Cyber Risk Management is the most relevant indicator of financial responsibility followed by Compliance & Disclosure and Internal Cyber Controls.

Table 4: SEM Path Coefficients

Hypothesis	Path	β	p	Decision
H1	BCO → FR	0.18	< .001	Supported
H2	CRM → FR	0.29	< .001	Supported
H3	ICC → FR	0.22	< .001	Supported
H4	CIG → FR	0.15	.002	Supported
H5	CD → FR	0.24	< .001	Supported

The analysis included five dimensions, all of which had a positive influence on Financial Accountability. The effect of Cyber-Risk Management was determined to be the strongest (β = 0.29) followed by Compliance & Disclosure (β = 0.24), Internal Cyber Controls (β = 0.22), Board Cyber Oversight (β = 0.18), and lastly, Cybersecurity Investment Governance (β = 0.15).

9.5: Fit of the Model. $\chi^2/df = 2.41$, CFI = 0.946, TLI = 0.938, RMSEA = 0.060, SRMR = 0.047, GFI = 0.918, which indicates good fit of the model overall.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

9.6: Variance Explained. R^2 for Financial Responsibility is 0.68, meaning that the five dimensions of cyber governance can explain around 68% of the variance of the construct – quite a notable explanatory force, considering that the rest 32% can be attributed to other organizational, financial or environmental factors.

9.7: Overall Interpretation. Cyber-Risk Management is the most powerful predictor followed by Compliance & Disclosure, Internal Cyber Controls, Board Cyber Oversight and Cybersecurity Investment Governance. All hypotheses presented in the study (H1-H6, including the process of Cyber Governance→Financial Accountability) were confirmed.

10. Discussion of Findings

The illustrative data strengthen the argument that cybersecurity should be considered as a vital element of both corporate governance and financial responsibility, and not just as a technical matter.

The positive impact of board-level oversight of cybersecurity on financial accountability is in line with the principles of Agency Theory, according to which boards that receive appropriate and reliable information on cyber risks would be capable of combining cyber risks into strategic and financial decisions.

Cyber-risk management has been shown to have the highest correlation with the financial performance due to the financial ramifications of cyber attacks such as downtime, restoration costs, legal fees, fines, and reputational loss, as the impact of which can be minimized through systematic identification, assessment, and mitigation of risks.

Internally instituted cyber controls add to the conventional definition of internal control, and since financial data is increasingly produced, processed, and transmitted in digital forms, in order to secure the security of financial information there must be efforts towards securing the digital systems as well.

Cybersecurity investment governance demonstrates a small but important effect, suggesting that the money by itself is not enough to ensure fiscal responsibility—there is a need for a transition from the "expenditure-centric" to the "risk-focused investment governance" methodology where budgets are assessed against risk tolerance, critical resources, and predicted risk mitigation.

Compliance and disclosure exhibit a significant effect on financial accountability that matches the Stakeholder Theory which states that investors, buyers, employees, and regulators all have a valid interest in cybersecurity disclosure, although the information ought to have substantial meaning rather than being fixtures, and should not reveal private information.

In conclusion, the five aspects form a continuous governance cycle, rather than acting separately—supervision from the board establishes the direction of motion, risk management raises alarms, protection measures facilitate the security process, allocation of resources occurs within the realm of governance of investments, and compliance and disclosure functions guarantee accountability, which is in line with the notion of the Resource-Based View.

11. Scope and Limitations: This study's empirical findings serve an illustrative purpose, which is to show the proposed analytical method and not the validated conclusions because the actual confirmations should wait until the accumulation and examination of the real primary data. Even when actual data will be available, there will be some limitations. This cross-sectional research design records perceptions at a certain point in time and cannot guarantee the causal pathway; however, the longitudinal research design could present the evolution of the cyber-governance maturity and financial accountability process. Another limitation is the reliance on self-reported perceptual measures, which can suffer from social-desirability bias. Furthermore, a purposive sampling technique is used, which is well-suited to reach the respondents who have knowledge regarding the topic under examination. Finally, only five governance dimensions have been analyzed within the proposed framework, and other aspects relevant to the research issue can be investigated in the future.

12. Suggestions, Recommendations, and Strategic Roadmap

Listed companies in India must: (1) implement cyber governance at the board level and report on incidences, threats, finances, and resilience with the help of external expertise; (2) make cyber risk part of enterprise risk management which also includes operational, financial, reputational, legal,

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

supply chain risk and continuity risk; (3) formulate policies on cyber investment based on risk, spending, losses, asset importance, and regulatory needs; (4) enhance internal controls over cyber risks like access management, authentication procedures, vulnerability monitoring, and internal audits, with the emphasis on financial controls; (5) improve the level of disclosure regarding cyber risks while ensuring that sensitive information is protected; (6) create a dashboard that would integrate cyber and financial risks related to value at risk, costs, incidents, and compliance; (7) promote the cooperation between finance and cybersecurity departments; (8) train the board and management in cybersecurity issues; (9) implement cyber risk management processes in vendor contracts; (10) audit the level of cyber risks regularly; (11) connect cyber risk management with corporate governance; and (12) create a cyber risk maturity model that would cover the flow from reactive to controlled, managed, integrated, and strategic stages with regular evaluations of the company's performance.

The recommended proposed plan is: Board Commitment → Cyber Risks Identification → Evaluation of Financial Effects → Investment on the Basis of Risks → Cyber Controls → Continuous Surveillance & Audit → Compliance & Transparent Disclosure → Response to Incidents & Recovery → Organizational Capability to Continue and Financial Responsibility for Stakeholders, indicating that the cyber governance process must be continuous, financially responsible and integrated into corporate governance.

13. Managerial Implications

There are numerous conclusions that are significant for the company's boards, executives, and functional leaders. Cybersecurity must belong to the board, instead of being just a matter handled by IT. The issues related to threats and vulnerabilities, as well as being prepared for such threats, must be on the agenda of the board and be discussed frequently. The board should be responsible with regard to the issues related to the CISO/CIO, that is, the CFO, internal audit, and risk and compliance on cyber risks as well and treat them as enterprise risk while planning finances for any related expenses. Organizations ought to boost collaboration across different units, factor in cyber risks into their risk-assessment practices, set up regimes of governance for third-party partners, draw up a cyber-incident response plan that takes financial aspects into account (i.e., emergency funds, insurers, and costs of recovery), and introduce measurable indicators of cyber governance (i.e., coverage of personnel training, the time taken to detect and respond to incidents, and vendor assessment). In sum, companies need to shift from reactive security measures to proactive security measures; the cyber security domain should become part of their corporate strategy and investment plans.

14. Conclusion

With corporate risk and financial responsibility in Indian listed companies: being transformed completely by digital transformation. The digital transformation creates a lot of opportunities in terms of efficiency and growth; it opens organizations to various cyber threats. This research explored cyber governance which has been defined with respect to board governance, cyber risk management, internal controls, governance of cybersecurity investments and compliance and disclosure in this research.

Results from SEM show the presence of a positive and significant correlation between the five cyber governance dimensions and financial accountability, with about 68% of its variance accounted for, with the most influential dimension being cyber risk management, followed by compliance and fraud, internal cyber control, cyber governance on the board level, and investment governance. It can be said that firms with strong cyber governance mechanisms are more able to defend their financial assets, prevent losses due to cyber incidents, provide responsibility, and keep trust of the stakeholders.

The main theoretical contribution of the research is the alignment of cybersecurity with financial accountability and emphasizing the importance of cooperation between boards, accountants, risk managers, auditors, compliance officers, cybersecurity experts in effective cyber governance. In case of the Indian companies listed on the stock exchange, cyber risk should be embedded in enterprise risk management and corporate governance systems of the company, as boards should be aware of the financial consequences, management should allocate resources according to risks involved and reporting should provide clarity in the process.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22233101

Effective cyber governance can potentially play an essential role in enhancing the financial accountability, organizational sustainability, stakeholder trust, and sustainable value of firms that rely on digital technology. The Integrated Cyber-Risk Governance Framework proposed provides a structured foundation for integrating cybersecurity, corporate governance, financial accountability, and sustainability.

References

- Alsadoun, A. A., &Albaz, M. M. (2025). The impact of cybersecurity risk disclosure and governance on firm value and stock return volatility. *Journal of Governance & Regulation, 14*(1), 194–205.
- Cortez, E. K., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation, 13*(4), 709–725.
- Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Risks, 11*(2), 32.
- Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal, 10*, Article 115.
- Franco, M. F., Künzler, F., von der Assen, J., Feng, C., & Stiller, B. (2023). RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports. *arXiv*.
- Frimpong, E. T., Schindlinger, D., Vadala, D., Ciccarelli, K., Olcott, J., & Barnett, J. (2024). *Cybersecurity, audit, and the board: How does board oversight impact cybersecurity performance?* Diligent Institute/Bitsight.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2010). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56.
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection.* ISO.
- Jiang, X., Martin, X., & Smith, J. (2022). Cybersecurity risk and the cross-section of stock returns. *Journal of Financial Economics*.
- Liu, C., & Babar, M. A. (2025). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*.
- Maréchal, L., & Celeny, D. (2024). Cyber risk and the cross-section of stock returns. *arXiv*.
- Maréchal, L., & Monnet, N. (2024). Disentangling the sources of cyber risk premia. *arXiv*.
- Matemane, R., Denhere, V., Mokabane, M., &Ojeyinka, T. A. (2024). Cybersecurity risk disclosure, board characteristics, and firm performance in the Fourth Industrial Revolution era: Evidence from an emerging economy. *African Finance Journal, 26*(1), 34–53.
- McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., &Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *arXiv*.
- Modi, A., Kuzminykh, I., & Ghita, B. (2023). Data driven approaches to cybersecurity governance for board decision-making: A systematic review. *arXiv*.
- Oktavendi, T. W., &Kholmi, M. (2024). How important is cybersecurity disclosure for firm value? *JurnalAkuntansiMultiparadigma, 15*(2), 377–386.
- Rahmah, S. A., &Mahastanti, L. A. (2026). Do risk disclosure and firm value drive Indonesian bank stock returns? *Review of Management and Entrepreneurship, 10*(1), 109–128.
- Securities and Exchange Board of India. (2024, August 20). *Cybersecurity and cyber resilience framework (CSCRF) for SEBI regulated entities (REs)* (Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113). SEBI.
- U.S. Securities and Exchange Commission. (2023). *Cybersecurity risk management, strategy, governance, and incident disclosure*. U.S. SEC.
- World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.
- World Economic Forum. (2025). *Global cybersecurity outlook 2025*. World Economic Forum.