Creative Economics and New Business Management Approaches
Volume 8, Issue 1, Feb 2026, PP 27-45
www.bmjournal.ir ISSN: 3060-5962

The Impact of Cybersecurity Risk Disclosures on Audit Fees and Cost of Debt: Evidence from Firms Listed on the Tehran Stock Exchange

Somayeh Farrokhi[1]

[1]*Department of Accounting, Astaneh Ashrafieh Branch, Islamic Azad University, Astaneh Ashrafieh, Iran.*

Abstract: *As digital infrastructure becomes central to corporate operations, cybersecurity has fundamentally evolved into a critical governance imperative. Consequently, the transparent disclosure of cybersecurity risks and mitigation strategies serves as a vital mechanism for communicating enterprise resilience. This study empirically investigates the dual economic consequences of cybersecurity risk disclosures on audit pricing and debt financing costs within a highly volatile emerging market context. Utilizing a comprehensive panel dataset of non-financial firms continuously listed on the Tehran Stock Exchange from 2019 to 2024, the research employs firm-fixed effects regression models to rigorously control for unobserved time-invariant heterogeneity and endogeneity. Drawing upon signaling theory and the audit risk model, the empirical findings reveal a statistically significant, bidirectional economic impact. First, the results document a robust positive relationship between the comprehensiveness of cybersecurity disclosures and audit fees. External auditors perceive extensive cyber disclosures as indicative of a highly complex digital risk environment, which inherently necessitates an expanded audit scope, elevated effort, and the deployment of specialized IT audit personnel. Conversely, the analysis establishes a significant negative association between these precise disclosures and the cost of debt. By proactively communicating their cyber risk management frameworks, firms effectively reduce information asymmetry with institutional lenders. This heightened transparency signals robust corporate governance and a minimized probability of systemic operational disruption, which creditors subsequently reward with substantially reduced borrowing costs, thereby elucidating the complex cost-benefit dynamics of non-financial risk reporting.*

Keywords: *Cybersecurity Risk Disclosures, Audit Fees, Cost of Debt, Information Asymmetry, Corporate Governance, Tehran Stock Exchange, Panel Data Analysis.*

I. Introduction

The contemporary corporate ecosystem has undergone a profound digital transformation, integrating sophisticated information technologies into the very fabric of organizational operations, supply chain management, and financial reporting. While this paradigm shift has undeniably catalyzed unprecedented operational efficiencies and competitive advantages, it has concurrently birthed a ubiquitous and rapidly evolving systemic threat: cybersecurity risk. No longer confined to the periphery of information technology departments, cybersecurity has ascended to the apex of corporate governance, becoming a critical priority for boards of directors, executive management, and external stakeholders. High-profile data breaches and ransomware attacks have unequivocally demonstrated that cyber incidents can inflict devastating financial losses, severely compromise proprietary intellectual property, and irreparably damage corporate reputation. Consequently, the mechanisms through which firms identify, manage, and communicate these risks have become a focal point of intense academic and regulatory scrutiny (Gordon et al., 2015). In response to the escalating severity of cyber threats, regulatory bodies globally are increasingly pressuring publicly traded companies to enhance the transparency of their non-financial reporting by explicitly detailing their cybersecurity vulnerabilities and corresponding mitigation architectures. However, the economic consequences of such disclosures remain theoretically ambiguous and empirically contested, creating a pressing need to understand how vital market participants—specifically external auditors and institutional creditors—price the information embedded within cybersecurity disclosures.

The theoretical foundation for examining the market's reaction to risk disclosures is deeply rooted in signaling theory and the concept of information asymmetry. In capital markets, an inherent informational gap exists between corporate insiders, who possess granular knowledge of the firm’s digital vulnerabilities and defense capabilities, and external stakeholders, who must rely on publicly available disclosures to assess the firm’s risk profile. From one perspective, extensive cybersecurity disclosures might be interpreted as a distress signal, alerting the market to underlying infrastructural frailties and an elevated probability of future cyber incidents. Conversely, signaling theory posits that high-quality, comprehensive disclosures function as a credible mechanism for well-governed firms to communicate their proactive risk management capabilities. By transparently detailing their cyber governance structures, incident response protocols, and investments in digital security, these firms differentiate themselves from opaque peers, thereby reducing uncertainty and cultivating trust

among stakeholders (Li et al., 2018). The duality of this theoretical framework necessitates a rigorous empirical investigation into how distinct stakeholder groups, possessing different risk appetites and analytical frameworks, interpret and react to the extent and quality of cybersecurity risk reporting.

From the perspective of external audit assurance, cybersecurity risk disclosures introduce a profound layer of complexity to the financial statement audit process. The traditional audit risk model mandates that auditors meticulously assess the risk of material misstatement arising from either error or fraud. In the modern digital enterprise, financial reporting systems are inextricably linked to the broader corporate IT infrastructure. Therefore, a firm explicitly disclosing substantial cybersecurity risks inherently signals a highly complex and potentially vulnerable internal control environment. To mitigate the elevated audit risk to an acceptable level, audit firms must fundamentally alter their engagement strategy. This adaptation typically involves expanding the overall scope of substantive testing, increasing total audit hours, and, crucially, deploying highly specialized and expensive IT audit professionals to evaluate the design and operating effectiveness of digital access controls, data encryption protocols, and disaster recovery systems (Haislip et al., 2016). The deployment of specialized personnel and the amplification of audit effort invariably translate into higher audit fees. Consequently, it is hypothesized that external auditors interpret comprehensive cybersecurity disclosures primarily through a risk-centric lens, viewing them as indicators of systemic IT complexity that demand premium pricing to compensate for the elevated assurance effort and potential litigation exposure.

In stark contrast, the perspective of institutional creditors and debt holders is uniquely shaped by their asymmetric payoff structure; creditors do not participate in the firm's upside potential but bear the full brunt of downside default risk. Therefore, debt providers are acutely sensitive to any operational disruptions that could impair the firm's ability to service its debt obligations. A catastrophic cyberattack can instantly paralyze operations, trigger massive regulatory fines, and precipitate severe liquidity crises, significantly elevating the probability of default. Within this context, proactive and highly transparent cybersecurity risk disclosures serve a fundamentally reassuring function. Creditors view extensive disclosures not as an admission of weakness, but as definitive evidence of robust internal governance and superior risk mitigation architectures (Wang et al., 2013). By demystifying their digital risk landscape, borrowing firms effectively alleviate the severe information asymmetry that typically plagues debt contracting. This transparency allows creditors to more accurately price the underlying

risk, rewarding firms that demonstrate mature cyber governance with more favorable lending terms and a substantially reduced cost of debt capital. This dynamic illustrates a critical divergence in market reactions: while auditors' price the complexity inherent in the risk, creditors price the governance quality signaled by the disclosure itself.

To rigorously investigate these intersecting economic dynamics, this study situates its empirical analysis within the unique institutional setting of the Tehran Stock Exchange (TSE). The Iranian corporate landscape presents an exceptionally compelling environment for this research. In recent years, Iranian enterprises have rapidly accelerated their integration into digital economic frameworks, yet they operate within a highly volatile macroeconomic environment characterized by complex geopolitical tensions and frequent, sophisticated state-sponsored cyber disruptions (Salehi et al., 2020). Furthermore, the regulatory environment governing non-financial reporting on the TSE is currently in a state of transformative evolution. While the Securities and Exchange Organization (SEO) of Iran has begun emphasizing the necessity of comprehensive risk reporting within the board of directors' annual activity reports, standardized frameworks for cybersecurity disclosures remain nascent. This environment of elevated actual cyber risk coupled with heterogeneous, predominantly voluntary disclosure practices creates optimal conditions for observing the true economic consequences of digital transparency. By analyzing a comprehensive panel dataset of listed firms from 2019 to 2024, this research aims to bridge a critical gap in the corporate governance and accounting literature, providing the first systematic evidence from a high-volatility emerging market on how cybersecurity risk disclosures simultaneously shape audit pricing strategies and debt financing costs.

II. Literature Review

The theoretical discourse surrounding the economic consequences of non-financial risk reporting is primarily anchored in the synthesis of signaling theory and the concept of information asymmetry, particularly within the context of agency conflicts. Historically, corporate disclosures were predominantly financial in nature, designed to provide shareholders and creditors with historical performance metrics. However, as the global economy has transitioned into a highly digitized paradigm, the perimeter of corporate risk has expanded exponentially to include systemic cyber vulnerabilities. The academic literature establishes that cybersecurity is no longer merely a technical operational issue but a fundamental component of enterprise risk management and corporate governance (Gordon et al., 2015). When managers possess private, granular information regarding the firm's digital vulnerabilities and defense

mechanisms, a state of profound information asymmetry exists between corporate insiders and external stakeholders. According to signaling theory, high-quality firms proactively utilize voluntary or expanded mandatory disclosures to signal their unobservable quality to the market. In the realm of cybersecurity, comprehensive risk disclosures serve as a credible signal of a robust internal control environment, proactive governance oversight, and a sophisticated risk mitigation architecture (Li et al., 2018). Firms that transparently communicate their cyber risk landscape differentiate themselves from opaque competitors, theoretically reducing stakeholder uncertainty. However, the interpretation of these signals is highly heterogeneous, heavily dependent on the specific analytical frameworks and risk exposures of distinct stakeholder groups, most notably external auditors and institutional creditors.

Focusing on the external audit function, the literature extensively documents that cybersecurity risk disclosures significantly disrupt traditional audit paradigms, primarily through the mechanisms delineated by the audit risk model. Auditors are mandated to provide reasonable assurance that financial statements are free from material misstatement, a task inherently reliant on the integrity of the client's internal controls over financial reporting (ICFR). As financial data generation, storage, and transmission become entirely reliant on complex IT infrastructures, any disclosed cybersecurity vulnerability inherently translates into elevated control risk. Academic evidence demonstrates that when firms explicitly disclose substantive cybersecurity risks, external auditors interpret these disclosures as indicative of systemic IT complexity and heightened vulnerability to data breaches, which could compromise financial data integrity (Haislip et al., 2016). To mitigate this elevated audit risk to an acceptable threshold, audit firms are compelled to substantially modify their engagement strategies. This adaptation necessitates a significant expansion of substantive testing, an increase in total audit hours, and the mandatory deployment of highly compensated, specialized IT audit professionals to evaluate complex digital access controls, encryption standards, and intrusion detection systems. Consequently, the literature consistently observes a positive association between the presence and extent of cyber risk disclosures and audit pricing, reflecting the premium required to compensate for the intensified audit effort and the elevated litigation risk associated with auditing digitally complex environments.

Conversely, the literature investigating the debt market's reaction to risk disclosures presents a fundamentally different economic dynamic, rooted in the asymmetric payoff structure of debt contracting. Unlike equity investors or external auditors, institutional creditors and bondholders are primarily concerned with downside risk—specifically, the probability of

default and the potential impairment of cash flows required for debt servicing. A catastrophic cyber incident can trigger severe operational paralysis, massive regulatory penalties, and acute liquidity crises, directly threatening the firm's solvency. Within this context, proactive and comprehensive cybersecurity risk disclosures are not viewed by creditors as a manifestation of infrastructural weakness, but rather as definitive evidence of superior corporate governance and mature risk management capabilities (Wang et al., 2013). By demystifying their digital risk exposures and detailing their strategic mitigation protocols, borrowing firms effectively alleviate the severe information asymmetry that plagues credit assessments. This transparency provides creditors with the verifiable data necessary to accurately price default risk. Consequently, empirical studies indicate that lenders reward firms demonstrating high-quality cyber governance and transparent reporting with more favorable contracting terms, culminating in a significantly reduced cost of debt capital. This dynamic underscores that while auditors price the mechanical complexity of the disclosed risk, creditors price the governance quality and risk mitigation capability signaled by the act of disclosure itself.

Situating this complex theoretical framework within the unique institutional context of emerging markets, such as the Tehran Stock Exchange (TSE), introduces critical empirical dimensions. The Iranian economic environment is characterized by intense macroeconomic volatility, reliance on heavily regulated banking institutions for debt financing, and a corporate landscape frequently targeted by sophisticated cyber disruptions (Moradi et al., 2021). Concurrently, corporate governance codes and non-financial reporting mandates issued by the Securities and Exchange Organization (SEO) of Iran are undergoing significant evolution, transitioning toward global transparency standards despite localized institutional voids (Salehi et al., 2020). In such high-volatility environments, the baseline level of information asymmetry is substantially elevated compared to developed markets. Therefore, the signaling value of comprehensive cybersecurity risk disclosures is theoretically amplified. Examining how Iranian auditors and domestic institutional lenders simultaneously evaluate and price these specific non-financial disclosures provides a stringent test of global accounting theories in an environment where actual cyber risk is exceptionally high and transparency mechanisms are still maturing.

Research Hypotheses

Based on the synthesis of the theoretical frameworks and the empirical evidence delineated in the preceding literature, this study formulates the following primary research

hypotheses to systematically investigate the dual economic consequences of cybersecurity risk reporting:

- H1: There is a statistically significant positive relationship between the comprehensiveness of cybersecurity risk disclosures and audit fees.
- H2: There is a statistically significant negative relationship between the comprehensiveness of cybersecurity risk disclosures and the cost of debt.

III. Methodology

The empirical research design of this study relies on a quantitative, ex-post facto methodology structured around a longitudinal panel data framework to rigorously test the formulated hypotheses concerning cybersecurity risk disclosures, audit pricing, and debt financing costs. The primary population encompasses all public joint-stock companies officially listed on the Tehran Stock Exchange (TSE). The temporal scope of the investigation spans a continuous six-year period from 2019 to 2024. This specific timeframe is deliberately selected because it captures a period characterized by a rapid acceleration in the digital transformation of Iranian enterprises, a concurrent escalation in sophisticated, state-level cyber threats targeting critical infrastructure, and the progressive implementation of enhanced corporate governance directives by the Securities and Exchange Organization (SEO) of Iran. To construct a highly reliable and homogenous panel dataset, a stringent set of exclusionary criteria is systematically applied to the initial population. First, all financial institutions, encompassing banks, insurance firms, and investment trusts, are entirely eliminated from the sample due to their fundamentally divergent regulatory constraints, unique capital structures, and the specialized nature of their financial reporting, which renders standard risk pricing models structurally inapplicable. Second, to prevent survivorship bias and maintain longitudinal consistency, firms that were delisted, experienced prolonged trading halts exceeding six months, or underwent significant structural reorganizations during the observation window are excluded. Third, companies whose fiscal year-ends do not correspond with the standard Iranian calendar year (ending in late March, or Esfand) are omitted to ensure the temporal synchronization of market and accounting data. Finally, a rigorous data availability filter is enforced, excluding any firm-year observations that lack the requisite financial data, audit fee disclosures, or comprehensive board of directors' reports necessary for executing the content analysis of cybersecurity disclosures. The application of these systematic filters yields a robust, balanced panel dataset, providing a mathematically sound foundation for

executing advanced multivariate econometric estimations and effectively controlling for unobserved firm-specific heterogeneity over time.

Table 1: Sample Selection Procedure

Criteria Description	Number of Firms
Total baseline firms listed on the Tehran Stock Exchange (TSE) at the beginning of 2019	492
Less: Financial institutions, banks, insurance, and investment holding companies	(68)
Less: Firms delisted or experiencing severe trading halts (exceeding 6 months) during 2019-2024	(51)
Less: Firms with non-standard fiscal year-ends (deviating from the uniform March/Esfand reporting cycle)	(42)
Less: Firms with systematically missing financial data, audit fees, or comprehensive board reports	(116)
Final sample of non-financial firms (Balanced Panel: 215 firms × 6 years = 1,290 observations)	215

The measurement of the primary variables requires a multidimensional analytical approach, beginning with the independent variable, cybersecurity risk disclosure quality. Because a universally standardized and heavily mandated cybersecurity reporting framework is still evolving within the TSE, this study constructs a comprehensive, proprietary disclosure index based on rigorous content analysis. Data is meticulously hand-collected from the annual board of directors' activity reports, internal control declarations, and official filings submitted to the comprehensive database of all Iranian registered companies (Codal). The index evaluates the presence, depth, and specificity of disclosures across multiple critical dimensions: the explicit identification of cyber threats, detailed descriptions of the IT governance architecture, investments in information security infrastructure, incident response protocols, and the integration of cyber risk into the enterprise risk management framework. The index is operationalized as a continuous variable scaled between 0 and 1, representing the proportion of disclosed items relative to the maximum possible disclosure score. The first dependent variable, audit pricing, is operationalized as the natural logarithm of total audit fees paid to the

independent external auditor. The logarithmic transformation is implemented to mitigate the severe right-skewness inherently present in raw audit fee data and to ensure the normality of the residuals within the regression estimations. The second dependent variable, the cost of debt, serves as the proxy for the debt market's pricing of the firm's risk profile. It is mathematically calculated as the firm's total interest expense for the fiscal year divided by the average of its short-term and long-term interest-bearing debt between the beginning and the end of the year. To isolate the specific economic impact of cybersecurity disclosures and mitigate omitted variable bias, the empirical models incorporate a robust vector of control variables firmly established in the audit and finance literature. For the audit fee model, controls include firm size (natural logarithm of total assets), operational complexity (the ratio of inventory and receivables to total assets), financial leverage (total debt to total assets), profitability (return on assets), an indicator for financial loss, and a dichotomous variable indicating whether the firm is audited by an industry-specialized, top-tier audit organization (the Iranian equivalent of a Big N auditor). The cost of debt model incorporates a distinct, yet overlapping, set of controls including firm size, financial leverage, the market-to-book ratio as a proxy for growth opportunities, operating cash flow scaled by total assets, and the tangible asset ratio, which represents the proportion of assets capable of being pledged as collateral. To empirically test the formulated hypotheses, the study deploys advanced multivariate panel data regression techniques. Specifically, firm and year fixed-effects models are utilized to rigorously control for unobserved, time-invariant corporate characteristics and macroeconomic shocks idiosyncratic to specific years. The following comprehensive econometric equations are established to test Hypothesis 1 (Audit Fees) and Hypothesis 2 (Cost of Debt), respectively:

$$LNAF_{i,t} = \beta_0 + \beta_1 CYBER\_INDEX_{i,t} + \beta_2 SIZE_{i,t} + \beta_3 INVREC_{i,t} + \beta_4 LEV_{i,t} + \beta_5 ROA_{i,t} + \beta_6 LOSS_{i,t} + \beta_7 BIGN_{i,t} + \mu_i + \lambda_t + \epsilon_{i,t}$$

$$COD_{i,t} = \alpha_0 + \alpha_1 CYBER\_INDEX_{i,t} + \alpha_2 SIZE_{i,t} + \alpha_3 LEV_{i,t} + \alpha_4 MTB_{i,t} + \alpha_5 CFO_{i,t} + \alpha_6 TANG_{i,t} + \mu_i + \lambda_t + \epsilon_{i,t}$$

IV. Empirical Results

Commencing the empirical evaluation, an extensive analysis of the descriptive statistics is requisite to delineate the fundamental distributional properties, central tendencies, and dispersion metrics of the variables incorporated within the comprehensive panel dataset of 1,290 firm-year observations from the Tehran Stock Exchange spanning the 2019–2024 timeframe. The primary independent variable of interest, the cybersecurity risk disclosure

index, exhibits a mean of 0.315 and a standard deviation of 0.172. This relatively low average score, constrained within a theoretical range of 0 to 1, quantitatively substantiates the premise that the majority of Iranian listed firms are still in the nascent stages of developing and publicly articulating comprehensive digital risk management frameworks. However, the considerable variation between the minimum observed value (0.050) and the maximum (0.845) indicates a highly heterogeneous reporting environment, wherein a subset of technologically progressive firms proactively issues extensive cyber disclosures, while others maintain minimalist, compliance-driven boilerplate reporting. Regarding the primary dependent variables, the natural logarithm of audit fees demonstrates a mean of 14.820, reflecting the substantial absolute financial expenditures required for statutory assurance services within this complex macroeconomic environment. The cost of debt, acting as the second dependent variable, averages 0.214 (or 21.4 percent), an elevated figure that accurately captures the severe systemic inflationary pressures, the stringent monetary policies enacted by the Central Bank of Iran, and the overarching liquidity constraints characterizing the domestic credit market during the observation window. The control variables further contextualize the sample's economic reality, with average financial leverage resting at 0.598, indicating a heavy reliance on debt financing, and a mean return on assets of 0.092, underscoring the operational profitability challenges faced by non-financial enterprises amidst persistent economic volatility and external sanctions.

Table 2: Descriptive Statistics (2019-2024 Panel Data, N=1,290)

Variables	Mean	Median	Std. Dev.	Minimum	Maximum
Natural Logarithm of Audit Fees (LNAF)	14.820	14.750	1.105	11.340	18.120
Cost of Debt (COD)	0.214	0.205	0.058	0.095	0.380
Cybersecurity Disclosure Index (CYBER_INDEX)	0.315	0.285	0.172	0.050	0.845
Firm Size (SIZE)	13.950	13.880	1.420	10.150	18.550
Financial Leverage (LEV)	0.598	0.605	0.185	0.120	0.950
Inventory and Receivables (INVREC)	0.385	0.370	0.155	0.040	0.810

Variables	Mean	Median	Std. Dev.	Minimum	Maximum
Return on Assets (ROA)	0.092	0.085	0.095	-0.180	0.410
Market-to-Book Ratio (MTB)	2.250	1.950	1.410	0.550	9.150
Tangible Asset Ratio (TANG)	0.415	0.400	0.210	0.050	0.910

Transitioning to the diagnostic evaluation of the dataset, a Pearson correlation matrix was computed to perform an initial assessment of the hypothesized bivariate relationships and to meticulously screen for potential multicollinearity anomalies that could compromise the validity of the multivariate regression estimates. The preliminary correlation coefficients align seamlessly with the theoretical postulates established in the literature review; the cybersecurity disclosure index exhibits a statistically significant positive zero-order correlation with audit fees and a corresponding negative correlation with the cost of debt. Crucially, to ensure the econometric stability of the proposed models, variance inflation factor (VIF) analyses were conducted across all predictor variables. The maximum VIF recorded was 2.58, a value substantially below the stringent, conventionally accepted threshold of 10.0, thereby providing robust empirical assurance that multicollinearity does not represent a structural threat to the integrity of the estimations. To determine the most appropriate panel data specification, the Hausman test was subsequently executed. The test yielded highly significant chi-square statistics for both the audit fee model ($p < 0.001$) and the cost of debt model ($p < 0.001$), decisively rejecting the null hypothesis of the random-effects specification. Consequently, the fixed-effects regression architecture was definitively adopted to rigorously control for unobserved, time-invariant firm-level heterogeneity. Furthermore, robust standard errors clustered at the firm level were methodically implemented across all multivariate models to neutralize potential inferential biases arising from heteroscedasticity and serial autocorrelation, ensuring the highest degree of statistical reliability.

Table 3: Fixed-Effects Panel Regression Results

Independent Variables	Model 1: Audit Fees (LNAF)	Model 2: Cost of Debt (COD)
Cybersecurity Disclosure Index (CYBER_INDEX)	0.142*** (4.15)	-0.038*** (-3.82)

Independent Variables	Model 1: Audit Fees (LNAF)	Model 2: Cost of Debt (COD)
Firm Size (SIZE)	0.315*** (9.42)	-0.012*** (-3.15)
Financial Leverage (LEV)	0.128*** (3.55)	0.045*** (4.62)
Inventory and Receivables (INVREC)	0.095** (2.41)	—
Return on Assets (ROA)	-0.052 (-1.35)	—
Market-to-Book Ratio (MTB)	—	-0.005** (-2.18)
Tangible Asset Ratio (TANG)	—	-0.021*** (-2.95)
Loss Indicator (LOSS)	0.082** (2.12)	—
Big N Auditor (BIGN)	0.185*** (5.65)	—
Firm Fixed Effects	Included	Included
Year Fixed Effects	Included	Included
Adjusted R-squared	0.645	0.412
F-Statistic (p-value)	48.25 (0.000)	32.18 (0.000)

Dependent Variables: Audit Fees and Cost of Debt

Delving into the core inferential outcomes presented in Table 3, Model 1 systematically evaluates the first hypothesis (H1) by estimating the direct impact of cybersecurity risk disclosures on external audit pricing. The empirical estimation reveals a highly significant, positive coefficient for the cybersecurity disclosure index (0.142, t-statistic = 4.15, $p < 0.01$). This robust finding provides definitive confirmation of H1, demonstrating unequivocally that external auditors operating within the Iranian market interpret comprehensive cyber disclosures as an unambiguous signal of profound internal IT complexity and elevated operational risk. In direct alignment with the theoretical mechanisms of the audit risk model, as firms transparently detail complex digital infrastructures, interconnected data networks, and inherent systemic vulnerabilities, auditors are practically compelled to respond. This response manifests as a mandatory expansion of substantive testing protocols, the necessary deployment of highly compensated IT audit specialists to verify encryption standards and access controls, and an overall amplification of audit effort to successfully mitigate the heightened risk of material

misstatements arising from digital breaches. Consequently, this requisite escalation in specialized labor and procedural scope translates directly into a statistically and economically significant premium levied upon the client's audit fees. The control variables within this model perform precisely as theoretically anticipated; firm size, financial leverage, operational complexity (inventory and receivables), the occurrence of financial losses, and engagement with a top-tier audit firm all exhibit significant positive associations with audit fees, verifying the structural integrity of the baseline pricing model.

Conversely, Model 2 investigates the second hypothesis (H2) by analyzing the debt market's pricing reaction to identical cybersecurity risk disclosures, yielding a starkly divergent economic outcome. The regression output documents a profound, statistically significant negative coefficient for the cybersecurity disclosure index concerning the cost of debt (-0.038, t-statistic = -3.82, $p < 0.01$). This empirical result forcefully validates H2, elucidating the powerful mitigating effect of non-financial transparency on institutional lending constraints. Unlike external auditors who price the mechanical complexity of the disclosed risk, domestic creditors and institutional lenders interpret comprehensive cybersecurity reporting through the theoretical lens of signaling theory, viewing it as definitive, verifiable evidence of superior corporate governance and proactive risk mitigation. By voluntarily demystifying their digital vulnerabilities and explicitly detailing their incident response architectures, borrowing firms successfully dismantle the severe information asymmetry that traditionally exacerbates agency conflicts in debt contracting. This heightened level of transparency drastically reduces lenders' uncertainty regarding the probability of catastrophic operational disruptions or regulatory defaults. Consequently, creditors logically reward this demonstrably mature cyber governance with more favorable credit assessments, ultimately resulting in a significant reduction in the firm's required cost of debt capital. This bidirectional dynamic confirms that while expansive digital transparency incurs immediate operational costs via elevated audit premiums, it simultaneously generates substantial, long-term financial benefits by unlocking cheaper avenues of debt financing within a highly constrained credit market.

V. Discussion

The empirical results of this comprehensive panel data analysis elucidate a profoundly nuanced, bidirectional economic reaction to the voluntary disclosure of cybersecurity risks within the high-volatility institutional context of the Tehran Stock Exchange (TSE). The definitive confirmation of the first hypothesis, demonstrating a statistically significant positive relationship between the comprehensiveness of cybersecurity risk disclosures and audit fees,

provides robust empirical validation for the theoretical postulates of the audit risk model in a digitized corporate era. When a firm transparently articulates its digital vulnerabilities, potential cyber threats, and complex IT mitigation architectures, external auditors do not view this transparency through the optimistic lens of corporate governance; rather, they interpret it as an unambiguous signal of elevated systemic risk and internal control complexity (Haislip et al., 2016). In modern financial reporting, the integrity of financial data is inextricably bound to the security of the underlying IT infrastructure. Therefore, explicit cyber disclosures trigger a mandatory reassessment of the client's Internal Control over Financial Reporting (ICFR). To maintain audit risk at an acceptable threshold, audit organizations are practically compelled to significantly expand the scope of their engagement. This expansion necessitates a structural shift from standard substantive testing toward highly complex IT General Controls (ITGC) and application control testing. In the specific context of the Iranian market, where standardized, universally adopted IT auditing frameworks are still in a state of nascent development, audit firms face steep technological learning curves. To effectively audit these heavily digitized environments, audit partners must deploy highly specialized, technically proficient, and heavily compensated IT audit personnel or external cybersecurity consultants to verify encryption protocols, test intrusion detection systems, and evaluate disaster recovery mechanisms (Salehi et al., 2020). The positive coefficient observed in the fixed-effects regression model quantitatively captures this dynamic, proving that the requisite escalation in specialized labor, extended audit hours, and the inherent assumption of elevated litigation risk by the auditor are directly passed on to the reporting firm in the form of substantial audit fee premiums. Consequently, from an assurance perspective, non-financial transparency regarding digital vulnerabilities is an inherently costly endeavor.

Conversely, the unequivocal validation of the second hypothesis presents a profound economic counterbalance, demonstrating a statistically significant negative association between identical cybersecurity risk disclosures and the firm's cost of debt capital. This specific finding seamlessly aligns with the foundational tenets of signaling theory and provides a stark contrast to the auditor's risk-centric paradigm (Li et al., 2018). While external auditors penalize the mechanical and operational complexity of the disclosed digital risks, institutional creditors and debt holders actively reward the corporate governance mechanisms that facilitated the disclosure itself. Debt contracting is fundamentally characterized by severe information asymmetry and an asymmetric payoff structure; lenders do not participate in exceptional corporate upside but suffer absolute losses in the event of default. In an emerging market like

Iran, where macroeconomic instability and state-sponsored cyber disruptions are prevalent realities, the baseline probability of operational paralysis—and subsequent default—is heavily scrutinized by credit institutions (Moradi et al., 2021). Within this high-stress environment, a firm that proactively and transparently details its cybersecurity risk landscape and corresponding mitigation strategies emits a highly credible signal of administrative maturity and robust enterprise risk management. From the creditor's perspective, opacity regarding cyber threats is perceived as a critical managerial blind spot, whereas comprehensive disclosure indicates that the board of directors has thoroughly integrated digital resilience into its strategic planning matrix (Gordon et al., 2015). By demystifying their internal IT infrastructure and explicitly outlining their incident response protocols, borrowing firms successfully dismantle the informational barriers that typically exacerbate agency conflicts between management and debt providers.

The juxtaposition of these two primary findings highlights a complex, multidimensional cost-benefit paradigm inherent in contemporary non-financial reporting. The reduction in the cost of debt mathematically illustrates that lenders utilize comprehensive cyber disclosures to downwardly revise their estimates of the firm’s default probability. When a firm demonstrates that it possesses the technological infrastructure and governance oversight to survive and quickly recover from a catastrophic data breach or ransomware attack, lenders perceive a structurally lower risk to future cash flows required for debt servicing (Wang et al., 2013). As a direct consequence, credit risk premiums are substantially compressed, resulting in more favorable interest rates and relaxed debt covenants. These dynamic underscores a critical divergence in stakeholder information processing: external assurance providers meticulously price the mechanical effort required to independently verify the disclosed digital complexity, while capital providers price the overall quality of the governance signal embedded within the act of voluntary transparency. For executive management operating within the TSE, these results empirically map the strategic trajectory of corporate disclosures; the immediate, tangible increase in operational compliance costs, manifested through elevated audit fees, is systematically offset—and potentially exceeded—by the substantial, long-term financial benefits derived from unlocking cheaper avenues of institutional debt financing.

VI. Conclusion

The exponential integration of digital technologies into the core operational and financial frameworks of modern enterprises has fundamentally elevated cybersecurity from a

rudimentary technical issue to a critical pillar of corporate governance and strategic risk management. Consequently, the mechanisms by which firms assess, mitigate, and publicly disclose their digital vulnerabilities have become subject to intense scrutiny from a diverse array of market participants. This comprehensive empirical study sought to systematically investigate the complex, often conflicting economic consequences of voluntary cybersecurity risk disclosures on two fundamental pillars of corporate finance and assurance: external audit pricing and the cost of debt capital. By situating this analysis within the highly volatile and dynamic institutional context of the Tehran Stock Exchange over a continuous six-year period from 2019 to 2024, the research addressed a significant void in the contemporary accounting literature regarding the pricing of non-financial digital risk in emerging markets. Utilizing a robust panel dataset comprising 1,290 firm-year observations from non-financial entities, and employing rigorous fixed-effects econometric modeling to control for unobserved heterogeneity and endogenous market forces, the empirical analyses yielded profound insights into how distinct stakeholder groups interpret and react to corporate transparency in the digital age. The findings unequivocally demonstrate a bidirectional economic impact, structurally validating the theoretical tension between the audit risk model and the tenets of signaling theory. First, the study documented a highly significant, positive relationship between the comprehensiveness of cybersecurity risk disclosures and total audit fees. This confirms that external assurance providers fundamentally interpret detailed digital risk reporting as a definitive signal of systemic IT complexity and an elevated probability of material misstatement stemming from internal control vulnerabilities. To mitigate this heightened audit risk, audit organizations are practically compelled to expand the scope of their substantive testing, extend audit hours, and deploy specialized, highly compensated IT audit personnel, the costs of which are directly transferred to the client via substantial fee premiums.

Conversely, the research simultaneously established a robust, statistically significant negative association between identical cybersecurity disclosures and the firm's cost of debt capital. This crucial finding powerfully illustrates that domestic institutional lenders and creditors process digital transparency through a fundamentally divergent analytical lens. Rather than penalizing the mechanical complexity of the disclosed risks, debt providers view comprehensive, voluntary cyber reporting as a highly credible signal of mature corporate governance, proactive board oversight, and superior enterprise risk management capabilities. By actively demystifying their digital infrastructures and detailing robust incident response protocols, borrowing firms successfully dismantle the profound information asymmetry that

typically exacerbates agency conflicts within credit markets. This verifiable transparency effectively reduces lenders' perceived uncertainty regarding the probability of catastrophic operational disruptions or default-inducing cyber events, leading them to reward the disclosing firms with significantly more favorable credit assessments, relaxed covenants, and a compressed cost of debt. The juxtaposition of these findings reveals a complex cost-benefit paradigm inherent in modern corporate reporting: while expansive digital transparency incurs immediate, tangible compliance and assurance costs, it concurrently unlocks substantial, long-term financial benefits by facilitating access to cheaper institutional capital. These insights provide vital, actionable implications for regulatory authorities, such as the Securities and Exchange Organization of Iran, suggesting that while mandatory, standardized cybersecurity reporting frameworks are necessary to protect stakeholders, regulators must be acutely aware of the associated assurance burdens placed upon reporting entities. For corporate boards of directors and executive management, the study empirically maps a strategic trajectory, demonstrating that investments in robust cyber governance and transparent reporting are not merely compliance exercises, but value-enhancing strategic decisions that optimize the firm's capital structure. Future research should expand upon these foundational findings by incorporating qualitative, textual analysis of the specific linguistic tone utilized in cyber disclosures, and by exploring how distinct categories of digital risk—such as data privacy breaches versus operational ransomware attacks—differentially impact equity market valuations and long-term firm survivability across diverse emerging economies.

References

Abbott, L. J., Parker, S., & Peters, G. F. (2004). Audit committee characteristics and restatements. *Auditing: A Journal of Practice & Theory*, 23(1), 69-87.

Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., & LaFond, R. (2009). The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research*, 47(1), 1-43.

Bédard, J., Chtourou, S. M., & Courteau, L. (2004). The effect of audit committee expertise, independence, and activity on aggressive earnings management. *Auditing: A Journal of Practice & Theory*, 23(2), 13-35.

Bell, T. B., Landsman, W. R., & Shackelford, D. A. (2001). Auditors' perceived business risk and audit fees: Analysis and evidence. *Journal of Accounting Research*, 39(1), 35-43.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471-482.

Blankespoor, E., Miller, B. P., & White, H. D. (2014). The role of dissemination in market liquidity: Evidence from firms' use of Twitter. *The Accounting Review*, 89(1), 79-112.

Botosan, C. A. (1997). Disclosure level and the cost of equity capital. *The Accounting Review*, 72(3), 323-349.

Christensen, H. B., Hail, L., & Leuz, C. (2021). Mandatory CSR and sustainability reporting: Economic analysis and literature review. *Review of Accounting Studies*, 26(4), 1176-1248.

Cohen, J. R., Krishnamoorthy, G., & Wright, A. M. (2004). The corporate governance mosaic and financial reporting quality. *Journal of Accounting Literature*, 23, 87-152.

DeFond, M., & Zhang, J. (2014). A review of archival auditing research. *Journal of Accounting and Economics*, 58(2-3), 275-326.

Diamond, D. W., & Verrecchia, R. E. (1991). Disclosure, liquidity, and the cost of capital. *The Journal of Finance*, 46(4), 1325-1359.

Florackis, C., Kanas, A., Kostakis, A., & Sainani, S. (2020). Idiosyncratic risk, risk-taking incentives and the relation between managerial ownership and firm value. *European Journal of Operational Research*, 283(2), 748-766.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3), 567-594.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 23(1), 33-71.

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrades. *Journal of Information Systems*, 30(1), 41-70.

Hay, D. C., Knechel, W. R., & Wong, N. (2006). Audit fees: A meta-analysis of the effect of supply and demand attributes. *Contemporary Accounting Research*, 23(1), 141-191.

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, 31(1-3), 405-440.

Kamiya, S., Kang, J. K., Kim, J., & Milidonis, A. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719-749.

Kim, Y., Li, H., & Li, S. (2014). Corporate social responsibility and stock price crash risk. *Journal of Banking & Finance*, 43, 1-13.

Lawrence, A., Minutti-Meza, M., & Zhang, P. (2011). Can Big 4 versus non-Big 4 differences in audit-quality proxies be attributed to client characteristics? *The Accounting Review*, 86(1), 259-286.

Leuz, C., & Verrecchia, R. E. (2000). The economic consequences of increased disclosure. *Journal of Accounting Research*, 38, 91-124.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, 40-55.

Minnis, M. (2011). The value of financial statement verification in debt financing: Evidence from private U.S. firms. *Journal of Accounting Research*, 49(2), 457-506.

Moradi, M., Salehi, M., & Bami, E. M. (2021). The effect of internal audit function and corporate governance on financial reporting quality: Evidence from Iran. *Journal of Financial Crime*, 28(2), 522-540.

O'Donnell, E., & Schultz, J. J. (2005). The halo effect in business risk audits: Can strategic risk assessment bias auditor judgment about accounting details? *The Accounting Review*, 80(3), 921-939.

Pittman, J. A., & Fortin, S. (2004). Auditor choice and the cost of debt capital for newly public firms. *Journal of Accounting and Economics*, 37(1), 113-136.

Salehi, M., Tarighi, H., & Rezanezhad, M. (2020). The relationship between board of directors' structure and company ownership with corporate social responsibility disclosure: Iranian angle. *Humanomics*, 36(1), 71-96.

Sengupta, P. (1998). Corporate disclosure quality and the cost of debt. *The Accounting Review*, 73(4), 459-474.

Simnett, R., Vanstraelen, A., & Chua, W. F. (2009). Assurance on sustainability reports: An international comparison. *The Accounting Review*, 84(3), 937-967.

Wang, T., Kannan, K., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, 24(2), 201-218.