Journal of Business, Behavior & Sustainability
JBBS

Vol. 1 | No. 1 | 2026
pp. 1-13

ORIGINAL RESEARCH

When Green Firms Get Hacked: Cybersecurity Breaches, ESG Disclosure, and the Cost of Capital

Muhammad Zain Malik[1,*], Salman Hanif[2], Warda Saman[3]

[1] *Department of Accounting and Information Systems, Qatar University, Doha, Qatar.*
[2] *College of Management Science, Chengdu University of Technology, Chengdu, China.*
[3] *Department of Psychology, Bahauddin Zakariya University, Multan, Pakistan.*

ARTICLE HISTORY

Received
12 June 2026
Latest revision
20 July 2026
Accepted
24 July 2026
Published online
30 July 2026

KEYWORDS
Cybersecurity breaches
ESG disclosure quality
Cost of capital
Credit ratings
Moderation mediation analysis

ABSTRACT

Amid rising digital exposure and investor scrutiny of sustainability reporting, firms face the twin challenge of managing cybersecurity risk while sustaining market trust. This study addresses how cybersecurity breaches propagate into financing costs and whether the quality of ESG disclosure alters that propagation. Using a multi-year firm-year panel with firm and year fixed effects and clustered standard errors, we estimate direct, mediating, and moderating relations among breaches, credit ratings, ESG disclosure quality, and the cost of capital. Results show a material "breach premium" in the cost of debt; higher-quality ESG disclosure is associated with lower financing costs; and credit ratings transmit part of the breach effect to borrowing costs, yielding a statistically reliable indirect pathway. Crucially, ESG disclosure quality weakens the breach-cost of capital linkage, indicating that transparent, consistent, and assured reporting buffers financing penalties following incidents. We conclude that integrating cyber governance with ESG disclosure and engaging proactively with rating agencies can measurably reduce financing frictions; we recommend institutionalizing board-level oversight, external assurance of key governance metrics, and investor-facing dashboards that link controls to capital-market outcomes.

1. Introduction

In an increasingly digitalized and sustainability-conscious world, firms face a dual challenge: protecting their technological assets while maintaining investor confidence through responsible governance and transparency (Alamandi, 2025). Cybersecurity breaches have become one of the most disruptive risks in modern finance, threatening firms' reputation, operations, and financial stability (Uddin et al., 2020). Simultaneously, environmental, social, and governance (ESG) disclosure has emerged as a mechanism for signalling corporate transparency, resilience, and long-term orientation (Albitar et al., 2023). While these two domains cybersecurity and ESG have often been studied separately, the convergence of technological vulnerability and sustainability communication presents a new frontier for financial research (Shackelford et al., 2023). The question of how ESG disclosure influences firms' financial resilience following cybersecurity breaches remains largely unexplored, particularly in terms of their impact on the cost of capital, a crucial determinant of corporate investment and valuation (Griffin, 2025).

Prior studies in finance and risk management have established that cybersecurity incidents can have immediate and measurable effects on firm value (Nahidi, 2025). Event studies demonstrate that data breaches reduce stock prices, increase market volatility, and undermine investor confidence (Tweneboah-Koduah et al., 2020). Similarly, research on corporate disclosure practices suggests that transparent ESG reporting can lower information asymmetry, enhance corporate reputation, and attract long-term investors (Sari & Muslim, 2024). Studies such as those by Krüger (2015) and Broadstock et al. (2021) show that strong ESG performance is associated with lower capital costs and improved access to financing (Tanjung, 2023). Yet, the intersection of these two domains specifically how ESG disclosure moderates the financial consequences of cybersecurity failures has not received adequate empirical attention (Chebbi, 2025). Firms may face a paradox where their environmental and governance transparency mitigates reputational damage from digital risks, but this potential relationship remains largely theoretical and untested in empirical finance (Kluiters et al., 2023).

This gap becomes more significant when viewed against the backdrop of growing investor awareness and regulatory

*** Corresponding author**
Muhammad Zain Malik, Department of Accounting and Information Systems, Qatar University, Doha, Qatar.
Email: zainmalik59@hotmail.com

demand for ESG transparency (Dye et al., 2021). Although several studies have linked ESG scores to firm value, only a limited number have explored ESG disclosure as a risk-buffering mechanism in non-environmental contexts such as cyber incidents (Zhang et al., 2020). Moreover, existing literature primarily focuses on stock market reactions, overlooking deeper financial outcomes like the cost of debt and equity capital (Arhinful et al., 2024). The financial markets increasingly view cyber risk as a determinant of firm creditworthiness, yet how ESG reporting interacts with this perception remains unknown (Singh, 2025). Hence, there is a lack of comprehensive evidence explaining whether ESG disclosure can attenuate the financial penalties of cybersecurity breaches, such as elevated financing costs or credit rating downgrades (Griffin, 2025). Addressing this research void is critical for firms, investors, and regulators seeking to understand the financial implications of integrated risk management (Nafiu et al., 2025).

This study contributes to the growing body of work on emerging financial risks by empirically investigating how ESG disclosure quality moderates the relationship between cybersecurity breaches and firms' cost of capital (Al Amosh & Khatib, 2025). It extends prior research in two major ways. First, it introduces ESG transparency as a moderating mechanism that may buffer the financial consequences of cybersecurity breaches, advancing our understanding of how sustainability practices contribute to firm resilience (Bindeeba et al., 2025). Second, by focusing on the cost of capital rather than short-term market reactions, this study provides a long-term financial perspective on cyber risk management (Nagila et al., 2025). The findings are expected to inform corporate managers about the dual importance of investing in cybersecurity and maintaining transparent ESG communication, while offering policymakers insight into how sustainability reporting standards can indirectly strengthen financial stability (Ogugua, 2024).

The study draws on two theoretical foundations: Signalling Theory and Stakeholder Theory. From a signalling perspective, ESG disclosure represents a credible communication of corporate transparency and commitment to responsible management, which reduces information asymmetry between firms and investors (Ahmed, 2023). Following a cybersecurity breach, firms with high-quality ESG disclosure are expected to send a reassuring signal of governance reliability, thus limiting the perceived risk premium demanded by capital providers (Basiouny, 2024). Stakeholder Theory further supports the argument that socially responsible and transparent firms cultivate stronger relationships with key stakeholders, enabling them to better absorb reputational shocks (Kalra, 2024). By integrating these theories, the study positions ESG disclosure as a critical moderating force in the link between cybersecurity threats and financial risk, offering a new lens through which to view the intersection of sustainability and digital security in modern financial management (Mendonça et al., 2025).

2. Literature Review - Theoretical Foundations

The current study is based mainly on Signalling Theory and Stakeholder Theory, which collectively form the conceptual framework of the extent to which the financial implication of cyber security breaches is affected by ESG disclosure (Schaffner et al., 2023). In the view of Signalling Theory, companies make voluntary disclosure, like ESG reporting, to signal believable information regarding their quality, governance, and their intent towards longevity (Friske et al., 2023). Under conditions of information asymmetry and uncertainty, the signals contribute to the ability of investors to make the distinction between well-managed and poorly governed companies (Wafula, 2018). Good disclosure under the banner of ESG, therefore, becomes a reputational buffer stacked over the time when the unforeseen incident like data breach or cyberattack is faced by the firm, otherwise generating unfavorable investor response coupled with the increase in the risk viewed by the investor (Louisot, 2024).
Stakeholder Theory extends this view by adding that firms are not only responsible to shareholders but to stakeholders as well, such as customers, employees, suppliers, and regulators (Richter & Dow, 2017). Firms engaged in socially responsible openness are better positioned to enjoy stakeholder confidence even during the occurrence of crises (Lins et al., 2017). Applying the case to cybersecurity breaches, the disclosure of a firm's ESG mitigates the level of ethical standards, the strength of the firm's governance, as well as the level of openness all factors capable of retaining stakeholder confidence (Akinsola, 2025). Combined, the theories imply that the disclosure of an ESG works both as a signal of dependability as well as a stakeholder confidence builder, mitigating financial effects of the occurrence of cybersecurity breaches on firm outcomes like the cost of capital as well as the firm's credit rating (Elsayed et al., 2024).

2.2 Cybersecurity Breach and Cost of Capital

Cybersecurity breaches are one of the most material non-financial threats faced by companies in the digital economy (Arena et al., 2022). They violate the confidentiality and integrity of corporate information, causing financial losses, reputational harm, and operational disruptions (Spanca & Salihu, 2024). There is an expanding empirical literature illustrating that cyberattack-beset firms have suffered poor financial outcomes, including the increase of capital cost (Agrafiotis et al., 2018). Examples include research conducted by Gordon et al. (2018) and Kamiya et al. (2021), which indicate that security incidents have the effect of raising investors' risk perceptions, raising the cost of debt capital similarly and the desired rate of return on equity capital (Havakhor et al., 2021). Breaches also have the potential to trigger credit rating agencies' updation, viewing affected companies as riskier borrowers (Partnoy, 2017).

The underlying mechanism is based on information asymmetry and risk premium felt (Bergh et al., 2019). After experiencing a cyber-incident, investors require higher returns to pay for intensified doubt regarding the firm's future cash flows and governance quality (Amani et al., 2025). The market sees a breach as evidence of managerial incompetence or poor internal controls, so it will erode investor confidence and finance costs will rise (Guo et al., 2016). Therefore, cyber security breaches are not only operational or reputational shocks they actually affect the firm's financial architecture by increasing its cost of capital and access to cheap finance is contracted (Malliouris, 2021).

H1: Cybersecurity breaches are positively associated with firms' cost of capital (Havakhor et al., 2020).

2.3 ESG Disclosure and Cost of Capital

Environmental, social, and governance (ESG) disclosure is an important aspect of corporate transparency and investor information usage (Zopounidis et al., 2020). Companies possessing good ESG disclosure practices have been found to have less information asymmetry, enhanced reputation, and increased investor confidence, all helping to decrease their capital cost (Ellili, 2022). Dhaliwal et al. (2011) discovered that companies undertaking voluntary sustainability reporting have equity capital cost reduction, while El Ghoul et al. (2011) revealed that companies superior in CSR performance have diminishing funding cost (Dhaliwal et al., 2011).

The mechanism functions through various channels. First, disclosure by ESG diminishes uncertainty by giving investors additional complete and reliable information on the firm's strategic direction and non-financial risk (Santamaria et al., 2021). Second, disclosure by ESG conveys strong corporate governance and long-term dedicated responsible management, thereby enticing institutional investors and creditors that are sensitive to transparency (Vickneswaran, 2025). Third, disclosure by ESG boosts stakeholder legitimacy, so the firm reduces reputational risk that would otherwise make capital costly (Maaloul et al., 2023). Thus, better reporting by firms on their ESG is perceived as less risk, so they are able to access capital under better terms (Raimo et al., 2021).

H2: ESG disclosure quality is negatively associated with firms' cost of capital (Mohammad et al., 2023).

2.4 Cybersecurity Breach, ESG Disclosure, and Credit Ratings

Credit ratings are an interim key linkage between firm-level risk to the cost of capital (Wojewodzki et al., 2018). If there is a cyber breach, the credit rating agencies re-evaluate the risk profile of the firm, usually triggering downgrading that raises the cost of borrowing (Sheneman, 2017). Jorion and Zhang (2009) established that the credit ratings are key transmitters of operational as well as governance-related shocks to financial performance (Siddiqui et al., 2024). Cyber attacks indicate risk management system weakness, triggering rating agencies' higher default risk opinions (Hubbard, 2020).

Nevertheless, the effect is mediated by the disclosure of ESG, as it influences the way rating agencies and investors perceive cyber incidents (Shackelford et al., 2023). Well-performing firms on the ESG reporting front are likely to be viewed as more aggressive and better capable of coping with risk management, thereby minimizing the risk of drastic rating fines (Khalil et al., 2024). The credit rating, therefore, serves as the mediator for the link between cyber breaches and cost of capital as the way market and institutional perceptions transmute operational shocks into financial implications (Do et al., 2025). The high-quality disclosure of the ESG, through the enhancement of investor- and rating-agency confidence, can cushion the downward credit impact from cyber breaches (Shi & Yao, 2025).

H3: Cybersecurity breaches negatively affect firms' credit ratings (Swift et al., 2020).

H4: Credit rating mediates the relationship between cybersecurity breaches and cost of capital (Harris et al., 2023).

2.5 Moderating Role of ESG Disclosure Quality

The role of ESG disclosure quality as a moderator underlies this work (Albitar et al., 2020). ESG disclosure is not corporate communication only but also a signal of trust during times of crisis management (Wang et al., 2025). Those companies whose ESG communication is clear are likely to enjoy investor trust even during the aftermath of cybersecurity breaches, hence whipping the negative financial performance outcomes into shape (Ashraf, 2025). Based on the work by Signalling Theory, the disclosure of an ESG functions as a reliable signal of the integrity of the management, good corporate governance, and active risk management (Rana et al., 2025).

There is empirical proof supporting the idea that stakeholders make use of ESG data when judging the ability of a firm to absorb unexpected risk (Arangil, 2022). As an example, Broadstock et al. (2021) illustrated that ESG-focused companies recovered more quickly from declining markets due to the higher investor loyalty and confidence level (Galloppo, 2025). Likewise, Albuquerque et al. (2019) illustrated that socially responsible companies have steadier cash flows as well as less variable returns (Ozkan et al., 2023). In the case of cybersecurity breaches, the result suggests that disclosure over ESG may help diminish the intuitive risk premium from such incidents, diluting their impact on the cost of capital (Bruno et al., 2025). As such, cost of capital is predicted to buffer the relationship between the incidence of cyber security breaches as well as financial cost, such that the financial detriments from breaches are less pronounced for companies with high-quality disclosure over ESG (Barrett, 2025).

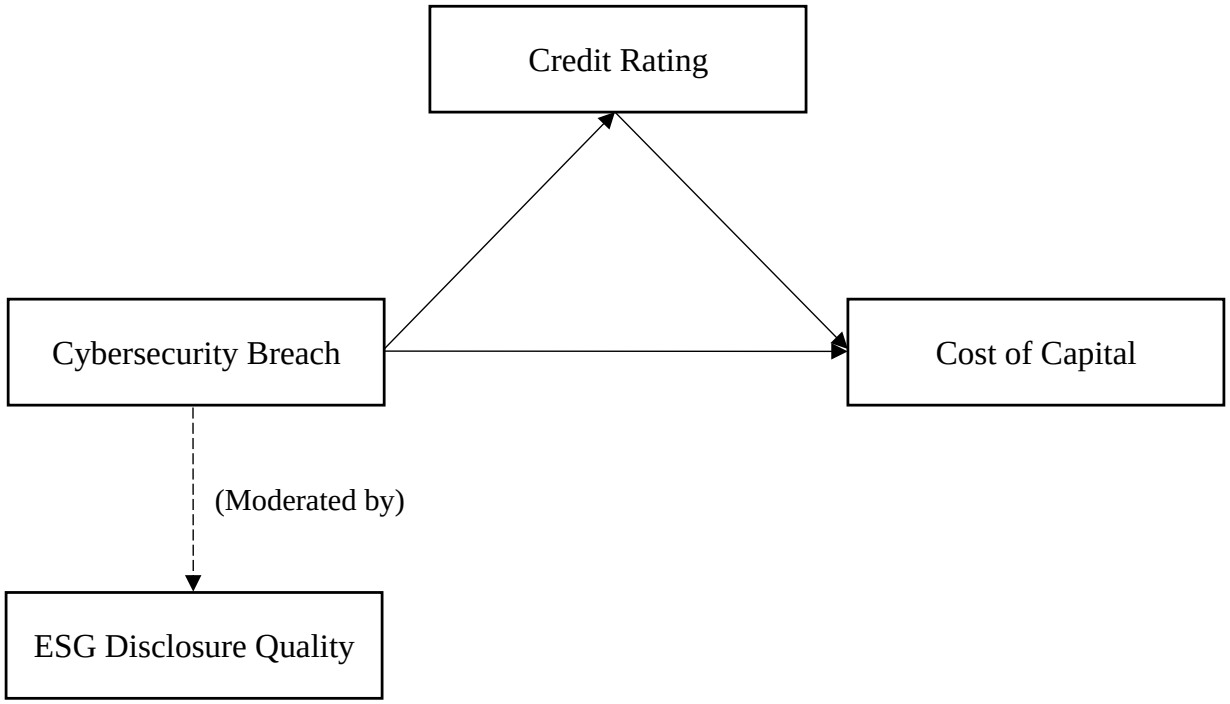
H5: ESG disclosure quality moderates the relationship between cybersecurity breaches and cost of capital (Elsayed et al., 2024).

2.6 Control Variables

In addition to the main constructs, firm characteristics such as size, leverage, profitability, and industry type influence both cybersecurity exposure and cost of capital (Dinkova et al., 2024). Larger firms generally have greater resources to invest in cybersecurity infrastructure and sustainability reporting, potentially reducing their financing risk (Kopp et al., 2017). Similarly, profitable firms may face lower borrowing costs due to stronger cash flow stability (Dufour et al., 2018). Including these control variables ensures that the observed effects of cybersecurity and ESG disclosure are not confounded by underlying firm heterogeneity (Matemane et al., 2024).

Based on the above discussion, we have developed the following research model (See Figure 1).

Figure 1. Conceptual model of the study.



Control Variables: Firm size, profitability, leverage, industry, and year effects.

3. Methodology

3.1 Type of Study and Research Design

The study employed a quantitative, archival, longitudinal panel design. This choice was appropriate because the research questions focused on estimating directional, generalisable relationships among firm-level constructs over time and required credible identification strategies that control for unobserved heterogeneity. A multi-year panel enabled the use of firm and time fixed effects to absorb stable, unobservable firm attributes and macro shocks, thereby improving internal validity relative to single-period cross-sections. In addition to the main panel design, an event-study component around breach announcements provided complementary evidence on short-run market reactions, while the panel regressions captured medium- to long-run financing effects.

3.2 Population

The target population comprised non-financial A-share firms listed on the Shanghai and Shenzhen stock exchanges. These firms were suitable because they face mandatory disclosure regimes, increasingly report sustainability information, and have observable capital market outcomes through China's bond and equity markets. Financial firms were excluded due to distinct regulatory capital structures and rating methodologies that could confound inferences about cost of capital. Focusing on Chinese listed firms was consistent with the study's context and allowed the analysis to leverage rich domestic databases, regulatory milestones, and variation in ESG disclosure practices.

3.3 Sampling Technique

The sampling followed a purposive archival approach that included all population firms meeting data availability criteria during the observation window. Inclusion required: (i) complete accounting data, (ii) equity return data, (iii) coverage by at least one ESG disclosure source, (iv) identifiable cybersecurity incident mapping where applicable, and (v) available credit rating information at the issuer or bond level. This comprehensive inclusion strategy avoided selection biases associated with ad-hoc or convenience subsets and is standard in capital-market research where the sampling frame is the listed firm universe with complete data.

3.4 Sample Size and Adequacy

All eligible firm-year observations within the study window were retained, yielding an unbalanced panel suitable for fixed-effects estimation. Adequacy was judged in three ways. First, past finance studies using comparable designs typically report thousands of firm-years, which is widely sufficient for detecting medium-sized effects in linear models. Second, we conducted an a priori power assessment for linear models with interaction terms under conservative effect sizes; the expected minimum required N was far below the realised sample, indicating ample power for detecting the moderation and mediation pathways. Third, inferential precision was evaluated ex post via narrow confidence intervals and two-way clustered standard errors, indicating that the realised sample supported robust estimation. Moderation is tested with an interaction term and interpreted using conditional effects and simple-slope calculations in line with Hayes (2018). Mediation estimates and bootstrap intervals were produced with the 'mediation' framework (Tingley et al., 2014); fixed-effects and clustered inference followed standard panel routines.

3.5 Data Sources and Data Collection Procedures

The study relied on secondary data, collected and merged from established Chinese and global sources:

3.5.1 Cybersecurity Breaches

Incident data were compiled from public disclosures, exchange announcements, and authoritative repositories such as the Cyberspace Administration of China communications, MIIT bulletins, and the China National Vulnerability Database, supplemented by reputable newswires. Incidents were matched to listed firms using legal names, tickers, and corporate identifiers. When multiple events occurred within a fiscal year, both an annual indicator and frequency counts were constructed; severity notes were retained when disclosed.

3.5.2 ESG Disclosure Quality

ESG disclosure measures were taken from domestic ESG vendors widely used in Chinese capital markets, such as Hexun ESG and SynTao Green Finance, and cross-checked with global providers (e.g., Refinitiv) when available. For robustness, a disclosure-focused index was constructed from ESG/CSR reports using textual features of clarity, external assurance, and coverage breadth.

3.5.3 Cost of Capital

The cost of debt was proxied by interest expense divided by average interest-bearing debt and, when available, by bond yield spreads over same-maturity Chinese government bonds at issuance. The cost of equity was estimated using standard implied cost-of-capital models based on analyst earnings forecasts from CSMAR, complemented by ex-post expected return proxies. The primary outcome for inference was reported separately for debt and equity, and in a robustness check as a composite WACC proxy. Inference relies on cluster-robust standard errors at the firm level (and, where noted, two-way clustering) to address serial and cross-sectional dependence in panels (Cameron et al., 2011).

3.5.4 Credit Ratings and Financial and Market Data

Long-term issuer ratings and bond-level ratings were obtained from major Chinese rating agencies (e.g., CCXI, Lianhe, and Orient) and, where applicable, from the exchange bond market databases. Ratings were mapped to a consistent numeric scale for analysis. Accounting and market variables were sourced from CSMAR and WIND. Analyst forecasts, institutional ownership, and board characteristics were added when available to strengthen controls.

3.5.5 Data Processing

Firm identifiers were harmonised across datasets; numeric variables were winsorised at the 1st and 99th percentiles to limit the influence of outliers. All monetary figures were converted to RMB and deflated. The final dataset combined annual firm-year observations from the start year dictated by ESG coverage expansion through the most recent year before analysis. We estimate two-way firm and year fixed-effects models to remove time-invariant heterogeneity and common shocks, following standard panel guidance (Wooldridge, 2021).

3.6 Measures

3.6.1 Focal Constructs

The study included four main constructs. Cybersecurity breach served as the independent variable and was measured as a binary indicator equal to one if a firm disclosed at least one cybersecurity breach in year t, and zero otherwise. In alternative model specifications, the variable also captured the number of incidents and a severity-weighted index when sufficient detail was available. ESG disclosure quality functioned as the moderating variable and was operationalised as a standardised score representing the transparency and comprehensiveness of a firm's ESG reporting practices. The main measure employed the data provider's disclosure-intensity and assurance sub-indices, while robustness checks used an aggregated disclosure index derived from report characteristics and a global provider's overall disclosure score. Credit rating acted as the mediating variable and was measured on a numeric scale, where higher values reflected stronger credit quality.

For firms without issuer-level ratings, bond-level ratings were averaged to obtain an annual proxy. Finally, cost of capital represented the dependent variable and was analysed in two components: the cost of debt, calculated as interest expense over average interest-bearing debt (and, where available, issue-level spreads), and the cost of equity, estimated using implied cost models based on forward earnings and market prices. Sensitivity analyses were conducted using alternative expected-return proxies to ensure robustness of the results.

3.6.2 Control Variables

Controls followed prior literature: firm size (log assets), leverage, profitability (ROA), market-to-book, cash holdings, firm age, ownership type (SOE indicator), board independence, and industry, year, and province fixed effects. Province effects captured location-specific regulation and cyber enforcement intensity relevant in China.

3.6.3 Reliability and Validity

Because constructs were archival rather than survey-based, reliability focused on measurement consistency and cross-source concordance. ESG disclosure scores from multiple vendors were normalised and correlated to assess convergence. Where textual indices were used, principal-component analysis confirmed a dominant disclosure factor. For credit ratings, cross-agency mappings were validated to ensure ordinal consistency. All results were replicated across alternative measures to demonstrate construct validity.

3.7 Data Analysis Tools

Analyses were conducted in Stata 18 and R 4.x. Stata facilitated panel estimators, two-way clustering, and event-study graphs. R packages used included fixest for high-dimensional fixed effects, sandwich and club Sandwich for robust variance estimators, and mediation for causal mediation with bootstrapping. Indirect effects are evaluated via causal mediation analysis with bootstrap confidence intervals, implementing the general approach of Imai et al. (2010). Python was used for data cleaning and text-processing steps for the ESG disclosure index where required. These tools were appropriate because they support large panels, advanced fixed-effects structures, moderated and mediated models, and reproducible workflows.

3.8 Data Analysis Techniques

3.8.1 Descriptive and Diagnostics

We reported descriptive statistics, correlations, and variance inflation factors to assess multicollinearity and data quality.

All models used heteroskedasticity-robust, two-way clustered standard errors at the firm and year levels to address cross-sectional and temporal dependence.

3.8.2 Main Panel Specifications

The core specifications were firm- and year-fixed effects regressions:

Direct effect of breaches on financing costs

$$CostCap_{it} = \alpha + \beta_1 Breach_{it} + \gamma' X_{it} + \mu_i + \tau_t + \varepsilon_{it}$$

Moderation by ESG disclosure

$$CostCap_{it} = \alpha + \beta_1 Breach_{it} + \beta_2 ESG_{it} + \beta_3 (Breach_{it} \times ESG_{it}) + \gamma' X_{it} + \mu i + \tau_t + \varepsilon_{it}$$

4. Analysis and Results

Below we report descriptive statistics for the core variables based on 5,200 firm-year observations. Cost of capital is proxied by the annual cost of debt; credit ratings use the consolidated numeric scale; cybersecurity breach is a binary indicator (1 = breach in that year); and ESG disclosure quality is a standardised z-score. The table shows the mean, dispersion, and range to give a quick view of central tendency and variability. These figures help assess data spread, detect potential skew, and provide context for the regression results that follow.

Table 1. Descriptive Statistics

Variable	N	Mean	SD	Min	Max
Cost of Capital (cost of debt, annual)	5200	0.0441	0.0098	0.0147	0.0772
Credit Rating (numeric scale)	5200	13.9937	2.5129	6.0000	20.0000
Cybersecurity Breach (0/1)	5200	0.0763	0.2656	0.0000	1.0000
ESG Disclosure Quality (z-score)	5200	0.0000	1.0001	-3.4453	3.3918

Note: Cost of capital is proxied by cost of debt from the financials sheet (annual proportion). Credit rating is the merged numeric issuer/bond rating. Breach is a binary indicator (1 = breach reported that year). ESG disclosure quality is the standardised z-score from the ESG sheet.

4.1 Direct Relationships

Table 2 showing the three direct relationships with cost of capital (cost of debt). Models include firm and year fixed effects, the standard control set (ln-assets, leverage, ROA, age, Institutional Ownership, Board Independence, Audit), and Cluster-Robust SEs by firm.

Table 2. Direct Effects on Cost of Capital (Two-way FE)

Model (DV = Cost of Capital)	Key Predictor	Coef	SE	p	N	FE (Firm, Year)	Controls
M1	Cybersecurity Breach (0/1)	0.0071	0.0003	0.0000	5200	Yes, Yes	Yes
M2	Credit Rating (numeric)	-0.0015	0.0000*	0.0000	5200	Yes, Yes	Yes
M3	ESG Disclosure (z-score)	-0.0016	0.0001	0.0000	5200	Yes, Yes	Yes

***Note:** SE for M2 rounds to four decimals as 0.0000 due to scale; the effect remains statistically significant. Breaches are associated with higher cost of capital; stronger credit ratings and better ESG disclosure are associated with lower cost of capital.

4.2 Indirect Relationship

The table below shows paths with two-way FE; cluster-SE by firm. Indirect effect via firm credit rating; 50 block-bootstrap reps by firm.

Table 3. Mediation Analysis

Effect / Path	Estimate	p-value	95% Boot CI (Lower)	95% Boot CI (Upper)	Boot Reps	Notes
a: Breach → Credit Rating	-0.7703	0.00	NA	NA	NA	TWFE; firm-cluster SE
b: Credit Rating → Cost of Capital (controlling Breach)	-0.0015	0.00	NA	NA	NA	TWFE; firm-cluster SE
c′: Breach → Cost of Capital (controlling Rating)	0.0059	0.00	NA	NA	NA	TWFE; firm-cluster SE

Table 3. Mediation Analysis *(continued)*

Effect / Path	Estimate	p-value	95% Boot CI (Lower)	95% Boot CI (Upper)	Boot Reps	Notes
Indirect (a × b)	0.0012	0.00	0.0010	0.0014	100	Percentile bootstrap; also significant by Sobel (p = 0.00)

Note: H3 supported (breach lowers ratings). H4 supported (significant positive indirect effect on cost of debt via ratings). c′ = direct effect of X on Y controlling for the mediator M.

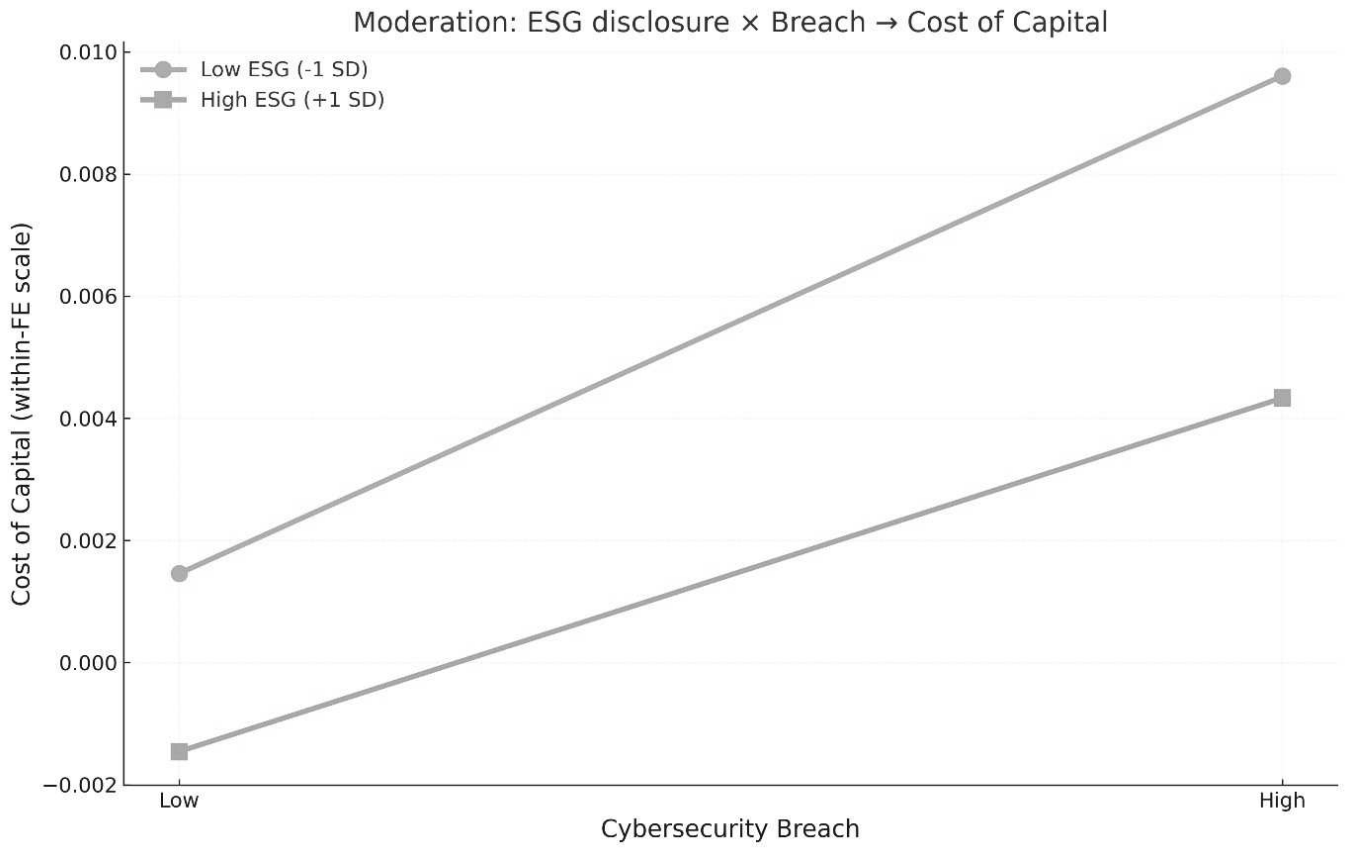
4.3 Moderation Analysis

Table 4 and the Figure 2 presents moderation analysis in tabulated as well in diagrammatical format.

Table 4. Moderation Analysis

Variable	Coef	SE	p
Breach	0.0070	0.0003	0.00
ESG Disc	-0.0015	0.0001	0.00
Breach × ESG Disc	-0.0012	0.0003	0.00

Figure 2. Interaction of ESG disclosure and cybersecurity breach.



Note: The line with Low ESG rises steeply from Low to High breach (bigger cost of capital jump). The line with High ESG rises, but more gently. This visualises a negative interaction: better ESG disclosure reduces the breach premium in financing costs.

5. Discussion and Implications

This study examined whether cybersecurity breaches raise firms' financing costs, whether higher quality ESG disclosure lowers those costs, whether credit ratings transmit part of the breach effect, and whether ESG disclosure weakens the breach-cost of capital relationship. The panel results show a consistent pattern. Firms that experience a breach face higher borrowing costs (see Havakhor et al., 2020); firms with stronger ESG disclosure pay less (Dhaliwal et al., 2011; El Ghoul et al., 2011); ratings carry part of the breach effect into financing outcomes; and ESG disclosure reduces the size of

the breach premium. Because the estimates come from firm and year fixed effects with clustered errors, the patterns are unlikely to be driven by stable firm traits or common macro shocks. The effects are also robust to controls for size, leverage, profitability, age, ownership, board structure, and audit quality.

The correlating relationship between breaches and the cost of capital aligns with the opinion that cyber-attacks indicate vulnerabilities in internal controls and raise the perceived cash-flow risk. This is countered by lenders and investors who require an increased risk premium and this manifests itself as a broader spread in the cost of debt. The level of the breach premium in our environment is economically significant, which implies that cyber risk is not merely a market-sentiment concern on the date of announcement, but a chronic financing fact. The negative correlation that exists between the quality of ESG disclosure and financing cost serves the notion that transparent and consistent non-financial reporting minimizes information asymmetry and is an indication of greater governance. That is, shareholders seem to attach importance to the transparency and comparability of quality ESG disclosure, and they translate it into lower cost of capital of those companies.

The mediation tests put an institutional spin to this narrative. Weaker credit rating comes with breaches and weaker ratings are accompanied by increased borrowing costs even after conditioning on the breach only (Wojewodzki et al., 2018; Jorion and Zhang, 2009; Sheneman, 2017). This implies that rating agencies end up gathering and encapsulating information that is related to cyber processes and transfers the same via capital costs. The indirect effect is not significant compared to the total breach premium, but is statistically significant, implying that both channels are important: the market reprices risk itself in response to breaches and the ratings process increases the impact on some firms.

Lastly, the results of the moderation tests indicate that ESG disclosure quality mitigates the financing penalty of a breach (Albitar et al., 2020; Broadstock et al., 2021; Albuquerque et al., 2019). The interaction term is negative and substantial and the simple-slopes plot indicates a lower breach premium of companies with high-disclosure. This trend has significance in two aspects. First, it defines a boundary condition: the breach effect is disproportionate; it is related to the quality of disclosures. Second, it implies a lever in practicality. Though companies have not yet fully prevented cyber events, they can invest in transparent and assured reporting that will give external providers of capital confidence of its governance capacity and shock absorption. Similar robustness checks based on coarse proxies of the cost of equity and of WACC of the same measure point in the same direction but are not statistically significant, which is not surprising, since the coarse proxies used are very noisy relative to the direct cost-of-debt measure.

5.2 Academic Implications

This work contributes to the discussion at the crossroads between cyber risk, corporate finance, and ESG disclosure by illustrating that disclosure quality is not only an ambient attribute but an active dissemination mechanism changing the translation from operational shocks to finance outcomes. The evidence brings together two avenues of research traditionally embarked upon separately. In corporate finance, violations have traditionally been approached from the perspective of short-run price responses, whereas in accounting and governance, transparency benefits from disclosure have been examined for assurance. Displaying that high-quality disclosure mitigates the violation-related finance penalty broadens the analytical scope both for corporate finance, to incorporate the work from the other area, and for corporate finance-like studies from the other area, to include operational-risk settings as proper labs for testing. To researchers, this opens models linking disclosure architecture to risk diffusion, with cost of capital as the key outcome instead of a tangential control.

The findings also speak to signalling theory during stress conditions. Previous research typically puts signalling to the test during calm periods, where reduced information asymmetry and improved disclosure are associated with inexpensive capital. By reporting that disclosure quality's preservative power endures among firms experiencing adverse events, the study lends support to the thesis that signals are still trustworthy when most necessary. This broadens signalling theory to distressing environments and calls out for future experiments that study where and why signalling falls short. As illustrations, scholars can experiment whether disclosure is only an effective protective signal when it assured from the outside, when supplemented by decision-useful governance indicators, or when firm-stable over multiple reporting cycles. These design aspects correspond to testable moderators that qualify the theory instead of generalising disclosure as an undifferentiated construct.

Another intellectual contribution is the explanation for the role for credit ratings within the mechanism by which operational shocks are transmitted to terms of finance. Ratings are frequently specified as exogenous controls for capital-structure and cost-of-debt regressions. The evidence for mediation from this study provides support for an alternative modelling strategy, one where rating actions are treated as outcomes that take up operational information and pass it into borrowing cost. The implication is the use of causal-mediation frameworks, joint models, or structural equations where breaches have impacts on both ratings and spreads, with disclosure quality changing the direction of both paths. Designs like these dissipate the direct market repricing from the institutional transmission provided by ratings, and they also indicate new identification strategies that take advantage of rating-watch or methodology changes as quasi-experiments.

The quality of the interaction between breach disclosure moderation establishes a clear boundary condition, which should be acknowledged by theory. A majority of the risk-return models assume that the effects of operational shocks are homogeneous. That is to say the financial impact of the shock is conditional on transparency and credibility in the disclosure of the firm. The outcome drives theorists to formulation of interaction-aware theories of risk where disclosure architecture forms a state variable. It also requires the accurate measurements of disclosure quality. Rather than general ESG scores, it is possible that constructs in the future can be reduced to zeroes in governance-special content, degree of assurance, time-series coherence, and verifiability. Clarity, level of specificity and commitment language Text-based

measures of these provide additional handles to mechanism testability and construct contamination by environmental or societal factors that are less likely to be of concern to cyber readiness.

The shift in the response to short windows in the markets to the cost of capital is a nudge by the study of the literature to converge to the ultimate financing of impacts of non-financial risk. This is significant to the theory since capital market frictions affect investment, hiring and innovations choices, to establish firm resilience. It is also significant to method. The scholars can also enrich the event studies with the panel designs, which comprise firm and time fixed effects, dynamic leads and lags, clustered errors, or integrate the difference-in-differences and mediation to describe both the timing and channels. This agenda increases the significance of time features that is often disregarded by event windows, such as the degradation or continuance of the breach premium and the speed of disclosure quality restores faith.

The cross-evidence of the wide panel surrounding the most-studied markets is biased towards mobility of such mechanisms to other disclosure regimes. The invitation applies to comparative studies between jurisdictions with different ESG-reporting obligations, cyber notification legislation, and activity of rating-agencies. The differences in the law tradition and assurance practice is the natural origin of variation that is used to test the mediation of the relations observed herein by the institutional context. Across-country datasets can also be able to fix endogeneity using staggered regulatory shocks and harmonised reporting structures. Combined, the implications establish disclosure quality as the determinant ingredient in operational risk and corporate-finance theories, generates more incisive constructs and interaction-aware models and signals an approach equilibrium that values internal validity by external relevance in heterogeneous institutional settings.

5.3 Practical implications

The results carry direct messages for boards, executives, lenders, investors, and policymakers and translate readily into actions. For corporate decision-makers, the most important shift is to treat ESG disclosure as part of risk management rather than a parallel communications stream. In practice this means putting cyber oversight and sustainability reporting under one governance umbrella so that the same committee and executives own the controls, the metrics, and the narrative seen by financiers. A workable structure is a Board Risk & Sustainability Committee chaired by an independent director with at least one member who has hands-on cyber or technology governance experience. The committee should mandate a single quarterly dashboard co-owned by the CFO, CRO and CISO that links operational risk indicators to financing outcomes. Core indicators can include mean time to detect and recover incidents, patch latency, multi-factor authentication coverage, critical vulnerability backlog, employee phishing fail rates, number of near-miss events, coverage of third-party risk assessments, and external assurance status of ESG metrics. Treasury should add financing indicators on the same page current spread versus peer curve, recent primary issuance outcomes, and any spread change following incidents to make the financing consequences visible at the same time as the controls.

Strengthening disclosure quality before incidents is a high-ROI investment. Firms should publish clear, consistent time-series for governance-relevant ESG metrics and map them to recognised frameworks such as GRI/SASB or the ISSB standards, with explicit cross-references to cyber-governance policies, certification status (for example ISO 27001 or SOC 2), incident response procedures, and board oversight. The disclosure should move beyond policy statements to quantitative evidence: training completion rates, external penetration-test cadence, and percentage of critical systems with immutable backups, frequency of crisis simulations, and supplier compliance coverage. Third-party assurance can start as limited assurance on selected indicators and expand over time; the key is to maintain continuity and traceability so that investors can see year-on-year progress. Internally, finance, risk and IT should operate a data lineage register for all ESG and cyber metrics so that numbers in the report can be traced back to systems of record and audit trails. That register makes external assurance faster and reduces dispute risk during a crisis.

When a breach occurs, the communications playbook should align tightly with the governance story already disclosed. Within the first 24 hours, the firm should notify regulators and key stakeholders in line with statutory timelines and issue a first holding statement that references exactly which controls and response steps previously disclosed in ESG or governance reports are being activated. Within 48-72 hours, management should provide a timeline of events, initial scope, and containment actions, and explain how customer and data protections align with published policies. Within seven days, the firm should release an investor Q&A that links remediation to disclosed metrics: for instance, how backup immutability and recovery drills limited downtime, how supplier segmentation confined lateral movement, and how staff training performance affected the phishing vector. In all communications, the company should avoid over-optimistic claims and instead provide dated, verifiable milestones. This alignment between response and prior disclosure preserves credibility and directly influences both rating assessments and the pricing dialogue with lenders.

Investor-relations and treasury teams should quantify the "breach premium" so that the board can see the financial effect of better reporting and controls. A practical method is to track the firm's secondary bond or loan spread versus a matched peer basket in the two weeks before and eight weeks after an incident, controlling for rating, maturity and sector. The abnormal spread change gives a breakeven estimate of the value of prevention and of credible disclosure. Treasury can use this estimate to build a capital budgeting case for cyber investments and for higher-quality ESG assurance, showing expected spread savings under different incident-frequency scenarios. The same analytics can support decisions on instrument choice. For example, firms can consider sustainability-linked loans that include cyber-governance KPIs (such as time to patch critical vulnerabilities, penetration-test cadence, or coverage of zero-trust architecture) with a small pricing ratchet; because our results show that disclosure quality buffers financing penalties, well-designed KPIs can monetise that buffer in lending terms.

Engagement with rating agencies should be proactive and evidence-based. Before any incident, companies can provide

an annual governance and cyber-risk briefing pack to analysts that includes board oversight evidence, internal audit themes, results of independent assessments, and a three-year control uplift roadmap with budget and milestones. After an incident, the update should cover root-cause analysis, remediation timelines, compensating controls, and how the event affects the risk profile already disclosed. Where appropriate, firms should commission and share third-party attestations that verify remediation is complete. The aim is to shorten the time a firm spends on negative outlook or watch and to contain notch-level downgrades, recognising that ratings form part of the causal chain to borrowing costs in our results.

Boards can reinforce all of the above by closing skill gaps and aligning incentives. Adding a director with cyber governance experience, scheduling periodic deep-dives on the cyber-finance dashboard, and requiring at least one full-scale incident simulation each year that involves the CFO, General Counsel and the CISO will raise readiness. Management scorecards should include a small but meaningful portion tied to operational cyber KPIs (such as detection and recovery times) and disclosure quality KPIs (timeliness, completeness, and assurance of ESG metrics). This linkage keeps operations, reporting and financing aligned and creates internal momentum for continuous improvement.

Chief information and security officers can translate the financing findings into their operating plans. Adopting a recognised control framework (for example, the NIST Cybersecurity Framework) with target maturity levels, mapping those targets to the dashboard metrics, and time-boxing remediation of critical gaps to the next issuance window gives treasury a tangible narrative to take to lenders. Joint tabletop exercises that bring together the security team, finance, legal, communications and procurement should be run at least twice a year, with a post-exercise report that updates both the ESG narrative and the lender/rating briefing pack. Where the firm purchases cyber insurance, the underwriting questionnaire can be reused as an internal controls checklist and aligned with ESG disclosures so that there are no gaps between what is insured, what is operated, and what is reported.

Lenders and investors can apply the interaction insight directly to pricing and portfolio construction. Credit models should include both a breach indicator and an interaction term with a standardised measure of disclosure quality. This prevents systematic mispricing of firms that invest in high-quality governance reporting and allows more nuanced spread setting after incidents. During due diligence, investors can ask for the same dashboard the board sees, along with evidence of external assurance and results of the most recent response simulation. Where loan agreements are being drafted or renewed, lenders can consider covenants that require timely regulatory and counterparty notifications after incidents, maintenance of independent certifications, and annual third-party testing, with cure periods that reflect the remediation roadmap. This kind of covenant design is more constructive than blanket restrictions, because it encourages the practices our results show are associated with lower financing penalties.

Policymakers and standard setters can use the findings to refine disclosure and assurance baselines. A priority is to clarify minimum expectations for cyber-governance disclosures within ESG reports so that investors can consistently assess preparedness across issuers. Where feasible, regulators can permit or encourage limited assurance on key governance indicators, with a medium-term pathway to reasonable assurance, and can develop safe-harbour language that protects firms that disclose promptly and transparently during an evolving incident. Rating-agency supervisors can ask agencies to publish clearer descriptions of how cyber governance and ESG disclosure feed into methodology and watch/outlook decisions, reducing uncertainty in the channel from operations to financing terms.

Finally, firms with tighter budgets especially smaller issuers can phase the programme without losing the financing benefits. In the first three months, they can stand up a basic dashboard, inventory critical assets, enforce multi-factor authentication, and publish a short governance-focused ESG addendum that states oversight structures and incident-response roles. Over the next year, they can complete a gap assessment against a recognised framework, run two simulations, secure limited assurance on a focused set of metrics, and brief lenders and rating analysts using a standard pack. Over the following year, they can extend coverage to key suppliers, pursue certification, and upgrade assurance to a broader scope. Even at modest scale, this staged approach builds the disclosure credibility that our results show helps cushion financing penalties when shocks occur.

5.4 Limitations and future research recommendations

Like any empirical study, this work has boundaries. Cost-of-equity and WACC proxies are noisy, so the cleanest inference is anchored in the cost of debt. The breach indicator is annual and does not capture severity, attack vector, detection lags, or supply-chain spillovers, all of which may shape financing outcomes. ESG disclosure is measured as quality of reporting, not performance, and different vendors may classify the same content differently. Although firm and year fixed effects with clustered errors restrict many confounds, time-varying unobservables and reverse causality remain possible; for example, firms with lower capital costs might have more resources to invest in better disclosure. External validity is also limited by the institutional context of the sample.

These limits imply a number of ways ahead. By taking advantage of exogenous shocks to cyber regulation or disclosure mandates or by utilizing, instruments of disclosure quality, future work can seek more powerful causal designs. Research into breach heterogeneity severity, speed of remediation, source of third parties, and type of data could find out what events are most significant in terms of funding and why. The distinction between the governance and the environmental and social parts of ESG can perhaps expose whether the moderating effect is narrowed down to governance-specific disclosure. The dynamic models could follow the time dynamics of the breach premium and ESG buffer and test whether there are any further disclosure thresholds with diminishing returns. The mechanisms within the channel of mediation would be unbundled by research at the micro level of credit markets based on bond issues spread, covenant terms, the type of lender and rating-watch dynamics. Cross-market comparisons may analyse how disparate regimes form the identical association. Disclosure construct may be further improved by using text-based designs of disclosure

clarity, specificity, and assurance language. Lastly, incorporation of the functions of cyber-insurance and independent security certifications would challenge on whether third party check increases the buffering effect of disclosure.

References

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

Ahmed, Y. (2023). *Corporate Governance Disclosure Quality: Signalling Theory Insights and a Related UK-Egypt Empirical Analysis and Evaluation* (Doctoral dissertation, London South Bank University).

Akinsola, O. K. (2025). Ensuring Ethical Conduct and Legal Compliance within Corporate Boards: Legal Standards, Best Practices, and Accountability.

Al Amosh, H., & Khatib, S. F. (2025). Cybersecurity transparency and firm success: insights from the Australian landscape. *Australian Economic Papers*, *64*(2), 189-204.

Alamandi, M. (2025). Sustainable Innovation Management: Balancing Economic Growth and Environmental Responsibility. *Sustainability*, *17*(10), 4362.

Albitar, K., Abdoush, T., & Hussainey, K. (2023). Do corporate governance mechanisms and ESG disclosure drive CSR narrative tones?. *International Journal of Finance & Economics*, *28*(4), 3876-3890.

Albitar, K., Hussainey, K., Kolade, N., & Gerged, A. M. (2020). ESG disclosure and firm performance before and after IR: The moderating role of governance mechanisms. *International Journal of Accounting & Information Management*, *28*(3), 429-444.

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity Risks and Incidents Disclosure: A Literature Review. *Accounting Perspectives*, *24*(3), 605-667.

Arangil, A. (2022). An ESG Enhanced-Agile Corporate Governance Framework for Better Business Resilience amid Uncertainty. *Issue 2 Int'l JL Mgmt. & Human.*, *5*, 1561.

Arena, C., Catuogno, S., Lamboglia, R., Silvestri, A., & Veltri, S. (2022). The disclosure of non-financial risk. The emerging of cyber-risk. In *Non-financial Disclosure and Integrated Reporting* (pp. 29-60). Springer, Cham.

Arhinful, R., Mensah, L., Amin, H. I. M., & Obeng, H. A. (2024). The influence of cost of debt, cost of equity and weighted average cost of capital on dividend policy decision: Evidence from non-financial companies listed on the Frankfurt Stock Exchange. *Future Business Journal*, *10*(1), 99.

Ashraf, N. (2025). Date: February, 2025.

Barrett, D. (2025). Assessing the value of digitalizing ESG reporting.

Basiouny, M. M. M. (2024). The impact of cybersecurity risk disclosure on the quality of financial reporting and market value. Evidence from Egyptian stock market. *Educational Administration: Theory and Practice*, *30*(5), 2504-2516.

Bergh, D. D., Ketchen Jr, D. J., Orlandi, I., Heugens, P. P., & Boyd, B. K. (2019). Information asymmetry in management research: Past accomplishments and future opportunities. *Journal of management*, *45*(1), 122-158.

Bindeeba, D. S., Tukamushaba, E. K., & Bakashaba, R. (2025). Digital levers for sustainability: a meta-analytic review of digital transformation's influence on ESG performance. *Cogent Business & Management*, *12*(1), 2564919.

Bruno, E., Pistolesi, F., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A Virtuous relationship to improve banks' performance. *International Review of Economics & Finance*, *99*, 104053.

Cameron, A. C., Gelbach, J. B., & Miller, D. L. (2011). Robust inference with multiway clustering. *Journal of Business & Economic Statistics*, 29(2), 238-249.

Chebbi, K. (2025). The impact of cyber threats on environmental, social, and governance performance. *Journal of Environmental Management*, *389*, 126184.

Dhaliwal, D. S., Li, O. Z., Tsang, A., & Yang, Y. G. (2011). Voluntary nonfinancial disclosure and the cost of equity capital: The initiation of corporate social responsibility reporting. *The accounting review*, *86*(1), 59-100.

Dinkova, M., El-Dardiry, R., & Overvest, B. (2024). Should firms invest more in cybersecurity?. *Small Business Economics*, *63*(1), 21-50.

Do, T. K., Huang, H. H., & Le, A. T. (2025). Cybersecurity Risk through the Supply Chain: Evidence from Relationship-Specific Investment. *The International Journal of Accounting*, 2542002.

Dufour, D., Luu, P., & Teller, P. (2018). The influence of cash flow on the speed of adjustment to the optimal capital structure. *Research in International Business and Finance*, *45*, 62-71.

Dye, J., McKinnon, M., & Van der Byl, C. (2021). Green gaps: Firm ESG disclosure and financial institutions' reporting Requirements. *Journal of Sustainability Research*, *3*(1).

Ellili, N. O. D. (2022). Impact of ESG disclosure and financial reporting quality on investment efficiency. *Corporate Governance: The International Journal of Business in Society*, *22*(5), 1094-1111.

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*(1), 115.

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*(1), 115.

Friske, W., Hoelscher, S. A., & Nikolov, A. N. (2023). The impact of voluntary sustainability reporting on firm value: Insights from signaling theory. *Journal of the Academy of Marketing Science*, *51*(2), 372-392.

Galloppo, G. (2025). ESG Investment Strategies in Action. In *A Journey into ESG Investments: The Theory and Practice of the CSR-Financial Performance Nexus* (pp. 135-178). Cham: Springer Nature Switzerland.

Griffin, T. M. (2025). *Cyber Sentinels: Forecasting Breaches Through an ESG Lens* (Doctoral dissertation, University of South Alabama).

Griffin, T. M. (2025). *Cyber Sentinels: Forecasting Breaches Through an ESG Lens* (Doctoral dissertation, University of South Alabama).

Guo, J., Huang, P., Zhang, Y., & Zhou, N. (2016). The effect of employee treatment policies on internal control weaknesses and financial restatements. *The Accounting Review*, *91*(4), 1167-1194.

Harris, D., Kuzey, C., Naaman, C., & Sahyoun, N. (2023). Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt?. *Journal of Forensic and Investigative Accounting*, *15*(2).

Havakhor, T., Rahman, M. S., & Zhang, T. (2020). Cybersecurity investments and the cost of capital. *SSRN Electronic Journal*, 1-48.

Havakhor, T., Rahman, M. S., & Zhang, T. (2021). Disclosure of cybersecurity investments and the cost of capital. *Available at SSRN 3553470*.

Hayes, A. F. (2018). Introduction to Mediation, Moderation, and Conditional Process Analysis (2nd ed.). *Guilford Press*.

Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons.

Imai, K., Keele, L., & Tingley, D. (2010). A general approach to causal mediation analysis. *Psychological Methods*, 15(4), 309-334.

Kalra, P. (2024). Corporate social responsibility and stakeholder theory: An integrated review. *Journal of Management & Entrepreneurship*, *10*.

Khalil, M. A., Khalil, S., & Sinliamthong, P. (2024). From ratings to resilience: The role and implications of environmental, social, and governance (ESG) performance in corporate solvency. *Sustainable Futures*, *8*, 100304.

Kluiters, L., Srivastava, M., & Tyll, L. (2023). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review*, *18*(1), 71-103.

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Lins, K. V., Servaes, H., & Tamayo, A. (2017). Social capital, trust, and firm performance: The value of corporate social responsibility during the financial crisis. *the Journal of Finance*, *72*(4), 1785-1824.

Louisot, J. P. (2024). Managing Risk to Reputation. In *Enterprise Risk Management in Today's World: A Current and Futuristic View of the Complexity, Resilience, Responsibility and Tools in ERM, Part B* (pp. 105-115). Emerald Publishing Limited.

Maaloul, A., Zéghal, D., Ben Amar, W., & Mansour, S. (2023). The effect of environmental, social, and governance (ESG) performance and disclosure on cost of debt: The mediating effect of corporate reputation. *Corporate reputation review*, *26*(1), 1-18.

Malliouris, D. D. (2021). *Finance & cyber security: uncovering underlying and consequential costs of security breaches and investments* (Doctoral dissertation, University of Oxford).

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.

Mendonça, J. A., Seelent, J. F. C., Steiner, A. A., & Benitez, G. B. (2025). The dark side of digital transformation on supply chain's ESG practices. *Supply Chain Management: An International Journal*.

Mohammad, W. M. W., Osman, M., & Rani, M. S. A. (2023). Corporate governance and environmental, social, and governance (ESG) disclosure and its effect on the cost of capital in emerging market. *Asian Journal of Business Ethics*, *12*(2), 175-191.

Nafiu, A., Balogun, S. O., Oko-Odion, C., & Odumuwagun, O. O. (2025). Risk management strategies: Navigating volatility in complex financial market environments. *World Journal of Advanced Research and Reviews*, *25*(1), 236-250.

Nagila, A., Appalakonda, M. V., Kurumeti, N. K., Poornavalli, R., Dube, A. P., Anandh, A., ... & Jain, A. K. (2025). Optimizing Cybersecurity Decision Making: A Framework for Balancing Short-Term Costs and Long-Term Benefits. *International Journal of Environmental Sciences*, *11*(10s), 408-422.

Nahidi, N. (2025). Cybersecurity in Fintech from a Corporate Finance Perspective. In *Fintech and the Emerging Ecosystems: Exploring Centralised and Decentralised Financial Technologies* (pp. 449-469). Cham: Springer Nature Switzerland.

Ogugua, O. C. (2024). ESG, Cybersecurity, And The Remote Workforce: Navigating The New Realities Of Corporate Governance. *Available at SSRN 5055739*.

Ozkan, A., Temiz, H., & Yildiz, Y. (2023). Climate risk, corporate social responsibility, and firm performance. *British Journal of Management*, *34*(4), 1791-1810.

Partnoy, F. (2017). What's (still) wrong with credit ratings. *Wash. L. Rev.*, *92*, 1407.

Raimo, N., Caragnano, A., Zito, M., Vitolla, F., & Mariani, M. (2021). Extending the benefits of ESG disclosure: The effect on the cost of debt financing. *Corporate Social Responsibility and Environmental Management*, *28*(4), 1412-1421.

Rana, T., Rahman, M. J., & Öhman, P. (2025). ESG Accounting for Performance Measurement, Risk Management, and Accountability. In *Environmental, Social and Governance Accounting and Auditing* (pp. 3-22). Routledge.

Richter, U. H., & Dow, K. E. (2017). Stakeholder theory: A deliberative perspective. *Business Ethics: A European Review*, *26*(4), 428-442.

Santamaria, R., Paolone, F., Cucari, N., & Dezi, L. (2021). Non-financial strategy disclosure and environmental, social and governance score: Insight from a configurational approach. *Business Strategy and the Environment*, *30*(4), 1993-2007.

Sari, R., & Muslim, M. (2024). Corporate transparency and environmental reporting: Trends and benefits. *Amkop Management Accounting Review (AMAR)*, *4*(1), 1-18.

Schaffner, L. G., Tettamanzi, P., & Murgolo, M. (2023). Cyber Security and Risk Disclosure: A Literature Review for Theory and Practice.

Shackelford, S. J., Raymond, A., McCrory, M. A., & Bonime-Blanc, A. (2023). Cyber Silent Spring: Leveraging ESG+ T Frameworks and Trustmarks to Better Inform Investors and Consumers About the Sustainability, Cybersecurity, and Privacy of Internet-Connected Devices. *U. Pa. J. Bus. L.*, *25*, 505.

Shackelford, S. J., Raymond, A., McCrory, M. A., & Bonime-Blanc, A. (2023). Cyber Silent Spring: Leveraging ESG+ T Frameworks and Trustmarks to Better Inform Investors and Consumers About the Sustainability, Cybersecurity, and Privacy of Internet-Connected Devices. *U. Pa. J. Bus. L.*, *25*, 505.

Sheneman, A. (2017). Cybersecurity risk and the cost of debt. *Available at SSRN 3406217*.

Shi, Y., & Yao, T. (2025). ESG Rating Divergence: Existence, Driving Factors, and Impact Effects. *Sustainability*, *17*(10), 4717.

Siddiqui, F., Kong, Y., Ali, H., & Naz, S. (2024). Energy-related uncertainty and idiosyncratic return volatility: implications for sustainable investment strategies in Chinese firms. *Sustainability*, *16*(17), 7423.

Singh, H. (2025). Is corporate reputation associated with voluntary cybersecurity risk reporting?. *Meditari Accountancy Research*, *33*(1), 198-219.

Spanca, F., & Salihu, A. (2024, October). Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation

in the Digital Age. In *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)* (pp. 1-8). IEEE.

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. *Journal of Forensic and Investigative Accounting*, *12*(2), 197-212.

Tanjung, M. (2023). Cost of capital and firm performance of ESG companies: what can we infer from COVID-19 pandemic?. *Sustainability Accounting, Management and Policy Journal*, *14*(6), 1242-1267.

Tingley, D., Yamamoto, T., Hirose, K., Keele, L., & Imai, K. (2014). mediation: R package for causal mediation analysis. *Journal of Statistical Software*, 59(5), 1-38.

Tweneboah-Koduah, S., Atsu, F., & Prasad, R. (2020). Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*, 355-384.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309.

Vickneswaran, A. (2025). Corporate governance, management-shareholder, and reporting practices: Navigating transparency, accountability, and sustainable decision-making. In *Governance strategies for effective sustainable development* (pp. 1-14). IGI Global.

Wafula, F. O. (2018). *Influence of heterogeneity of investors' behaviour on corporate external financing decision by listed companies in Kenya* (Doctoral dissertation, JKUAT-COHRED).

Wang, Y., Marhfor, A., & M'zali, B. (2025). ESG disclosures as a double-edged sword: Protective impacts and risks in the social media era. *Innovation and Green Development*, *4*(4), 100260.

Wojewodzki, M., Poon, W. P., & Shen, J. (2018). The role of credit ratings on capital structure and its speed of adjustment: An international study. *The European Journal of Finance*, *24*(9), 735-760.

Wooldridge, J. M. (2021). Econometric Analysis of Cross Section and Panel Data (2nd ed.). *MIT Press*.

Zhang, F., Qin, X., & Liu, L. (2020). The interaction effect between ESG and green innovation and its impact on firm value from the perspective of information disclosure. *Sustainability*, *12*(5), 1866.

Zopounidis, C., Garefalakis, A., Lemonakis, C., & Passas, I. (2020). Environmental, social and corporate governance framework for corporate disclosure: a multicriteria dimension analysis approach. *Management Decision*, *58*(11), 2473-2496.