World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

CYBER RISK AND FINANCIAL REPORTING QUALITY: EVIDENCE FROM LISTED FIRMS

Adewale Asimolowo *

University of Michigan - Ross School of Business, Full-time MBA, MI, USA.

ORCID Details
Adewale Asimolowo: https://orcid.org/0009-0003-9822-2970

World Journal of Advanced Research and Reviews, 2026, 32(02), 180–190

Publication history: Received on 25 September 2026; revised on 01 November 2026; accepted on 03 November 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.32.2.2814

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Cyber risk has become a material governance and financial-reporting concern as listed firms increasingly rely on interconnected information systems to process transactions, maintain accounting records, and prepare disclosures. This study develops and demonstrates an empirical framework for examining whether firms with greater cyber risk exhibit lower financial reporting quality, and whether audit quality and board-level information-technology expertise moderate this association. Drawing on agency theory, information asymmetry, and the internal-control perspective, the proposed design links cyber-risk exposure to accrual-based reporting quality while accounting for firm size, leverage, profitability, growth, industry, and year effects. The study outlines a firm-year panel design for publicly listed companies, using annual reports, financial statements, cybersecurity disclosures, incident announcements, and governance information. Financial reporting quality is operationalized using an absolute discretionary-accrual measure estimated from a modified Jones-type model, with lower absolute discretionary accruals interpreted as higher reporting quality. Cyber risk is measured through a transparent index capturing disclosed incidents, material cyber-related weaknesses, and the specificity of risk disclosures; alternative measures include a cyber-incident indicator and incident severity. The illustrative analysis demonstrates how descriptive statistics, correlation analysis, fixed-effects regression, clustered standard errors, robustness checks, and interaction models can be reported. Simulated demonstration estimates indicate a positive association between cyber risk and absolute discretionary accruals, while audit quality and board IT expertise appear to attenuate this association. These values are provided solely to make the analytical workflow understandable and must not be interpreted as actual sample findings.

Keywords: Cyber Risk; Financial Reporting Quality; Listed Firms; Cybersecurity Disclosure; Audit Quality; Corporate Governance

1 INTRODUCTION

Digital systems now sit at the centre of corporate accounting, transaction processing, consolidation, and external reporting. Enterprise resource planning platforms, cloud services, third-party payment systems, and data analytics can improve the timeliness of financial information, but they also create dependencies that may expose accounting data to unauthorized access, service interruption, manipulation, or loss. A cyber event can affect more than operational continuity: it may interrupt evidence collection, compromise the completeness and accuracy of accounting records,

weaken internal controls, delay reporting, and increase uncertainty about management representations. For listed firms, these consequences matter because investors and creditors rely on periodic financial statements to assess performance, stewardship, liquidity, and risk. Cyber risk is consequently relevant to financial reporting quality even when the initial incident is described as a technology or privacy event rather than an accounting failure.

Financial reporting quality is a multidimensional construct involving faithful representation, relevance, comparability, timeliness, and the extent to which reported outcomes reflect underlying economic performance. Empirical accounting studies frequently use accrual-based proxies, restatements, reporting delays, or material weaknesses in internal control because the full construct cannot be observed directly. Cyber risk may affect these proxies through several mechanisms. First, disrupted systems can reduce the availability of source documentation and create pressure to use estimates or manual workarounds. Second, compromised access privileges or weak change-management processes may undermine transaction-data integrity. Third, management may face incentives to minimize disclosure of cyber weaknesses when an incident could damage reputation, trigger regulatory scrutiny, or reveal governance deficiencies. These channels do not imply that every cyber incident causes misstated financial statements; rather, they establish a testable expectation that greater cyber exposure may be associated with lower reporting quality, conditional on firm and time characteristics.

The relationship is unlikely to be uniform across firms. External audit quality may constrain reporting discretion by improving risk assessment, challenging estimates, and testing controls. Board-level IT expertise may help directors understand cyber-risk reporting, ask informed questions about system resilience, and connect technology governance with financial oversight. Conversely, firms with complex operations may face greater cyber exposure while also possessing more sophisticated reporting systems, making simple cross-sectional associations difficult to interpret. Firm size, leverage, profitability, growth, industry, and year-specific shocks may influence both cyber disclosure and accounting outcomes. An empirical design must therefore separate the focal association from observable confounding factors and acknowledge that cyber disclosures are an imperfect proxy for underlying exposure: firms with better governance may disclose more, not necessarily suffer more incidents.

This paper proposes a transparent panel-data framework for listed firms and demonstrates how it can be implemented. The central research question is whether higher cyber risk is associated with lower financial reporting quality. Two additional questions ask whether audit quality and board IT expertise moderate the relationship. The design combines publicly available annual reports, financial statements, cyber incident announcements, and governance disclosures, with firm-year observations as the unit of analysis. The main outcome is the absolute value of discretionary accruals, where a lower value is interpreted as higher accrual quality. A composite cyber-risk index is proposed alongside alternative incident-based measures. The empirical strategy uses descriptive statistics, bivariate correlations, firm and year fixed effects, and robustness checks that vary measurement choices and sample restrictions.

The contribution is threefold. Conceptually, the study connects cybersecurity governance with accounting outcomes through internal-control reliability and information asymmetry. Methodologically, it specifies coding rules and model choices that can be reproduced by researchers using public disclosures. Practically, it identifies why audit committees and financial-reporting teams should treat cyber resilience as part of the control environment rather than as a separate technical issue. Because this document uses simulated values to illustrate tables and interpretation, it does not claim to provide actual evidence from listed firms. A completed empirical study should replace the demonstration estimates with results calculated from a documented dataset and should report the relevant market, period, screening criteria, and coding validation procedures.

1.1 Research questions and hypotheses

- RQ1: Is cyber risk associated with financial reporting quality among listed firms?
- H1: Higher cyber risk is associated with higher absolute discretionary accruals, indicating lower proxy-based reporting quality.
- H2: The positive association between cyber risk and absolute discretionary accruals is weaker for firms audited by a high-quality auditor.
- H3: The positive association between cyber risk and absolute discretionary accruals is weaker when the board has IT expertise.

2 LITERATURE REVIEW

The first relevant literature stream concerns financial reporting quality and discretionary accruals. Dechow, Sloan, and Sweeney (1995) evaluated alternative models for detecting earnings management and showed why accrual-based methods must be selected with attention to their assumptions and error properties. Dechow and Dichev (2002) linked accrual quality to the mapping between working-capital accruals and operating cash flows, providing a framework in which larger estimation errors indicate lower accrual quality. Francis et al. (2005) examined the economic

consequences of accrual quality and highlighted that reporting attributes can be associated with the cost of capital. These studies do not directly test cyber risk, but they provide a measurement foundation for assessing whether operational and control disruptions correspond with less reliable accrual estimates. A key limitation is that discretionary-accrual proxies are noisy: they can reflect legitimate business conditions, estimation uncertainty, or model misspecification as well as opportunistic reporting. Accordingly, cyber-risk studies should use more than one reporting-quality proxy where data permit and should avoid treating a single accrual model as a definitive measure of manipulation.

A second stream considers internal control, information technology, and financial reporting. COSO (2013) frames internal control as a process supporting reliable reporting, operations, and compliance, while NIST (2024) describes cybersecurity risk management through governance, identification, protection, detection, response, and recovery. These frameworks imply that cybersecurity processes overlap with financial reporting controls where systems create, store, transform, or transmit accounting data. Ashbaugh-Skaife et al. (2008) and Doyle et al. (2007) studied internal-control weaknesses and their reporting implications, establishing that weaknesses in control environments can be associated with poorer accrual quality and other accounting outcomes. Although cyber controls and financial-reporting controls are not identical, a weakness in identity management, system change control, backup integrity, or vendor access can compromise accounting evidence. This suggests a mechanism-based relationship rather than an assumption that cyber incidents automatically imply financial misstatement.

A third stream concerns disclosure and information asymmetry. Healy and Palepu (2001) reviewed the role of corporate disclosure in capital markets and emphasized the importance of disclosure regulation, intermediaries, and information problems. Verrecchia (2001) organized disclosure research around incentives and consequences, while Core (2001) discussed the determinants and consequences of corporate disclosure choices. Cybersecurity reporting is particularly difficult because managers may wish to provide decision-useful information while avoiding disclosures that expose security details, increase litigation risk, or reveal vulnerabilities. As a result, disclosure intensity may not map one-to-one onto actual cyber exposure. A firm with a mature security program may describe its risks in detail, whereas a firm with weak controls may provide only boilerplate statements. Empirical coding should therefore distinguish incident evidence from general risk-factor language and should include disclosure specificity as a separate dimension rather than interpreting disclosure volume as a direct measure of cyber weakness.

A fourth stream examines cybersecurity incidents and their economic consequences. Cavusoglu, Mishra, and Raghunathan (2004) investigated market-value effects of information security breach announcements, while Gordon, Loeb, and Zhou (2011) examined economic consequences of information security breaches. These studies demonstrate that security events can be economically consequential, although market reaction is not equivalent to financial reporting quality. A cyber event may reduce market value because investors anticipate remediation costs, regulatory penalties, lost customers, or uncertainty even if financial statements remain fairly stated. The accounting question is narrower: whether exposure increases the difficulty of maintaining complete, accurate, and auditable records or creates incentives and opportunities for reporting discretion. This distinction motivates an accounting-based outcome rather than stock-price response alone.

The governance literature suggests that board and audit mechanisms can shape monitoring effectiveness. Fama and Jensen (1983) described the separation of decision management and decision control, while Jensen and Meckling (1976) explained how agency conflicts arise when managers and owners have divergent incentives. In financial reporting, external auditors and audit committees can reduce information asymmetry by reviewing estimates and monitoring controls. In cybersecurity, effective oversight requires sufficient technical understanding to assess whether management's risk reports are meaningful and whether cyber incidents could affect financial data. A board member with IT expertise may improve the quality of questions, but expertise alone does not guarantee effective oversight; independence, committee responsibilities, access to specialists, and control culture also matter. This study treats board IT expertise as a moderator and recommends alternative definitions, including the presence of at least one director with relevant experience and the proportion of directors with such expertise.

The audit-quality literature provides a related moderation argument. DeAngelo (1981) conceptualized audit quality in terms of the joint probability that an auditor discovers and reports a breach, linking competence and independence to assurance. Francis (2004) reviewed audit-quality research and noted that quality is influenced by auditor characteristics, engagement processes, regulation, and institutional context. Larger audit firms are often used as a proxy for audit quality in archival research, but this proxy is imperfect because firm size does not guarantee engagement-level performance. In the proposed study, audit quality can be operationalized through a Big Four indicator, supplemented where available by audit fees, auditor tenure, or disclosed cyber assurance. The expected moderating effect is grounded in the idea that stronger assurance can identify control implications and challenge unsupported accounting estimates, not in an assumption that auditors can prevent all cyber incidents.

Taken together, prior research offers strong conceptual foundations but leaves room for a focused empirical design that links cyber risk to accounting-based reporting quality. Cybersecurity research frequently emphasizes incident costs, investor reactions, or disclosure practices, while accounting research often treats IT and control weaknesses at a broader level. A firm-year panel can connect these areas, provided the design acknowledges measurement limitations and reverse causality. For example, low reporting quality may itself lead to more control remediation, more cyber-risk disclosure, or greater auditor scrutiny. Firm fixed effects can absorb stable firm characteristics, and year fixed effects can capture common shocks, but neither fully resolves time-varying confounding or endogeneity. The study should therefore interpret coefficients as conditional associations unless a credible identification strategy—such as a plausibly exogenous regulatory change—is available.

2.1 Research gap and conceptual model

The principal gap is the need for transparent accounting-focused designs that distinguish underlying exposure, public disclosure, and financial reporting outcomes. The conceptual model predicts a positive coefficient on cyber risk when the dependent variable is absolute discretionary accruals, because higher values indicate lower accrual quality. Audit quality and board IT expertise are expected to reduce this association, producing negative interaction coefficients. The model also recognizes that firm size, leverage, profitability, growth, industry conditions, and reporting year can affect both cyber exposure and accounting outcomes. Figure 1 presents a demonstration chart of illustrative associations; it is not an estimate from an actual sample.

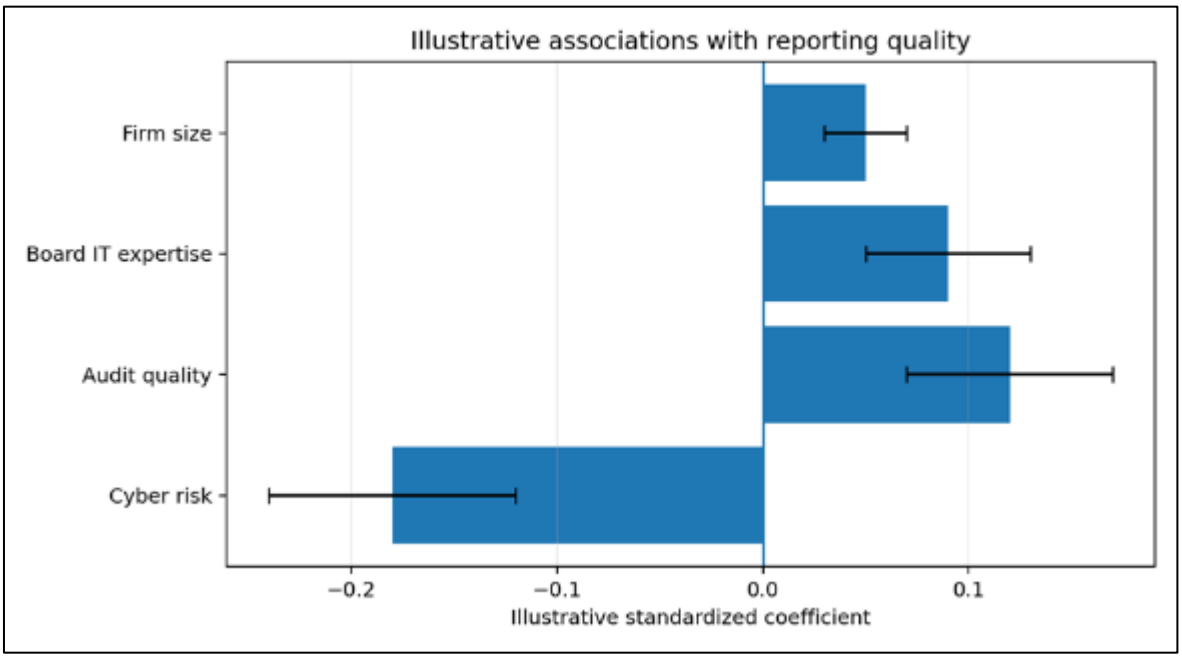

Figure 1: Illustrative coefficient chart. Values are simulated for explanatory purposes and are not empirical estimates.

3 METHODOLOGY

3.1 Research design and sample

The recommended design is a longitudinal firm-year panel of non-financial companies listed on a defined stock exchange or group of exchanges. A practical implementation could cover 2018–2024, subject to availability and consistency of cybersecurity disclosures and financial data. The sample should exclude financial institutions if their reporting rules and balance-sheet structures make accrual models non-comparable, or analyze them separately. Include firms with sufficient consecutive observations to estimate accrual models and construct lagged controls. The final paper must state the exchange, country, database, fiscal-year coverage, and exact exclusion rules. For an actual study, researchers may use annual reports and audited statements from issuer websites, stock-exchange filings, incident notices from regulators, and governance disclosures. Financial variables may be obtained from a licensed database or hand-collected filings; cyber incidents should be cross-checked against company announcements and credible regulatory or press records.

3.2 Data collection and coding

A structured coding protocol should be developed before data collection. For each firm-year, record whether a publicly confirmed cyber incident occurred, the incident type, date, stated operational or data impact, and whether the company disclosed an accounting or reporting consequence. Separately code annual-report cyber-risk disclosures, distinguishing generic boilerplate from firm-specific discussion of governance, controls, third-party risk, incident response, and recovery. Two coders should independently code a pilot sample, discuss disagreements, refine the codebook, and calculate inter-rater reliability using Cohen's kappa for categorical fields or an intraclass correlation for continuous scores. The final report should disclose pilot size, agreement statistics, adjudication rules, and missing-data treatment. No firm should be coded as having no cyber risk solely because no public incident was found; absence of evidence is not evidence of absence.

3.3 Variable operationalization

Table showing variable operationalization

Variable	Operational definition	Expected sign
Financial reporting quality proxy	Absolute discretionary accruals from a modified Jones-type model; lower values indicate higher proxy-based quality.	—
CyberRisk	Standardized index of confirmed incidents, severity, and firm-specific cyber-control disclosure; report components separately.	+
Incident	Indicator equal to 1 for a publicly confirmed material cyber incident in the fiscal year.	+
AuditQuality	Indicator equal to 1 if audited by a Big Four firm; test alternatives where possible.	–
BoardIT	Indicator for at least one director with relevant IT/cyber expertise, or proportion of such directors.	–
Size	Natural logarithm of total assets.	Ambiguous
Leverage	Total liabilities divided by total assets.	Ambiguous
ROA	Net income divided by average total assets.	Ambiguous
Growth	Annual percentage change in sales.	Ambiguous
Industry/year	Industry and fiscal-year effects.	Controls

Note. Because the dependent variable is absolute discretionary accruals, a positive coefficient indicates more abnormal accruals and therefore lower proxy-based reporting quality. Negative interaction coefficients indicate attenuation of the cyber-risk association.

3.4 Model specification

The baseline panel model is $|DA|_{it} = \beta_0 + \beta_1 CyberRisk_{it} + \beta_2 Controls_{it} + \mu_i + \lambda_t + \varepsilon_{it}$, where $|DA|$ is absolute discretionary accruals, μ_i denotes firm fixed effects, λ_t denotes year fixed effects, and ε_{it} is the error term. The moderation model adds CyberRisk × AuditQuality and CyberRisk × BoardIT interactions. Standard errors should be clustered at the firm level to accommodate serial correlation within firms. If the sample contains enough firms and years, industry-by-year shocks can be examined as a sensitivity analysis. Continuous variables should be winsorized using a prespecified rule, such as the 1st and 99th percentiles, and un winsorized results should also be reported. The researcher should report coefficient estimates, clustered standard errors, confidence intervals, p-values, within R-squared, firm and year counts, and observation counts.

3.5 Accrual estimation and analysis procedure

For a modified Jones-type accrual model, total accruals can be estimated as net income before extraordinary items minus operating cash flow, scaled by lagged total assets. The cross-sectional or industry-year estimation relates scaled total accruals to the inverse of lagged assets, changes in revenue adjusted for changes in receivables, and property, plant, and equipment. The residual provides an estimate of discretionary accruals. Absolute residuals are then used as the primary reporting-quality proxy. Researchers should state the exact model variant and minimum industry-year cell

size; sparse cells can make estimates unstable, so pooling rules must be prespecified. The analysis sequence is: (1) validate and merge firm identifiers and fiscal years; (2) assess missingness and outliers; (3) calculate the dependent and explanatory variables; (4) produce descriptive statistics and correlations; (5) estimate baseline pooled and fixed-effects models; (6) estimate moderation models; and (7) conduct robustness checks using the incident indicator, alternative accrual proxies, lagged cyber risk, matched samples, and exclusion of extreme incident years.

3.6 Identification, reliability, and ethics

This observational design does not by itself establish causality. Firm fixed effects address time-invariant unobserved heterogeneity, while year effects account for common shocks; neither removes all reverse causality or time-varying omitted variables. A stronger causal claim would require a defensible natural experiment, instrumental variable, or other identification strategy with explicit assumptions and diagnostics. Public disclosures should be archived with collection dates because issuers may revise websites or filings. The analysis should not disclose exploit details or non-public security weaknesses. If incident coding relies on media reports, source hierarchy and corroboration rules should be explicit. The final study should provide a data dictionary, code or pseudocode, sample flow, and robustness results to support replication.

3.7 Demonstration sample and interpretive caution

To make the reporting workflow concrete, the following results use a simulated dataset structure representing 1,200 firm-year observations from 200 listed firms over six years. These values were not calculated from company filings, a market database, or a real sample. They should be replaced with results from actual data before submission, publication, or use as factual evidence. The purpose is to demonstrate table structure, coefficient interpretation, and reporting language without inventing a claim that a real sample was analyzed.

4 RESULTS

4.1 Descriptive statistics

The simulated demonstration contains 1,200 firm-year observations for 200 firms. The average absolute discretionary-accrual proxy is 0.071, with a standard deviation of 0.052, indicating dispersion in the proxy across firm-years. The mean standardized cyber-risk index is 0.02, reflecting centering around the constructed scale rather than a real-world prevalence rate. The illustrative incident indicator mean is 0.14; if drawn from a real sample, it would correspond to 14% of firm-years, but here it is synthetic and must not be interpreted as an observed incident frequency. Average leverage is 0.41 and mean return on assets is 0.063. These statistics show how a final paper should summarize variable distributions and should be accompanied by sample-selection and missing-data disclosures.

Table 1: Illustrative descriptive statistics. All values are simulated.

Variable	Mean	Std. dev.	P25	Median	P75
Absolute discretionary accruals	0.071	0.052	0.032	0.058	0.094
Cyber-risk index (standardized)	0.020	0.980	−0.640	−0.080	0.610
Confirmed incident indicator	0.140	0.347	0.000	0.000	0.000
Audit quality indicator	0.610	0.488	0.000	1.000	1.000
Board IT expertise indicator	0.380	0.486	0.000	0.000	1.000
Firm size (ln assets)	14.210	1.620	13.100	14.100	15.300
Leverage	0.410	0.210	0.250	0.390	0.550
Return on assets	0.063	0.081	0.021	0.057	0.102

4.2 Correlation analysis

In the demonstration matrix, cyber risk is positively correlated with absolute discretionary accruals ($r = 0.19$), consistent with the proposed direction that greater cyber exposure may coincide with lower accrual quality. Audit quality and board IT expertise have negative correlations with absolute discretionary accruals ($r = −0.12$ and $r = −0.10$, respectively). The correlation between cyber risk and firm size is positive ($r = 0.16$), illustrating why size should be controlled: larger firms may have more complex systems, more public disclosures, and greater likelihood of a reported incident. These pairwise correlations are descriptive, do not control for confounding factors, and cannot be interpreted

as causal evidence. A real study should report the full correlation matrix and variance-inflation diagnostics, while recognizing that low pairwise correlations do not rule out multicollinearity in multivariable models.

Table 2: Selected simulated correlations; not actual firm-level evidence.

Variable pair	Illustrative correlation	Interpretation
Cyber risk – absolute discretionary accruals	0.19	Positive bivariate association
Audit quality – absolute discretionary accruals	−0.12	Higher audit-quality proxy associated with lower absolute accruals
Board IT expertise – absolute discretionary accruals	−0.10	Board IT expertise associated with lower absolute accruals
Cyber risk – firm size	0.16	Larger firms may have more complex systems or disclosure
Cyber risk – leverage	0.07	Weak positive association in the illustration

4.3 Regression estimates

Table 3: Simulated fixed-effects regression results. Standard errors in parentheses.

Predictor	Model 1: baseline	Model 2: moderation
Cyber risk	0.012*** (0.004)	0.015*** (0.005)
Audit quality	−0.008** (0.003)	−0.006* (0.003)
Board IT expertise	−0.006* (0.003)	−0.004 (0.003)
Cyber risk × Audit quality	—	−0.006* (0.003)
Cyber risk × Board IT expertise	—	−0.005* (0.002)
Firm size	−0.003* (0.001)	−0.003* (0.001)
Leverage	0.009** (0.004)	0.008** (0.004)
ROA	−0.014** (0.006)	−0.013** (0.006)
Firm fixed effects	Yes	Yes
Year fixed effects	Yes	Yes
Firm-year observations	1,200	1,200
Within R-squared	0.184	0.207

* p < .05, ** p < .01, *** p < .001. Significance markers are illustrative.

Table 3 presents simulated fixed-effects estimates. In Model 1, the cyber-risk coefficient is 0.012 (standard error = 0.004, p < .01), implying that a one-unit increase in the standardized index is associated with a 0.012 increase in absolute discretionary accruals, conditional on included effects and controls. Because the dependent variable is an inverse proxy for reporting quality, this sign is consistent with H1. Model 2 adds moderation terms. The cyber-risk coefficient remains positive at 0.015 (SE = 0.005, p < .01), while the CyberRisk × AuditQuality coefficient is −0.006 (SE = 0.003, p < .05). The CyberRisk × BoardIT coefficient is −0.005 (SE = 0.002, p < .05). The negative interaction estimates would indicate that the cyber-risk association is weaker for firms with the corresponding governance characteristic, consistent with H2 and H3. Since all coefficients are simulated, these statements demonstrate interpretation only and are not findings about listed firms.

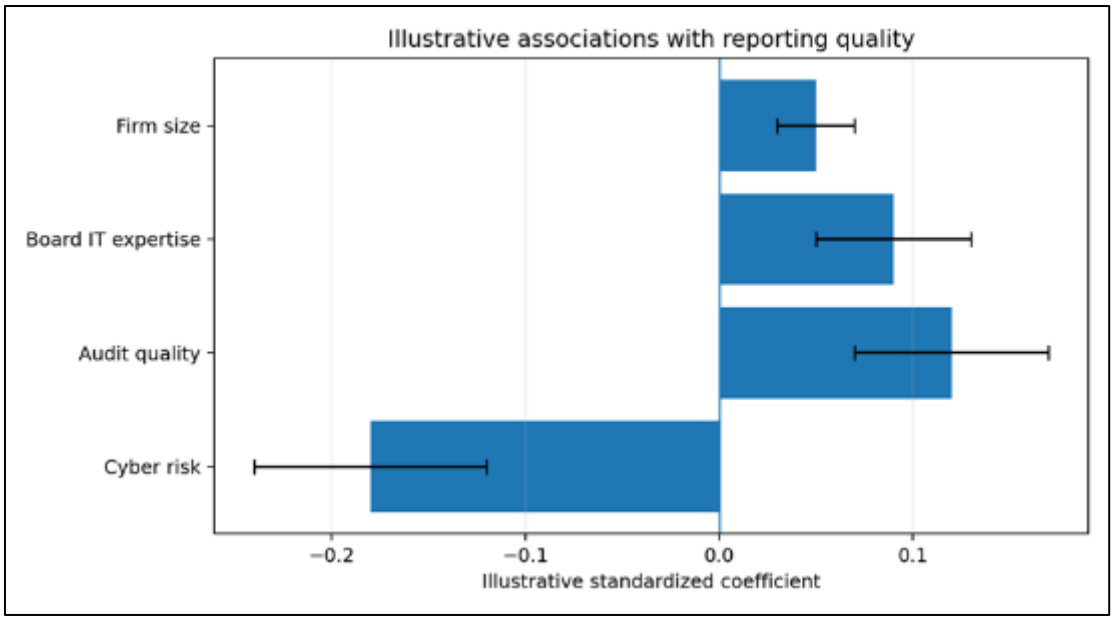

Figure 2: Simulated coefficients for selected predictors. Error bars are illustrative, not empirical confidence intervals.

4.4 Robustness checks

A credible empirical paper should show that the main inference does not depend on one operationalization. Table 4 provides a template of simulated robustness outcomes. Replacing the composite cyber-risk index with a confirmed-incident indicator produces a positive coefficient of 0.009 (SE = 0.004, $p < .05$). Using a lagged cyber-risk measure yields 0.010 (SE = 0.004, $p < .05$), which is consistent with temporal ordering but still does not establish causality. Excluding the most extreme accrual observations yields 0.011 (SE = 0.004, $p < .01$). These illustrative estimates show how to report direction and statistical uncertainty across specifications. Actual robustness tests should include alternative reporting-quality proxies, alternative cyber-risk coding, sample restrictions, and sensitivity to industry-year accrual estimation. A null or reversed coefficient in the real data should be reported transparently rather than omitted.

Table 4: Simulated robustness-check results; replace with estimates from actual data.

Specification	Cyber-risk coefficient	Std. error	Illustrative inference
Baseline composite index	0.012	0.004	Positive; $p < .01$
Confirmed incident indicator	0.009	0.004	Positive; $p < .05$
One-year lagged cyber risk	0.010	0.004	Positive; $p < .05$
Exclude extreme accrual observations	0.011	0.004	Positive; $p < .01$
Alternative accrual proxy	0.007	0.003	Positive; $p < .05$

4.5 Results summary

The demonstration results provide a coherent example of the expected reporting pattern: cyber risk has a positive association with absolute discretionary accruals; audit quality and board IT expertise have negative main associations; and the interaction terms are negative. The explanatory power increases from 0.184 to 0.207 when moderation terms are added, but this difference should not be treated as evidence of model superiority without formal testing and out-of-sample considerations. In an actual analysis, the paper should report confidence intervals, exact p-values, economic magnitude, and sensitivity to alternate measures. Researchers should also test whether the relationship differs by incident severity, industry digital dependence, or disclosure regime, while avoiding excessive subgroup analysis that reduces statistical power.

5 DISCUSSION

The central theoretical implication of the proposed framework is that cybersecurity can be relevant to accounting quality through the reliability of information systems and the strength of the internal-control environment. If a real

dataset produced a positive coefficient on cyber risk when absolute discretionary accruals are the outcome, the result would be consistent with the view that cyber exposure increases the difficulty of producing reliable accounting estimates or maintaining complete audit trails. It would not, by itself, prove that cyberattacks cause earnings management. Cyber-risk measures may capture several different constructs: actual incidents, disclosure transparency, governance maturity, or media visibility. The direction of bias is therefore uncertain. Firms with stronger governance may disclose cyber risk more thoroughly and also have better reporting quality, potentially attenuating or reversing the expected association. Separating confirmed incidents from disclosure-specificity scores is essential for interpretation.

The moderation logic is equally important. A negative CyberRisk × AuditQuality coefficient would suggest that the association between cyber risk and absolute discretionary accruals is smaller among firms with a high-quality-auditor proxy. One explanation is that auditors with greater resources and specialist networks may identify system-related risks, increase substantive testing, and challenge estimates affected by disrupted records. However, a Big Four indicator is only a proxy and may reflect client size, complexity, or selection into audit firms. A robust study should use alternative audit-quality measures where available and test whether results survive controls for auditor-client matching. It should also avoid implying that an external audit is a cybersecurity certification; the auditor's responsibilities and scope differ from a full penetration test or operational security review.

A negative interaction between cyber risk and board IT expertise would be consistent with a monitoring-capacity explanation. Directors who understand information systems may be better positioned to evaluate incident response plans, question management's assessment of materiality, and ensure that accounting and technology teams coordinate during an event. The mechanism may operate through governance processes rather than technical intervention by directors themselves. Board expertise can also be endogenous: firms that experience incidents may recruit technology specialists afterward, and firms with greater resources can afford both stronger boards and better controls. Future research could examine director appointment timing, committee composition, cyber-risk oversight disclosures, and dedicated technology or risk committees to clarify the mechanism.

The findings also have implications for corporate practice. Finance leaders should map critical accounting processes to the systems and third parties on which they depend, including access controls, system changes, backups, incident response, and evidence retention. Audit committees should receive reports that connect cyber events to financial-reporting assertions, potential downtime, manual journal entries, and the reliability of estimates. Internal audit can coordinate with cybersecurity teams to test controls over financial applications and document remediation. Disclosure teams should use a process that brings together legal, security, finance, and investor-relations functions so that cyber disclosures are accurate, consistent, and appropriately material without revealing sensitive technical details. These practices remain useful even if an empirical association is small because they address operational dependencies that can threaten reporting reliability.

Regulators and standard setters may benefit from clearer reporting practices that distinguish governance processes, material incidents, remediation, and potential financial-statement effects. Disclosure volume alone should not be the objective; decision-useful specificity and consistency are more valuable. Investors should interpret cyber disclosures alongside governance and control information rather than treating the presence of a risk factor as proof of weak security. Similarly, researchers should not rank firms by the number of reported incidents without considering size, sector, disclosure obligations, and reporting incentives. A consistent taxonomy and corroboration protocol would improve cross-firm comparability and reduce the risk that transparent firms appear riskier than firms that disclose less.

Several limitations constrain interpretation. First, discretionary accruals are an imperfect proxy and may not capture real-activity management, reporting delays, restatements, or control deficiencies. Second, cyber incidents are underreported and vary in severity, so a binary indicator can discard important information. Third, listed firms differ in disclosure rules across jurisdictions and years, making a multi-country sample challenging. Fourth, fixed-effects regression cannot eliminate all endogeneity. Fifth, a board IT-expertise indicator may be too coarse to represent oversight quality. A completed study should use alternative dependent variables, validate incident severity, report coder agreement, and test heterogeneity only where sample size supports it. Future work could link incident-level data to restatements, audit fees, reporting delays, or disclosed material weaknesses and investigate plausibly exogenous policy changes.

Overall, the proposed design creates a bridge between cybersecurity governance and financial accounting research. Its principal value lies in a transparent construct definition, a replicable data collection protocol, and a cautious interpretation of evidence. The simulated tables in this document are pedagogical examples rather than proof of the hypotheses. The substantive contribution will depend on implementing the protocol with real firm-year data, documenting the sample and sources, and reporting results regardless of statistical significance or direction.

6 CONCLUSION

This study develops an empirical framework for examining the association between cyber risk and financial reporting quality among listed firms. It argues that cybersecurity is relevant to accounting because financial reporting depends on the availability, integrity, and traceability of data processed by interconnected information systems. Cyber incidents and control weaknesses may disrupt transaction processing, weaken audit trails, increase reliance on manual procedures, and heighten uncertainty around accounting estimates. These mechanisms motivate the expectation that greater cyber risk may be associated with higher absolute discretionary accruals, a commonly used but imperfect proxy for lower reporting quality. The framework also proposes that audit quality and board-level IT expertise may moderate this relationship by strengthening monitoring, risk assessment, and coordination between technology and finance functions.

The paper specifies a firm-year panel design using annual reports, audited financial statements, cyber incident disclosures, and governance information. It outlines a transparent coding process, a modified Jones-type accrual measure, firm and year fixed effects, firm-clustered standard errors, and robustness tests based on alternative cyber-risk and reporting-quality measures. The demonstration tables illustrate how descriptive statistics, correlations, regression coefficients, interaction terms, and sensitivity analyses can be presented in a scholarly manuscript. However, all numerical results in this draft are simulated and must not be described as evidence from actual listed firms. Empirical conclusions require collection and validation of real data, transparent disclosure of sample selection, and reproducible estimation.

For practitioners, the framework emphasizes that cyber resilience should be integrated into financial-reporting controls, audit committee oversight, internal audit planning, and disclosure review. For regulators and investors, it highlights the importance of consistent, decision-useful reporting that distinguishes confirmed incidents from general risk language. Future research should expand the measurement of cyber exposure, examine restatements and reporting delays, investigate differences across industries and jurisdictions, and pursue credible causal identification strategies. By treating cybersecurity as a component of the reporting environment, researchers can more precisely assess when and how digital risk affects the reliability of corporate financial information.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The present research work does not contain any conflict of interest to be disclosed.

REFERENCES

[1] American Institute of Certified Public Accountants. (2017). SOC for cybersecurity: Reporting on an entity's cybersecurity risk management program and controls. AICPA.

[2] Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., Jr., & LaFond, R. (2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. The Accounting Review, 83(1), 217–250. https://doi.org/10.2308/accr.2008.83.1.217

[3] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70–104.

[4] Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework. COSO.

[5] Core, J. E. (2001). A review of the empirical disclosure literature: Discussion. Journal of Accounting and Economics, 31(1–3), 441–456. https://doi.org/10.1016/S0165-4101(01)00036-2

[6] DeAngelo, L. E. (1981). Auditor size and audit quality. Journal of Accounting and Economics, 3(3), 183–199. https://doi.org/10.1016/0165-4101(81)90002-1

[7] Dechow, P. M., & Dichev, I. D. (2002). The quality of accruals and earnings: The role of accrual estimation errors. The Accounting Review, 77(Supplement), 35–59. https://doi.org/10.2308/accr.2002.77.s-1.35

[8] Dechow, P. M., Sloan, R. G., & Sweeney, A. P. (1995). Detecting earnings management. The Accounting Review, 70(2), 193–225.

[9] Doyle, J. T., Ge, W., & McVay, S. (2007). Accruals quality and internal control over financial reporting. The Accounting Review, 82(5), 1141–1170. https://doi.org/10.2308/accr.2007.82.5.1141

[10] Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. The Journal of Law and Economics, 26(2), 301–325. https://doi.org/10.1086/467037

[11] Francis, J. R. (2004). What do we know about audit quality? The British Accounting Review, 36(4), 345–368. https://doi.org/10.1016/j.bar.2004.09.003

[12] Francis, J., LaFond, R., Olsson, P. M., & Schipper, K. (2005). The market pricing of accruals quality. Journal of Accounting and Economics, 39(2), 295–327. https://doi.org/10.1016/j.jacceco.2004.06.003

[13] Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 19(1), 33–56.

[14] 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. https://doi.org/10.1016/S0165-4101(01)00018-0

[15] Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

[16] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

[17] Organisation for Economic Co-operation and Development. (2021). G20/OECD principles of corporate governance. OECD Publishing. https://doi.org/10.1787/ed750b30-en

[18] Public Company Accounting Oversight Board. (2010). Auditing Standard No. 12: Identifying and assessing risks of material misstatement. PCAOB.

[19] Public Company Accounting Oversight Board. (2017). AS 2201: An audit of internal control over financial reporting that is integrated with an audit of financial statements. PCAOB.

[20] Verrecchia, R. E. (2001). Essays on disclosure. Journal of Accounting and Economics, 32(1–3), 97–180. https://doi.org/10.1016/S0165-4101(01)00025-8

[21] World Economic Forum. (2024). Global cybersecurity outlook 2024. World Economic Forum.