Cybersecurity Incidents and Accounting Restatements

The Role of Audit Quality and Implications for Firm Value

Aliyu Nafiu, Habeeb Yahya*

9 January 2026

Abstract

This study examines the impact of cybersecurity incidents on financial reporting quality and the market value of U.S. firms. We find that cyber shocks significantly increase the likelihood of core financial restatements by impairing accounting infrastructure and transaction integrity. Using an attention-based view, we document a "managerial triage" effect where resources shift toward core remediation at the expense of technical compliance. However, quality audit effectively mitigates these reporting failures through rigorous technical scrutiny. In addition, our valuation analysis shows that while breaches harm firm value, financial restatements help recover investor trust by signaling transparency. In contrast, technical adjustments deepen value losses by revealing broader systemic weaknesses. These findings alert boards to the danger of neglecting technical compliance during core remediation and inform regulators that investors distinguish between transparent reporting corrections and signals of systemic instability.

Keywords: Cybersecurity; financial restatements; audit quality; Big 4; firm value; signaling theory

JEL Classification: G32, G34, M41, M42

*The authors are in alphabetical order. Yahya (corresponding author): Postdoctoral Researcher, Turku School of Economics (TSE), University of Turku. Address: TSE, Department of Accounting and Finance, 20014 University of Turku, Finland. Email: hbyahy@utu.fi. Aliyu Nafiu: PhD student in Accounting, University of Texas at El Paso. Yahya appreciates the research grant from Liikesivistysrahasto for the financial support.

1 Introduction

The rapid digitalization of corporate operations has fundamentally transformed the landscape of financial reporting (Al Natour and Al-Lahham, 2021). In the contemporary digital economy, a firm's information technology (IT) infrastructure is no longer merely a support function; it serves as the primary repository and processing engine for financial data (Grabski et al., 2011), forming the structural backbone of internal controls over financial reporting (ICFR) (Doyle et al., 2007). While this integration has enhanced operational efficiency, it has simultaneously introduced systemic vulnerabilities. A cybersecurity incident, ranging from data breaches to system compromises, represents an exogenous shock that can fundamentally impair the integrity and availability of these systems (Juma'h and Alnsour, 2020; Ganin et al., 2020). Despite the growing prevalence of such incidents, the accounting literature remains divided on the downstream consequences for reporting quality. Some studies suggest that cyber events weaken internal controls, disrupt information flows, and heighten uncertainty in the reporting environment (Ko et al., 2006; Zafar et al., 2016), while others find more limited or mixed effects (Gordon et al., 2011; Cavusoglu et al., 2004). This study investigates the nexus between cyber incidents and accounting restatements, exploring whether such shocks lead to a general deterioration of reporting quality or a selective failure of core financial processes.

The theoretical link between cybersecurity failures and reporting quality is rooted in the degradation of system reliability and the amplification of information asymmetry (Akerlof, 1970). When a cyber breach occurs, the resulting operational chaos and potential corruption of transactional records weaken the internal control environment, heightening the inherent risk of financial misstatement (Masoud and Al-Utaibi, 2022). Early empirical evidence on this relationship, however, provides inconsistent conclusions. Some studies suggest that the systemic disruption following a breach increases the overall propensity for errors (Lois et al., 2021), while others find that the subsequent increase in regulatory and auditor scrutiny may

actually preempt the issuance of restatements (Rosati et al., 2017). We address this ambiguity by examining the comprehensive effect of cyber shocks on aggregate restatement risk, proposing that the systemic nature of these incidents drives a material decline in financial reliability.

Moving beyond aggregate measures, we argue that a deeper investigation requires differentiating between the types of reporting failures. Grounded in signaling theory (Spence, 1973), we distinguish between "Financial Restatements", which correct errors in core accounts like revenue and assets, and "technical or judgmental adjustments" such as those related to uncertain tax positions (FIN48) or timing rules (SAB108). We posit that if a cyber breach impairs core accounting systems and data integrity, its consequences should be concentrated in the most severe error categories that reflect a failure in fundamental accounting processes (Hennes et al., 2008). Conversely, non-core adjustments, which are often driven by interpretive complexity or managerial judgment rather than transactional record integrity, may remain unaffected (Palmrose et al., 2004). We further apply the Attention-Based View (ABV) to suggest a "managerial triage" mechanism, i.e., following a breach, firms redirect finite resources toward remediating core systems, potentially leading to a selective impact where core reporting integrity is compromised while specialized compliance functions are neglected (Ocasio, 1997).

Central to this discussion is the role of external governance in mitigating the risks posed by cyber-induced control weaknesses. Under agency theory, auditing serves as a crucial governance mechanism to reduce information asymmetry (Jensen and Meckling, 1976). We examine whether high-quality auditors, specifically Big 4 firms, act as a buffer against reporting failures. Given their superior technical resources and specialized IT-audit expertise, Big 4 auditors are better positioned to scrutinize compromised accounting processes more closely after a breach (Alsakini et al., 2024). This heightened scrutiny is expected to function as a crucial governance safeguard, detecting and correcting errors before they necessitate a public restatement. Our study thus evaluates the interaction between cyber incidents and auditor

type to determine if superior external assurance can safeguard reporting credibility even when internal systems are under stress. Finally, we examine the real economic consequences of these failures by analyzing capital market reactions. While a cyber breach itself acts as a negative signal of organizational vulnerability (Kamiya et al., 2021), the interpretation of a subsequent restatement is conditional. Using the lens of signaling theory, we investigate whether a restatement acts as a "corrective signal", restoring investor confidence through transparent disclosure, or a "compounding signal" that reinforces concerns about systemic governance failures (Hennes et al., 2008). We anticipate that the market reaction will be heterogeneous, i.e., corrective core financial restatements may mitigate part of the initial valuation penalty, whereas technical or timing restatements following a breach may signal broader, unresolved internal control deficiencies, thereby amplifying the erosion of firm value (Ashbaugh-Skaife et al., 2009).

The findings of this study provide substantive evidence that cyber incidents serve as a catalyst for severe reporting failures, particularly core Financial Restatements. This aligns with the systemic disruption perspective of Alsakini et al. (2024) and Masoud and Al-Utaibi (2022), who argue that cyber shocks degrade accounting infrastructure and escalate material misstatement risk. While our results contrast with earlier evidence suggesting breaches may not lead to restatements (Rosati et al., 2017), we clarify that the impact is specifically concentrated in the structural reliability of core transactional data rather than aggregate reporting. Furthermore, we find that Big 4 auditors effectively moderate this relationship, significantly attenuating the likelihood of a restatement post-breach by applying superior technical scrutiny (DeAngelo, 1981; Haislip et al., 2016). Our alternative measure of audit quality, the audit fee ratio, further confirms this significant moderating role of audit quality. Regarding market consequences, our results indicate that the negative valuation shock of a breach is significantly mitigated when firms issue a core financial restatement, which investors interpret as a credible corrective signal. Conversely, issuing technical or judgmental adjustments (e.g., FIN48) following a breach amplifies the valuation penalty, as the market

likely perceives these as indicators of broader, unresolved systemic failures (Beneish et al., 2008; Ashbaugh-Skaife et al., 2009). This divergence underscores a "managerial triage" where resource diversion toward core remediation safeguards fundamental data integrity but leaves peripheral compliance vulnerable

Our study makes a number of key contributions to the accounting, IT, and governance literature. First, we provide a more granular understanding of how cyber risk propagates through the financial reporting system by differentiating between restatement severities. Second, we extend the literature on audit quality by demonstrating the specific conditions under which Big 4 auditors provide superior monitoring. Third, we offer fresh evidence on the "correction versus compounding" signaling dynamics in the capital markets. By documenting that the impact of cyber risk is concentrated in core financial processes and is conditional on both auditor quality and restatement type, we provide crucial insights for regulators, investors, and boards of directors tasked with managing the fallout of cybersecurity failures in an increasingly digitalized reporting environment.

The remainder of this paper is organized as follows. Section 2 establishes the theoretical framework, synthesizes the relevant literature, and develops the formal hypotheses. Section 3 describes the data and empirical methodology. Section 4 presents and discusses the baseline results, additional analyses, and robustness checks. Finally, Section 5 concludes with a discussion of the theoretical contributions and practical implications for regulators and practitioners.

2 Theoretical Framework, Literature Review, and Hypothesis Development

2.1 Cyber Incidents and Aggregate Restatement Risk

The theoretical foundation for establishing a link between cybersecurity failures and overall reporting quality lies in information asymmetry (Akerlof, 1970) and the degradation of system reliability (Garg et al., 2003). In the digital economy, a firm's IT infrastructure is indispensable, acting as the primary repository and processing engine for financial data, thereby forming the backbone of its internal controls over financial reporting (ICFR) (Doyle et al., 2007). A cyber incident, such as a major data breach or system compromise, represents an exogenous shock that fundamentally impairs the integrity and availability of these systems. This impairment severely amplifies information asymmetry because external stakeholders lose confidence in the reliability of the information produced by the compromised system. Managers themselves face increased uncertainty regarding the accuracy of records, complicating the timely and correct compilation of financial statements, which significantly raises the probability of reporting errors (Kamiya et al., 2021).

Earlier studies provide strong, yet not entirely consistent, support for the argument that cyber shocks impair reporting quality. A strand of these studies suggests that cybersecurity failures disrupt internal controls, introduce operational complexity, and elevate the risk of material misstatements that are difficult to detect during the normal closing process (Usman et al., 2023; Alsakini et al., 2024). They generally argue that the chaos and loss of data integrity following a breach create the necessary conditions for errors to propagate through the accounting system, ultimately resulting in a restatement. However, counter-evidence exists. For instance, Rosati et al. (2017) found that while a cybersecurity breach increases regulatory scrutiny, evidenced by a higher probability of receiving an SEC Comment Letter, it does not necessarily translate into a financial restatement. This highlights a critical,

unresolved ambiguity; the subsequent deterioration in reporting quality, if it occurs, may stem either from a systemic breakdown in controls that causes actual errors or merely from heightened caution and increased scrutiny. This inconsistency in conclusion motivates the need to examine the comprehensive effect on all types of restatements, capturing the aggregate deterioration in the reporting environment following a cyber incident, regardless of the precise error type.

To provide clarity on whether cyber incidents represent a material shock leading to undeniable failures in reporting mechanisms, this study focuses on the immediate, measurable consequence captured in the issuance of any financial restatement in the subsequent reporting period. The core premise is that if the cyber incident causes systemic disruption and compromises data integrity, the subsequent weakening of the internal control environment (Blakely et al., 2022), will lead to increased operational uncertainty and collectively heighten the overall propensity for errors (Lois et al., 2021). By examining the broad category of restatements, we aim to capture a comprehensive measure of post-breach reporting deterioration. This reasoning leads directly to the core prediction regarding the general impact of cyber risk on financial reliability.

H1: *Firms that experience a cyber incident in the prior year are significantly more likely to issue an aggregate financial restatement in the subsequent year.*

2.2 Cyber Incidents and Restatement Type Severity

A deeper investigation requires differentiating the types of reporting failure, a distinction rooted in the theoretical argument of signaling theory (Spence, 1973) and the inherent nature of accounting errors. Restatements serve as a negative signal to the market, but their impact depends on the severity of the error being corrected (Hennes et al., 2008). Errors that correct misstatements in core financial accounts, i.e., financial restatements (e.g., revenue, assets), signal a failure in the firm's fundamental accounting processes and are linked to the structural

integrity of financial data (Campbell et al., 2003). In contrast, technical adjustments (like FIN48 for uncertain tax positions) or timing/threshold-based adjustments (SAB108) are often non-core, arising from interpretive complexity or managerial judgment on materiality, rather than a systemic breakdown of transactional records (Palmrose et al., 2004). This distinction is paramount because if a cyber breach impairs core accounting systems and data integrity, its consequences should be concentrated in the most severe error category, signaling a substantive failure.

A complementary theoretical perspective supporting the selective impact argument stems from the Attention-Based View (ABV) of the firm. Cybersecurity breaches represent acute crises that severely constrain managerial attention and finite organizational resources, forcing firms to triage remediation efforts (Ocasio, 1997). Studies show that following a major IT failure, executive focus and capital expenditures are redirected immediately toward shoring up core operational systems to ensure business continuity and satisfy immediate regulatory demands (Kuhn Jr et al., 2013). This necessary redirection of attention and resources implies a potential neglect of specialized, non-core compliance functions, such as complex tax calculations or subtle SAB108 materiality assessments, which are typically handled by specialized departments or require focused, non-systemic analysis (August et al., 2025). Consequently, the probability of detecting or preventing errors in specialized accounts may decrease (leading to a null or negative effect on their detection). At the same time, the direct, systemic failure of core transaction processing drives up the rate of fundamental financial restatements (Masoud and Al-Utaibi, 2022). This managerial triage mechanism reinforces the hypothesis that the consequence of the cyber shock is not uniformly distributed across all types of reporting failures, but is selectively concentrated where the systemic failure is most pronounced.

In addition, existing literature on restatements confirms the differential nature of these reporting failures. Palmrose et al. (2004) highlights that the market reaction is far more severe for restatements involving core financial accounts, highlighting their signaling value regarding fundamental system failure. Specialized restatements, such as those related to uncertain tax

positions (FIN48), are often driven by regulatory complexity and specialized analysis, which are arguably less directly exposed to breaches affecting operational or financial transaction systems (Gleason et al., 2017). Similarly, timing-based adjustments (Out-of-Period) or those related to prior-period immateriality rules (SAB108) rely more on management judgment and materiality thresholds than on the integrity of real-time operational data processing (Burks, 2011). Therefore, if the cyber shock primarily degrades the reliability of financial transaction processing and core data, we should observe a disproportionate effect on Financial Restatements, while tax and timing adjustments should remain unaffected or possibly even show a negative relationship if resources are shifted away from specialized analyses toward core remediation efforts.

Therefore, there is motivation to disentangle whether cyber incidents lead to a uniform rise in all reporting failures or selectively target the core financial reporting infrastructure. A robust positive association between cyber breaches and Financial Restatements would offer compelling evidence that the shock compromises the integrity of core financial data, whereas a null or negative association with technical or timing adjustments would reinforce the argument that the impact is specific to the financial accounting infrastructure, rather than peripheral or specialized compliance systems. This assessment sharpens the causal link between cybersecurity failures and material misstatements, and thus, we state our second hypothesis as:

H2: *A cyber incident is positively and significantly associated with the likelihood of a Financial Restatement.*

2.3 The Moderating Role of External Assurance Quality

A cyber incident represents a shock that elevates information risk by weakening internal controls, corrupting transactional data, and increasing the likelihood of material misstatements. Under the agency theory (Jensen and Meckling, 1976), high-quality auditors serve as

external monitors whose role is to mitigate such risks by enhancing assurance over financial reporting. Thus, auditing serves as a crucial governance mechanism to mitigate conflicts of interest and reduce information asymmetry (Watts and Zimmerman, 1978). High-quality auditors, typically Big 4 firms, possess superior technical expertise and resources, enabling them to conduct more rigorous evaluations of internal controls and detect irregularities more effectively than non-Big 4 auditors (Francis et al., 1999; Krishnan, 2003). Following a cyber breach, the internal control environment is demonstrably weakened, heightening the inherent risk for financial misstatement Masoud and Al-Utaibi (2022). This context mandates that a high-quality auditor adopt a more conservative and stringent approach, intensifying audit procedures on the compromised accounting processes. This enhanced scrutiny is expected to function as a crucial governance buffer, catching and correcting errors that might otherwise propagate into financial statements and necessitate a costly restatement later (Rosati et al., 2022).

Documented evidence supports the role of high-quality external monitoring in mitigating information risk. DeFond and Zhang (2014) affirm that audit quality is negatively associated with misreporting risk, particularly in environments marked by high complexity or uncertainty. Specifically, studies focusing on cybersecurity suggest that Big 4 auditors help constrain the downstream reporting consequences of failures by scrutinizing internal controls more closely after a breach, thereby strengthening the reliability of the financial data presented (Alsakini et al., 2024). This suggests that the Big 4's superior resources and reputation capital incentivize them to be more diligent in high-risk situations. The moderating effect is expected to be strongest for financial restatements, as these represent the most material misstatements, which fall squarely within the core focus of a traditional financial audit. Therefore, evaluating the interaction between a cyber incident and the presence of a Big 4 auditor provides a direct test of whether external governance mechanisms effectively safeguard reporting credibility when internal systems are compromised.

The reporting environment following a cyber breach is a critical test of whether audit qual-

ity can effectively contain elevated misstatement risk, as shocks to internal controls heighten reliance on the auditor's independent verification rather than the client's systems (Asare et al., 2013). In such settings, the differential capabilities of Big 4 auditors are likely to matter most. Their deeper methodological rigor and greater access to specialized IT-audit expertise enable more effective detection of weaknesses that may not be visible to lower-tier auditors (Abbott et al., 2016; Dzuranin and Mălăescu, 2016). Additionally, because Big 4 firms face higher litigation exposure and reputational costs when material misstatements occur, they are incentivized to enforce stricter audit procedures in high-risk environments (Francis, 2004; DeAngelo, 1981). These incentives and capabilities suggest that Big 4 auditors are better positioned to mitigate the propagation of errors following cybersecurity disruptions. If these mechanisms operate as theory and prior evidence suggests, then the escalation from cyber incident to financial restatement should be less pronounced for Big 4–audited firms. This leads to the expectation that audit quality moderates, not merely accompanies, the relationship between cybersecurity breaches and subsequent reporting failures. Hence, we hypothesize that:

H3: *The positive association between incident and the likelihood of a Financial Restatement is significantly attenuated for firms audited by a Big 4 auditor.*

2.4 Cyber Incidents, Restatements, and Firm Value

Understanding how capital markets interpret the mixed signals generated by a cyber incident followed by a restatement, drawing upon signaling theory, is important (Muktadir-Al-Mukit and Ali, 2025; Das et al., 2012). The initial cyber breach acts as a negative signal of deep organizational vulnerability, which could reduce firm valuation due to anticipated long-term operational, reputational, and legal costs (Eling and Wirfs, 2019; Goel and Shawky, 2009; Kamiya et al., 2021). The subsequent restatement serves as a secondary signal, the interpretation of which is highly conditional. A restatement, while confirming a prior error, can

be viewed by investors in two different ways. First, as a corrective signal, where transparent disclosure (e.g., of a financial restatement) reduces uncertainty and restores some investor confidence (Hennes et al., 2008); or second, as a compounding signal, where a technical or complex restatement (e.g., FIN48 or Out-of-Period) following a major breach is seen as evidence of broader, systemic internal control failures, intensifying the initial market penalty (Lois et al., 2021).

Empirical findings confirm that the market reaction to restatements is heterogeneous, dependent on the nature, severity, and informational content of the correction (Anderson and Yohn, 2002; Palmrose et al., 2004). Although studies (e.g., Kuhn and Morris, 2017) have documented evidence of a link between weaknesses in IT internal control and firms' market value, the informative role of restatement or otherwise is yet to be explored. Investors interpret restatements as signals about a firm's underlying reporting reliability, but the magnitude of the response depends heavily on whether the error reflects a breakdown in core accounting processes or a narrower, technical adjustment (Her et al., 2010). When restatements stem from fundamental financial account errors, markets infer weaknesses in internal controls and organizational oversight, resulting in greater value erosion (Zhang, 2007). This raises an important issue for firms experiencing cyber incidents, namely, whether the market evaluates subsequent restatements differently depending on the firm's cyber-risk environment. Cyber breaches reveal vulnerabilities in data integrity and internal reporting infrastructure, which research shows can heighten investor uncertainty and elevate perceived operational and financial risk (Eling and Schnell, 2016). In such a setting, a financial restatement, one that directly addresses potential misstatements arising from the breach, may be interpreted as a credible corrective action that helps reduce information asymmetry and restore confidence in reporting quality. Conversely, investors may perceive restatements in areas unrelated to the breach, such as tax-related FIN48 issues or timing-based adjustments, as evidence that control weaknesses extend beyond the immediate incident (Beneish et al., 2008). Such findings reinforce concerns about systemic governance failures and can ultimately amplify

the valuation penalty (Ashbaugh-Skaife et al., 2009). Understanding how cyber risk shapes the informational content of restatements is therefore essential for explaining how investors update their beliefs about firm reliability and long-term value.

Consequently, it is expected that the market's response to the restatement is contingent on the firm's cyber-risk environment. Examining the interaction effects to determine which type of corrective disclosure, if any, helps firms recover from the persistent negative valuation shock of a cyber incident offers insight into these dynamics. Thus, we state our hypothesis capturing both the baseline penalty of the cyber incident and the conditional market reaction to the subsequent attempt at reporting correction. This assessment of the market's update process provides crucial insight into the real economic consequences of integrated cyber incidents and financial reporting failures.

H4: *Cybersecurity incidents are associated with a persistent decrease in firm value, a relationship moderated by the nature of subsequent reporting.*

3 Research design

3.1 Data

The data for this study covers a period of 25 years, from 2000 to 2024, focusing on U.S. publicly traded firms. The sample period begins in 2000 to ensure sufficient coverage of digital-era corporate disclosures and the early adoption of integrated IT reporting frameworks. We utilize data from several primary sources. Cybersecurity incident details, including the type of information compromised and disclosure timelines, are obtained from the Audit Analytics (Ideagen) Cybersecurity module. We also rely on this source for financial restatement data, including the categorization of restatement types, and for detailed audit information such as auditor identity and fee structures. Firm-level financial characteristics, operational data,

and fiscal year-end stock price data (used to calculate Tobin's Q) are sourced from Compustat. Finally, corporate governance and board-level metrics, such as board independence and gender diversity, are collected from LSEG Workspace (formerly Refinitiv). After merging these disparate sources and requiring non-missing values for our primary variables, our final sample consists of 61,229 firm-year unbalanced observations.

3.2 Empirical design

3.2.1 Variables

This study uses a streamlined narrative to define and categorize the primary metrics for reporting failures and cybersecurity risk. Our primary measure of reporting quality is the issuance of a restatement. Following the Audit Analytics classification, we distinguish between four types: (i) Financial restatements ($Restate\_Financial_{it}$), which correct core accounts like revenue or assets and signal fundamental system failures (Palmrose et al., 2004); (ii) FIN-48 restatements ($Restate\_FIN48_{it}$), relating to uncertain tax positions; (iii) Out-of-Period Adjustments ($Restate\_OutOfPeriod_{it}$ or OOPA), correcting prior errors in the current period; and (iv) SAB 108 restatements ($Restate\_SAB108_{it}$), involving SEC-mandated misstatement quantification adjustments. Similarly, we categorize cybersecurity incidents into four distinct groups: (i) $Breach\_Financial_{it}$, identifying the compromise of payment or banking details; (ii) $Breach\_Personal_{it}$, denoting the loss of personally identifiable information (PII); (iii) $Breach\_NotDisclosed_{it}$, representing incidents where the firm's filing did not specify the data type, reflecting higher information asymmetry; and (iv) $Breach\_Other_{it}$, encompassing theft of intellectual property or internal corporate records.

To isolate high-impact events, we construct an indicator, $Most\_Significant\_Breach_{it}$, equal to one if the incident involves either financial or personal data, as these categories drive the highest legal and systemic risk (Rosati et al., 2022). Finally, we define high-significance restatements as those categorized as $Restate\_Financial$, as they reflect breakdowns in fun-

damental transaction processing rather than technical or judgmental adjustments (Hennes et al., 2008). This classification allows us to test the "managerial triage" hypothesis: whether the operational strain of a cyber shock causes firms to selectively protect core reporting integrity while peripheral or specialized compliance functions (such as tax or timing adjustments) are neglected.

We control for firm characteristics that may affect a firm's restatement propensity and market valuation as control variables. The variables include profitability (ROA) as a proxy for financial performance is the earnings before interest and taxes over the total assets of the firm, the natural logarithm of the book value of total assets of the firm as a measure of Firm_Size, the debt-to-equity ratio as a measure of Leverage, tangible assets of a firm over its total assets as a measure of Tangibility, and cash and short-term investments of a firm over its total assets as a measure of CashHolding. Others are Sales_growth, calculated as the percentage change in a firm's sales, which is expected to capture revenue improvements that enable firms to access resources for investment in internal control systems, audit and governance characteristics, such as Big_4, to proxy for external monitoring quality, and Ln_IT_FEES as a proxy for technology-related assurance procedures. Finally, we incorporate board characteristics, including BoardSize (the natural log of the number of board members), IndBoard (the proportion of independent directors), and GenderDiversity (the proportion of female directors on the board), which serve as crucial internal governance safeguards against reporting errors.

3.2.2 Model specification

To investigate whether cybersecurity incidents influence a firm's financial reporting quality and whether high-quality auditors mitigate this risk, we estimate the following logistic panel regression models:

$$RESTATEMENT_{it} = \beta_0 + \beta_1 CYBER\_BREACH_{it-1} + \boldsymbol{\beta Controls}_{it} + \gamma Firm_i + \delta Year_t + \epsilon_{it} \tag{1}$$

where $RESTATEMENT_{it}$ is an indicator variable equal to one if firm i issues a financial restatement in year t, and zero otherwise. To test our selective impact hypothesis, we replace the aggregate restatement variable with specific restatement types, including *Financial*, *FIN-48*, *Out-of-Period*, and *SAB 108* adjustments. This allows us to observe whether the disruption of a cyber shock is concentrated in core financial accounts versus technical compliance adjustments.

Our primary test variable is $CYBER\_BREACH_{it-1}$, which represents a lagged indicator of whether a firm experienced a documented cybersecurity incident. In separate specifications, we partition this variable into four distinct breach types—*Financial*, *Personal*, *Not Disclosed*, and *Other*—to account for the heterogeneous nature of digital risk. Control variables, firm-fixed effects, and year-fixed effects are included in all specifications to account for time-invariant firm characteristics and macroeconomic shocks.

To examine the moderating role of external assurance, we interact the $CYBER\_BREACH_{it-1}$ variable with the Big_4_{it} indicator variable as follows:

$$\begin{aligned} RESTATEMENT_{it} &= \beta_0 + \beta_1 CYBER\_BREACH_{it-1} + \beta_2 Big_{4it} \\ &+ \beta_3 (CYBER_B REACH_{it-1} \times Big_{4it}) \ + \boldsymbol{\beta Controls}_{it} + \gamma Firm_i + \delta Year_t + \epsilon_{it} \end{aligned} \tag{2}$$

The coefficient of interest, β_3, captures whether high-quality auditors attenuate the positive association between cybersecurity incidents and reporting failures. A negative and significant β_3 would suggest that Big 4 auditors provide a crucial governance buffer by applying superior technical scrutiny to compromised reporting systems.

Finally, to assess the market consequences, we estimate a firm-value model where the dependent variable is $Ln\_Tobin'sQ_{it}$, measured as the natural logarithm of the ratio of a firm's market value to its asset replacement cost at fiscal year-end. Following standard empirical literature (e.g., Chung and Pruitt, 1994), we proxy replacement cost as the sum of the book value of equity and the book value of total liabilities. In this specification, we include interaction terms between the prior cyber breach and the subsequent issuance of a restatement. This enables us to test the signaling dynamics of reporting corrections to determine whether a core financial restatement acts as a corrective signal that mitigates valuation penalties or a compounding signal of systemic failure.

3.3 Descriptive statistics

Table 1 presents the summary statistics for the key variables employed in our empirical analysis. The primary dependent variable, RESTATEMENT, has a mean value of 0.10, indicating that approximately 10% of the firm-year observations in our sample involve an accounting restatement during the sample period. Furthermore, the summary statistics for restatement types indicate that average Restate_OutOfPeriod (0.69), Restate_FIN48 (0.81), Restate_Financial (0.52), and Restate_SAB108 (0.98) represent significant portions of the corrective actions taken by firms. On cybersecurity incidents, the mean values for specific breach categories such as Breach_Financial (0.71) and Breach_NotDisclosed (0.89) suggest a high prevalence of documented incidents within the sampled firms, while Breach_Personal (0.49) and Breach_Other (0.90) further confirm this pattern. Ln_Tobin's Q shows an average market valuation of 0.55, providing a baseline for our subsequent analysis of how cyber incidents and restatements jointly influence firm value.

Insert Table 1 approximately here

The average log-transformed records lost (Ln_NUMBER_OF_RECORDS_LOST) stands at

9.98. Audit fees (Ln_AUDIT_FEES) show a mean of 15.02, while specialized fee categories like Ln_IT_FEES exhibit significant variation (St. Dev. = 1.35), potentially reflecting heterogeneous investments in IT-related audit procedures. The audit environment is characterized by a strong presence of high-quality assurance, with 79% of the firms being audited by a Big_4 firm. The financial characteristics of the sample show that firms are generally profitable, with a mean Profitability of 0.07, though 15% of the observations report a Loss. The average firm is moderately leveraged (0.27) and maintains a CashHolding ratio of 0.13. Corporate governance metrics reveal a high degree of board independence, with an average of 78.9% of board members being independent (IndBoard), and a mean BoardSize of approximately 10 members.

Table 2 reports the Pearson correlation matrix for the variables used in our analysis. The restatement indicators show strong internal correlations, particularly among Restate_Financial Restate_FIN48, and Restate_OutOfPeriod, highlighting that firms experiencing one form of misreporting are likely to exhibit related restatement types. In contrast, the overall RESTATEMENT indicator variable is only weakly correlated with most firm characteristics, suggesting that the incidence of restatements is not driven by simple observable firm traits. Meanwhile, cyber breach variables display the expected structure, monetary breach costs are strongly and positively correlated with the volume of records compromised, and breach categories exhibit significant negative associations with one another, consistent with mutually exclusive classifications of incident types. Tobin's Q is moderately correlated with breach severity measures and with key audit and governance variables, reflecting that higher-valued firms tend to be larger, more complex, and more exposed to cyber risk. Overall, the correlations indicate clear clustering among restatement measures, breach severity indicators, and valuation-related firm attributes, showing the need for multivariate controls in the empirical analysis.

Insert Table 2 approximately here

4 Empirical Results and Discussion

4.1 Univariate analysis

To provide a comprehensive view of the sample's internal dynamics, the univariate analyses here partition the data by restatement significance, breach severity, and audit quality. These comparisons serve as a preliminary diagnostic to identify how systematic disparities in reporting integrity and cyber risk exposure correlate with fundamental firm characteristics and governance structures. By isolating the distinct operational profiles of firms across these dimensions, we establish the empirical motivation for the rigorous control environment and multivariate specifications employed in our study.

We begin by examining the underlying firm characteristics associated with reporting quality, specifically partitioning the sample based on the structural impact of financial errors. Table 3 shows the univariate comparisons between firms associated with high significance restatements and those linked to other types of reporting adjustments to delineate the structural differences across these cohorts (Rice et al., 2015)[1]. The results indicate that firms with high significance restatements exhibit a marginally higher aggregate likelihood of restating while maintaining fundamentally different underlying financial and audit characteristics. Specifically, these firms are generally smaller in scale and more likely to report a loss, yet they maintain higher levels of intangible assets and research and development expenditures. In the auditing domain, the high significance cohort incurs lower total audit and tax fees and is notably less likely to be audited by a Big 4 firm compared to the control group (DeFond and Zhang, 2014). Furthermore, these firms display comparatively weaker governance attributes characterized by lower board independence and reduced gender diversity. Despite having higher cash holdings and sales growth, the market assigns a valuation discount to these firms, which likely reflects heightened information uncertainty and systemic reporting

[1] High-significance restatements are defined as indicator variables where the restatement affects core transaction processing, i.e., financial restatement.

risk (Scholz, 2008). These systematic disparities suggest that restatement significance is closely tied to firm-level complexity and oversight quality, which underscores the necessity of the rigorous controls employed in the subsequent multivariate analysis.

Insert Table 3 approximately here

Building on these reporting disparities, we next evaluate how the specific nature of a cybersecurity shock relates to a firm's financial and governance profile. Table 4 shows the univariate comparisons between firms experiencing the most critical data breaches and those undergoing other incident types to highlight systematic differences across these cohorts. The most significant breaches are characterized by a distinct operational and governance profile where firms in the high significance group exhibit a significantly higher likelihood of issuing core financial restatements despite a lower aggregate propensity for general restatements (Klamm and Watson, 2009)[2]. This pattern suggests that while these firms may report fewer total errors, the misstatements they do manifest tend to be more severe and impactful to fundamental accounting records (Beneish et al., 2008). Economically, these firms possess a substantially larger organizational scale and higher complexity, which is reflected in their higher audit and non-audit fee structures as well as their higher probability of being audited by the Big 4 (Rosati et al., 2022). Although these firms maintain more robust governance metrics, including larger boards with greater independence and gender diversity, they still suffer from a comparative valuation discount and higher leverage. These findings underscore the severe financial and reputational headwinds associated with sensitive data compromises and justify the inclusion of rigorous controls in the subsequent multivariate analysis.

Insert Table 4 approximately here

Given the distinct profiles identified in the previous partitions, we conclude the univariate analysis by investigating the systematic role of elite external monitors in managing these

[2] The Most Significant Breach category is defined as an indicator variable equal to one if the incident involved either financial or personal data, and zero otherwise.

complex risks. Table 5 reports the results of the difference-in-means tests, revealing that firms audited by the Big 4 differ fundamentally from their non-Big 4 counterparts across nearly all operational and financial dimensions. While the aggregate likelihood of a restatement does not vary substantially between the two groups, the specific nature of reporting failures is significantly different; Big 4 clients show a higher propensity for core financial restatements, whereas non-Big 4 clients exhibit higher frequencies of technical tax and timing adjustments (Francis, 2004). Furthermore, while the Big 4 cohort tends to experience a greater volume of compromised records in cyber incidents, these firms also command significantly higher market valuations and maintain more robust profitability. The data also confirm a substantial audit fee premium, highlighting that elite auditors typically oversee larger, more complex entities with greater resource commitments to specialized tax and audit services (Simunic, 1980; Hay et al., 2006). Finally, the governance profiles suggest that firms selecting high-quality auditors are characterized by more independent and diverse boards, further justifying the need to control for these endogenous selection factors in our analysis (Beasley, 1996).

Insert Table 5 approximately here

4.2 Cyber incidents and accounting restatements

Our baseline model focuses on examining whether prior-year cyber breaches increase the probability that a firm issues any restatement in a given year. The result of this analysis is presented in Table 6. Across all breach categories, the coefficients are positive and highly significant, indicating that firms experiencing a cyber incident in the previous year are more likely to subsequently issue a restatement in their reports. On one hand, this pattern is consistent with research showing that cybersecurity events disrupt internal controls, undermine data integrity, and introduce operational uncertainty that heightens misstatement risk (Alsakini et al., 2024). Since these restatements are aggregated, the estimates capture a broad

deterioration in reporting quality following cyber disruptions rather than effects tied to specific error types. On the other hand, the results contradict documented evidence according to Rosati et al. (2017) that a cybersecurity breach does not result in financial restatement, even though there is a higher probability of an SEC Comment Letter and a higher-quality audit.

Insert Table 6 approximately here

Importantly, the results remain robust after the inclusion of extensive financial, operational, and governance controls. The breach coefficients increase slightly in magnitude under the full specification, suggesting that cybersecurity incidents have an incremental effect on restatement risk that is not subsumed by firm characteristics such as size, leverage, or profitability. This finding aligns with evidence that cyber shocks create unique strains on accounting systems, through system outages, corrupted records, and weakened internal oversight, that increase the propensity for errors even in otherwise well-controlled firms (Alsakini et al., 2024). The consistently negative association between firm size and restatements mirrors prior findings that larger firms maintain more sophisticated reporting infrastructures and stronger internal control environments (Doyle et al., 2007).

The significance of several governance variables in the full model provides additional insight into factors moderating restatement likelihood. The negative coefficients on board independence and gender diversity are consistent with research showing that stronger oversight and diverse boards reduce misreporting risk by improving monitoring quality (Abbott et al., 2004; Krishnan and Parsons, 2011). Meanwhile, sales growth, intangibles, and loss indicators behave as predicted in the restatement literature, reflecting the heightened reporting challenges faced by firms with greater operational complexity or financial stress (Palmrose et al., 2004). Overall, the results provide strong evidence that cyber breaches serve as a material shock to the reporting environment, increasing the probability that firms

will issue some form of restatement in subsequent periods, independent of typical financial or governance determinants.

Restatement in firms can be of different types, including financial reporting, technical, or timing-based adjustments. Prior research highlights that restatements differ in severity, with financial restatements reflecting material errors in core accounts, while tax-related and timing-based restatements often arise from interpretational complexity or judgment-based adjustments rather than systemic breakdowns (Palmrose et al., 2004). To this effect, we consider different types of restatement, i.e., Financial, FIN48, Out-of-Period, and SAB108, to assess whether cyber breaches are associated with particular types of reporting errors. The results in Table 7 show that all breach categories are strongly and positively associated with the likelihood of a Financial restatement, with coefficients exceeding 1.25 and significant at the 1% level. These restatements represent core misstatements that materially affect the primary financial statements, and their sensitivity to cyber incidents suggests that breaches meaningfully undermine the integrity of the underlying accounting system. This aligns with evidence that cybersecurity failures weaken internal control environments, disrupt transaction processing, and compromise the reliability of financial data (Usman et al., 2023). Further, this pattern is consistent with studies showing that cyber shocks impair monitoring, increase operational complexity, and expose vulnerabilities in firms' financial reporting infrastructure, thereby heightening the probability of substantive misstatements (Kamiya et al., 2021).

Insert Table 7 approximately here

In contrast, the FIN48 restatements, related to uncertain tax positions, are sharply negative and highly significant across all breach types. This indicates that cyber breaches reduce the likelihood of tax-related restatements. One interpretation is that FIN48 adjustments involve specialized tax analysis that may be less directly disrupted by breaches of operational

or financial systems. Prior literature notes that tax restatements often stem from interpretational or regulatory complexity rather than breakdowns in internal control environments (Gleason et al., 2017). Meanwhile, coefficients for Out-of-Period and SAB108 restatements are statistically insignificant, suggesting that the timing- and threshold-based error categories are not meaningfully influenced by cybersecurity disruptions. These errors typically relate to immaterial prior-period adjustments or SAB108 quantification rules, which depend less on operational system integrity and more on managerial judgment and materiality thresholds.

Collectively, the results indicate that cyber breaches do not raise the probability of all types of restatements uniformly; instead, they are strongly associated with the most severe and impactful category, Financial restatements, while exhibiting either null or negative associations with technical tax or timing adjustments. This pattern highlights the notion that cybersecurity failures impair the reliability of core financial reporting processes rather than peripheral or specialized systems (Campbell et al., 2003). It further supports the argument that cyber incidents degrade the quality of firms' information environments in ways that directly elevate the risk of material misstatements (Hennes et al., 2008). By distinguishing restatement types, the analysis highlights that breaches primarily propagate through disruption to the financial accounting infrastructure rather than the tax, timing, or materiality-assessment components of the reporting system.

4.3 External assurance role in cyber incidents and restatements in firms

High-quality auditors play a central role in ensuring the integrity of financial reporting, particularly when firms face heightened information risk following cyber breaches. Because cybersecurity incidents weaken internal controls and compromise data reliability, strong external assurance is essential for preventing errors from propagating into financial statements (Rosati et al., 2022; Blakely et al., 2022). Evaluating whether Big 4 auditors mitigate these

risks is therefore crucial for understanding how audit quality functions as a governance mechanism that safeguards reporting credibility under cyber-related shocks (Francis et al., 1999; Krishnan, 2003). The results in Table 8 show that without a Big_4 as the auditor of a firm in the year of a cyber incident, breaches are most strongly associated with financial restatements, reflecting the way cybersecurity failures weaken internal controls and disrupt the systems that support core financial reporting (Basiouny et al., 2024; Masoud and Al-Utaibi, 2022). In contrast, the breach coefficients for FIN48, out-of-period, and SAB108 adjustments are negative or insignificant, suggesting that cyber incidents primarily compromise the accuracy of the main financial statements rather than tax-related or technical reporting processes. This is consistent with our earlier result without audit quality influence.

Insert Table 8 approximately here

However, the moderating role of Big 4 auditors appears to attenuate the relationship between cyber breaches and restatement likelihood, particularly for financial restatements Rosati et al. (2022). The negative and statistically significant interaction terms indicate that high-quality auditors help constrain the downstream reporting consequences of cybersecurity failures. This aligns with evidence that Big 4 auditors provide stronger monitoring, greater irregularity detection, and more rigorous evaluations of internal controls (Krishnan, 2003). By imposing stricter assurance procedures following breaches and scrutinizing affected accounting processes more closely, Big 4 auditors help prevent cyber-related disruptions from escalating into more severe reporting failures.

Meanwhile, the moderating effect is not uniform across restatement categories. While Big 4 auditors significantly dampen the impact of financial breaches on financial restatements, the interaction effects are weaker or statistically insignificant for FIN48 and SAB108 restatements. This pattern suggests that auditor influence is strongest in domains directly tied to core financial statements, consistent with evidence that audit quality has its greatest effect where material misstatement risk is highest (DeFond and Zhang, 2014). Restatements

related to uncertain tax positions or timing adjustments may depend more on specialized tax expertise, materiality assessment frameworks, or internal reporting processes than on external audit oversight. Overall, the findings support the theoretical view that cyber breaches disrupt financial reporting quality by undermining accounting system reliability, but that high-quality auditors serve as an effective buffer against the most severe consequences of these disruptions.

4.4 Cyber breach and restatement impact on firm value

As firms grow more dependent on digital infrastructures, cyber breaches and financial reporting errors have become critical sources of uncertainty that can alter investor confidence and reshape market valuation (Bolster et al., 2010). Examining how these events interact offers important evidence on how markets interpret organizational vulnerabilities and the extent to which corrective disclosures help restore or further erode firm value. The result in Table 9 indicates that cyber breaches have substantial and persistent negative effects on firm value (Ln_Tobin's Q) one year after the incident. Across all specifications, lagged Financial, Not Disclosed, and Personal breaches are associated with strong and statistically significant reductions in firm value. This aligns with evidence that cyberattacks generate long-lasting operational, reputational, and legal costs that depress valuation beyond the immediate event window (Goel and Shawky, 2009; Kamiya et al., 2021). The particularly pronounced negative effects for Not Disclosed breaches support prior findings that withholding or delaying information intensifies market penalties (Gordon et al., 2011). Overall, the results reinforce the idea that markets treat cyber events as signals of deeper organizational vulnerabilities that materially impair firm value.

Insert Table 9 approximately here

The interaction terms show that the market interprets restatements differently depending

on the restatement category and the breach type that preceded it. This is also in line with earlier evidence on market reactions to restatement announcements (Palmrose et al., 2004). Financial restatements mitigate part of the negative valuation effect of prior Financial and Personal breaches, suggesting that investors perceive these restatements as corrective transparency rather than further evidence of reporting failures. This is consistent with research showing that timely and credible disclosure can restore investor confidence after reporting or operational shocks (Burks, 2011; Hennes et al., 2008). In contrast, FIN48 tax-related restatements and Out-of-Period restatements amplify the valuation penalties following Personal or Financial breaches, respectively. These findings align with literature suggesting that tax-related or timing errors signal broader internal control weaknesses when combined with cybersecurity deficiencies (Lois et al., 2021). SAB108 restatements show little interaction with breach type, except for a modest standalone negative effect, suggesting that markets view these adjustments as technical corrections rather than indicators of managerial misconduct or systemic failures. Prior studies similarly document relatively mild reactions to SAB108 restatements (Burks, 2011). These findings suggest that the market response to restatements is conditional on a firm's cyber-risk environment: corrective restatements reduce valuation losses, while restatements associated with internal control weaknesses intensify them. This underscores the interconnectedness of cybersecurity and financial reporting credibility in shaping firm value.

5 Additional considerations and robustness tests

First, we consider an alternative measure of audit quality to address potential endogeneity and capture a more granular proxy of auditor effort. This supplemental test acknowledges the findings of Lawrence et al. (2011), which suggest that the superior quality often associated with the Big Four firms might stem from client selection biases instead of auditors' actual performance. This implies that a simple indicator for the Big Four status could fail

to represent the true level of audit rigor. Additionally, research by Francis (2004) indicates significant heterogeneity within the Big Four itself, noting that audit quality often depends on the expertise of the specific local office or partner rather than the overall brand name. Further studies emphasize that audit fees serve as a better proxy for audit effort and specialized knowledge (DeFond and Zhang, 2014). Consequently, we employ audit fees ratio, i.e., the ratio of audit fees to total fees (total fees include non-audit fees paid to auditors) following Rajgopal et al. (2021), as an alternative metric to verify whether the intensity of the audit process serves as a moderating factor in the cyber breach and accounting restatement outcomes.

Insert Table 10 approximately here

The results in Table 10, substantiate our earlier conclusions using Big_4 as an audit quality measure. A higher concentration of fees directed toward core assurance services signifies a prioritized commitment to audit depth, which appears to substantially decrease the likelihood of reporting failures after a digital shock. Specifically, we find that the interaction between financial breaches and audit fees is negative and is statistically significant for both Financial and Out-of-Period restatements. This consistent pattern, especially in financial restatement across both structural and effort-based proxies, reinforces the theory that heightened audit scrutiny provides a necessary defense for financial integrity. These findings suggest that when auditors dedicate substantial resources to the engagement, they can effectively identify and rectify the internal control vulnerabilities arising as a result of cyber incidents.

Next, we examine if the severity of cybersecurity breach plays a significant impact on accounting restatement using the number of records lost as a proxy. This allows us to determine whether the systemic risk signaled by a breach is compounded by its scale or if high-severity events trigger compensatory monitoring that mitigates reporting errors. The results in Table 11 indicate that the impact of cybersecurity severity is uniquely concentrated in financial restatements, whereas the coefficients for FIN48, Out-of-Period, and SAB108

restatements remain statistically indistinguishable from zero. These findings confirm our main result that cybersecurity failures primarily compromise the core accounting systems and internal controls over financial reporting that govern material accruals and revenue recognition, rather than specialized tax positions or technical adjustments (Ashbaugh-Skaife et al., 2008).

Insert Table 11 approximately here

The significant negative interaction terms observed only in financial restatement show that the marginal impact of a breach on core reporting quality decreases as the volume of lost records increases. This result is consistent with the notion that while breaches signal underlying IT control weaknesses (Haislip et al., 2016), larger, more visible "mega-breaches" attract substantial external monitoring and auditor effort that can reduce the need for restatement (Hoitash et al., 2008). The insignificance across the other three restatement types, FIN48, Out-of-Period, and SAB108, further reinforces that cybersecurity risk is not a universal driver of all accounting errors, but rather a specific indicator of vulnerability in the fundamental information systems that support high-stakes financial reporting. Overall, this result suggests that cybersecurity vulnerabilities serve as a timely proxy for idiosyncratic deterioration within the firm in the internal control environment.

6 Conclusion

This study provides a comprehensive examination of how cyber incidents propagate through the financial reporting environment and influence firm valuation. By distinguishing between different categories of reporting failures, we demonstrate that cyber shocks do not lead to a uniform deterioration in accounting quality but are specifically associated with an increased likelihood of core financial restatements. Grounded in the attention-based view, our findings

suggest a "managerial triage" mechanism where firms experiencing acute digital crises prioritize the remediation of fundamental accounting infrastructure at the expense of specialized compliance functions. The empirical evidence further highlights the critical role of external governance, as Big 4 auditors effectively mitigate the escalation of cyber risk into material reporting failures through superior technical scrutiny. Additionally, our results indicate that the market interprets subsequent restatements as conditional signals. While core financial restatements function as credible corrective disclosures that reduce uncertainty following a breach, technical or judgmental adjustments amplify valuation penalties by signaling systemic internal control deficiencies.

These findings offer important implications for regulators and practitioners in the U.S. capital markets. For boards of directors and audit committees, the results highlight the importance of integrating cybersecurity oversight with financial reporting controls, as digital vulnerabilities pose a direct threat to transactional data integrity. For regulators, our evidence supports the push for more transparent and granular cyber-risk disclosures, as investors clearly differentiate between structural failures and technical adjustments when updating firm valuations. Ultimately, this research clarifies that in an increasingly digitalized economy, financial reliability is inextricably linked to the resilience of a firm's IT infrastructure and the quality of its external monitors.

While this study offers robust insights, it is subject to several limitations. First, although our analysis categorizes breaches into financial, personal, not disclosed, and others, the data is restricted to incidents that eventually entered the public domain. This may introduce a selection bias, as truly suppressed or undetected breaches are excluded; future research could utilize private incident logs to determine if similar reporting pressures exist for non-public shocks. Second, while we control for IT_FEES as a proxy for technology-related assurance, this measure may not fully capture the specific IT-audit procedures or the depth of forensic involvement employed post-breach. Subsequent studies could investigate how the qualitative intensity of specialized forensic audit teams—rather than just the expenditure—influences

the detection of cyber-related misstatements. Finally, as this study focuses on the U.S. market, future cross-country analyses could explore how varying international regulatory frameworks and data privacy laws influence the link between digital shocks and financial reliability.

References

Abbott, L. J., Daugherty, B., Parker, S., and Peters, G. F. (2016). Internal audit quality and financial reporting quality: The joint importance of independence and competence. *Journal of Accounting Research*, 54(1):3–40.

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

Akerlof, G. A. (1970). The market for "lemons": quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3):488–500.

Al Natour, J. R. A. Q. and Al-Lahham, M. I. O. (2021). The impact of information technology on the quality of accounting information (sfac no 8, 2010). *Turkish Journal of Computer and Mathematics Education*, 12(13):885–903.

Alsakini, S. A. K., Alawawdeh, H. A., and Alsayyed, S. (2024). The impact of cybersecurity on the quality of financial statements. *Appl. Math*, 18(1):169–181.

Anderson, K. L. and Yohn, T. L. (2002). The effect of 10k restatements on firm value, information asymmetries, and investors' reliance on earnings. *Information Asymmetries, and Investors' Reliance on Earnings (September 2002)*.

Asare, S. K., Fitzgerald, B. C., Graham, L. E., Joe, J. R., Negangard, E. M., and Wolfe, C. J. (2013). Auditors' internal control over financial reporting decisions: Analysis, synthesis, and research directions. *Auditing: A Journal of Practice & Theory*, 32(Supplement 1):131–166.

Ashbaugh-Skaife, H., Collins, D. W., Kinney Jr, W. R., and LaFond, R. (2008). The effect of sox internal control deficiencies and their remediation on accrual quality. *The Accounting Review*, 83(1):217–250.

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

August, T., Noh, D., Shamir, N., and Shin, H. (2025). Cyberattacks, operational disruption, and investment in resilience measures. *Management Science*, 71(9):7390–7413.

Basiouny, M. M. M. et al. (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.

Beasley, M. S. (1996). An empirical analysis of the relation between the board of director composition and financial statement fraud. *Accounting Review*, pages 443–465.

Beneish, M. D., Billings, M. B., and Hodder, L. D. (2008). Internal control weaknesses and information uncertainty. *The Accounting Review*, 83(3):665–703.

Blakely, B., Kurtenbach, J., and Nowak, L. (2022). Exploring the information content of cyber breach reports and the relationship to internal controls. *International Journal of Accounting Information Systems*, 46:100568.

Bolster, P., Pantalone, C. H., and Trahan, E. A. (2010). Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis*, 5(1).

Burks, J. (2011). Are investors confused by restatements after sarbanes–oxley? *The Accounting Review*, 86(2):507–538.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448.

Cavusoglu, H., Mishra, B., and 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.

Chung, K. H. and Pruitt, S. W. (1994). A simple approximation of tobin's q. *Financial Management*, pages 70–74.

Das, S., Mukhopadhyay, A., and Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, 8(4):27–55.

DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of Accounting and Economics*, 3(3):183–199.

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

Doyle, J. T., Ge, W., and McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44(1–2):193–223.

Dzuranin, A. C. and Mălăescu, I. (2016). The current state and future direction of it audit: Challenges and opportunities. *Journal of Information Systems*, 30(1):7–20.

Eling, M. and Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5):474–491.

Eling, M. and Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3):1109–1119.

Francis, J. R. (2004). What do we know about audit quality? *The British Accounting Review*, 36(4):345–368.

Francis, J. R., Maydew, E. L., and Sparks, H. C. (1999). The role of Big 6 auditors in the credible reporting of accruals. *Auditing: A Journal of Practice & Theory*, 18(2):17–34.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., and Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 40(1):183–199.

Garg, A., Curtis, J., and Halper, H. (2003). Quantifying the financial impact of it security breaches. *Information Management & Computer Security*, 11(2):74–83.

Gleason, C. A., Pincus, M., and Rego, S. O. (2017). Material weaknesses in tax-related internal controls and last chance earnings management. *The Journal of the American Taxation Association*, 39(1):25–44.

Goel, S. and Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7):404–410.

Gordon, L. A., Loeb, M. P., and 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.

Grabski, S. V., Leech, S. A., and Schmidt, P. J. (2011). A review of ERP research: A future agenda for accounting information systems. *Journal of Information Systems*, 25(1):37–78.

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

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

Hennes, K. M., Leone, A. J., and Miller, B. P. (2008). The importance of distinguishing errors from irregularities in restatement research: The case of restatements and CEO/CFO turnover. *The Accounting Review*, 83(6):1487–1519.

Her, Y.-W., Lim, J., and Son, M. (2010). The impact of financial restatements on audit fees: Consideration of restatement severity. *International Review of Accounting, Banking and Finance*, 2(4):1–22.

Hoitash, R., Hoitash, U., and Bedard, J. C. (2008). Internal control quality and audit pricing under the sarbanes-oxley act. *Auditing: A Journal of Practice & Theory*, 27(1):105–126.

Jensen, M. C. and Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4):305–360.

Juma'h, A. H. and Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, 28(2):275–301.

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

Klamm, B. K. and Watson, M. W. (2009). SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems*, 23(2):1–23.

Ko, M., Dorantes, C., et al. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, 17(2):13–22.

Krishnan, G. V. and Parsons, L. M. (2011). Gender diversity in the boardroom and firm financial reporting quality. *Accounting Horizons*, 25(4):409–432.

Krishnan, J. (2003). Audit quality and the pricing of discretionary accruals. *Auditing: A Journal of Practice & Theory*, 22(1):109–126.

Kuhn, J. R. and Morris, B. (2017). It internal control weaknesses and the market value of firms. *Journal of Enterprise Information Management*, 30(6):964–986.

Kuhn Jr, J. R., Ahuja, M., and Mueller, J. (2013). An examination of the relationship of IT control weakness to company financial performance and health. *International Journal of Accounting & Information Management*, 21(3):227–240.

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

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., and Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, 13(1):25–47.

Masoud, N. and Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, 76(2):131–140.

Muktadir-Al-Mukit, D. and Ali, M. H. (2025). The dynamics of stock market responses following the cyber-attacks news: Evidence from event study. *Information Systems Frontiers*, pages 1–18.

Ocasio, W. (1997). Towards an attention-based view of the firm. *Strategic Management Journal*, 18(S1):187–206.

Palmrose, Z.-V., Richardson, V. J., and Scholz, S. (2004). Determinants of market reactions to restatement announcements. *Journal of Accounting and Economics*, 37(1):59–89.

Rajgopal, S., Srinivasan, S., and Zheng, X. (2021). Measuring audit quality. *Review of Accounting Studies*, 26(2):559–619.

Rice, S. C., Weber, D. P., and Wu, B. (2015). Does SOX 404 have teeth? Consequences of the failure to report existing internal control weaknesses. *The Accounting Review*, 90(3):1169–1200.

Rosati, P., Gogolin, F., and Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3):701–728.

Rosati, P., Gogolin, F., and Lynn, T. G. (2017). Cyber-security incidents, external monitoring and probability of restatements. *External Monitoring and Probability of Restatements (July 29, 2017)*.

Scholz, S. (2008). The changing nature and consequences of public company financial restatements. *The US Department of the Treasury*.

Simunic, D. A. (1980). The pricing of audit services: Theory and evidence. *Journal of Accounting Research*, pages 161–190.

Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, 87(3):355–374.

Usman, A., Ahmad, A. C., and Abdulmalik, S. O. (2023). The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, 8(8):32.

Watts, R. L. and Zimmerman, J. L. (1978). Towards a positive theory of the determination of accounting standards. *Accounting Review*, pages 112–134.

Zafar, H., Ko, M. S., and Osei-Bryson, K.-M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, 18(6):1205–1215.

Zhang, I. X. (2007). Economic consequences of the Sarbanes–Oxley Act of 2002. *Journal of Accounting and Economics*, 44(1-2):74–115.

Table 1: Descriptive Statistics

This table reports summary statistics for all variables used in the study. Continuous variables are winsorized at the 1st and 99th percentiles where appropriate. Tobin's Q, Fee and breach-cost variables are in natural logarithms. Indicator variables (e.g., *RESTATEMENT*, *Loss*, breach categories, *Big_4*, restatement types) equal one when the condition applies and zero otherwise. *Tangibility*, *CashHolding*, *Intangibles*, and *leverage* are balance-sheet ratios. *Capex* is capital expenditures scaled by total assets. *Firm_Size* and *Ln_NEmployee* are natural logarithms of total assets and number of employees.

Variable	N	Mean	St. Dev.	Min	Max
RESTATEMENT	61,229	0.10	0.30	0	1
Restate_OutOfPeriod	61,229	0.69	0.46	0	1
Restate_FIN48	61,229	0.81	0.39	0	1
Restate_Financial	61,229	0.52	0.50	0	1
Restate_SAB108	61,229	0.98	0.14	0	1
Breach_Financial	61,229	0.71	0.45	0	1
Breach_NotDisclosed	61,229	0.89	0.31	0	1
Breach_Personal	61,229	0.49	0.50	0	1
Breach_Other	61,229	0.90	0.30	0	1
Ln_Tobin's Q	54,211	0.55	0.34	−1.29	1.56
Ln_NUMBER_OF_RECORDS_LOST	21,575	9.98	4.38	0.69	20.60
Ln_BREACH_COST	23,150	4.20	7.08	0.00	19.21
Ln_BREACH_COST_USD	7,568	12.67	6.67	0.00	19.76
Ln_AUDIT_FEES	61,229	15.02	1.33	11.31	17.82
Ln_NON_AUDIT_FEES	61,229	12.64	3.49	0.00	17.19
Ln_TOTAL_FEES	61,229	15.30	1.31	11.80	18.21
Ln_BENEFITS_FEES	61,229	0.26	1.62	0.00	10.99
Ln_IT_FEES	61,229	0.15	1.35	0.00	12.61
Ln_TAX_FEES	61,229	9.42	5.69	0.00	16.13
Ln_TAX_FEES_COMPLIANCE	7,440	12.37	1.76	6.69	15.93
Ln_TAX_FEES_NON_COMPLIANCE	6,346	11.23	4.64	0.00	15.72
Ln_AUDIT_RELATED_FEES	61,229	9.60	5.79	0.00	16.71
Ln_OTHER_FEES	61,229	5.53	5.66	0.00	15.79
CashHolding	61,224	0.13	0.15	0.00	0.98
Tangibility	58,564	0.22	0.23	0.00	0.98
leverage	61,006	0.27	0.25	0.00	3.89
Firm_Size	61,224	9.02	2.29	1.24	15.20
Intangibles	59,987	0.21	0.21	0.00	0.96
Profitability	61,224	0.07	0.13	−4.50	0.73
Loss	61,224	0.15	0.36	0	1
Capex	60,757	0.04	0.04	−0.01	0.58
Book_to_Market	57,245	4.88	109.95	−1,273.45	7,071.35
RandD_Expenses	28,715	1,233.57	4,957.05	0.00	88,544.00
AuditBoardCommittee	48,787	0.99	0.08	0	1
BoardSize	48,787	10.31	2.91	3	98
GenderDiversity	48,787	19.00	11.63	0.00	66.67
IndBoard	48,787	78.90	14.35	0.00	100.00
Ln_NEmployee	60,871	9.37	1.92	0.69	14.65
Sales_growth	59,031	0.06	0.23	−3.45	5.35
Big_4	61,229	0.79	0.29	0	1

Table 2: Pearson Correlation Matrix

This table presents the Pearson correlation matrix for all variables in our analysis. Values in **bold** denote correlations that are statistically significant at the 1% level.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)	(26)	(27)	(28)	(29)	(30)	(31)	(32)	(33)	(34)	(35)	(36)	(37)	(38)	(39)	(40)
(1) RESTATEMENT																																								
(2) Restate_OutOfPeriod	0.024																																							
(3) Restate_FIN48	0.009	**-0.327**																																						
(4) Restate_Financial	-0.022	**-0.641**	**-0.466**																																					
(5) Restate_SAB108	-0.029	**-0.097**	**-0.070**	**-0.137**																																			
(6) Ln_N_OF_RECORDS_LOST	-0.013	0.024	**-0.079**	0.051	-0.030																																			
(7) Ln_BREACH_COST	-0.013	0.003	-0.004	0.012	-0.049	**0.231**																																		
(8) Ln_BREACH_COST_USD	-0.011	**-0.092**	0.045	0.054	-0.023	0.143	**1.000**																																	
(9) Breach_Financial	0.038	0.032	-0.026	-0.008	-0.001	0.048	**-0.198**	**-0.175**																																
(10) Breach_NotDisclosed	-0.016	-0.026	-0.023	0.048	-0.021	**-0.111**	-0.041	**-0.156**	**-0.222**																															
(11) Breach_Personal	0.001	0.006	0.015	-0.021	0.012	-0.0002	**0.298**	**0.186**	**-0.645**	**-0.353**																														
(12) Breach_Other	-0.043	-0.032	0.039	-0.002	0.003	**-0.080**	**-0.132**	0.157	**-0.208**	**-0.114**	**-0.332**																													
(13) Ln_ Tobin's Q	-0.003	-0.004	**-0.092**	**0.089**	-0.043	**0.226**	0.020	-0.028	-0.021	0.042	0.053	**-0.099**																												
(14) Ln_AUDIT_FEES	**-0.100**	**-0.090**	**-0.094**	**0.153**	0.019	**0.094**	-0.114	0.143	-0.029	0.101	-0.049	0.021	0.101																											
(15) Ln_NON_AUDIT_FEES	-0.039	-0.023	**-0.098**	**0.100**	-0.006	**0.099**	0.010	0.056	**-0.061**	0.084	0.001	0.003	**0.138**	**0.476**																									
(16) Ln_TOTAL_FEES	**-0.089**	**-0.090**	**-0.106**	**0.161**	0.019	**0.113**	-0.109	0.138	-0.033	0.114	-0.048	0.012	0.124	**0.967**	**0.581**																									
(17) Ln_BENEFITS_FEES	0.036	0.031	-0.011	-0.014	-0.021	0.003	-0.046	-0.117	-0.001	-0.021	0.016	-0.003	0.009	-0.046	0.012	-0.042																									
(18) Ln_IT_FEES	0.010	0.009	-0.009	-0.001	0.001	0.024	-0.017	-0.034	0.007	0.001	0.0003	-0.012	0.016	-0.040	**0.101**	0.078	0.023																							
(19) Ln_TAX_FEES	-0.047	-0.033	-0.053	0.078	-0.023	**0.154**	0.076	0.070	-0.095	0.027	0.065	0.007	**0.213**	**0.407**	**0.568**	**0.435**	0.020	-0.086																					
(20) Ln_TAX_FEES_COMPLIANCE	0.025	**0.107**	**-0.122**	-0.001	0.001	**0.155**	-0.128	**-0.347**	0.060	-0.045	-0.045	0.017	-0.081	**0.435**	**0.538**	**0.463**	0.025	—	**0.789**																					
(21) Ln_TAX_FEES_NON_COMP	**-0.112**	**-0.080**	-0.047	**0.093**	**0.117**	0.024	0.020	**-0.154**	**-0.211**	0.012	**0.114**	**0.142**	**0.114**	**0.324**	**0.522**	**0.380**	-0.047	—	**0.619**	0.229																				
(22) Ln_AUDIT_RELATED_FEES	**-0.059**	-0.042	**-0.090**	**0.111**	-0.002	0.057	-0.049	0.058	**-0.046**	**0.096**	-0.036	0.029	**0.068**	**0.534**	**0.607**	**0.556**	-0.143	-0.109	**0.383**	0.219	0.222																			
(23) Ln_OTHER_FEES	0.009	**-0.057**	0.007	0.037	0.036	-0.033	-0.060	**-0.125**	-0.030	0.023	0.012	0.003	**0.095**	**0.137**	**0.334**	**0.229**	-0.009	**0.168**	0.071	-0.084	**0.309**	0.036																		
(24) CashHolding	0.023	**0.066**	**-0.043**	-0.023	-0.017	**0.112**	0.013	**-0.197**	**0.080**	-0.052	0.032	**-0.123**	**0.202**	-0.091	-0.004	**-0.086**	0.005	0.019	**0.066**	-0.025	-0.003	-0.068	0.012																	
(25) Tangibility	**0.055**	0.023	-0.014	-0.006	-0.013	-0.047	-0.061	0.014	0.016	0.034	**-0.076**	0.066	-0.013	**-0.157**	**-0.122**	**-0.169**	0.005	-0.012	**-0.159**	0.007	**-0.407**	**-0.119**	-0.017	**-0.250**															
(26) leverage	-0.013	**0.036**	-0.036	0.005	-0.037	**0.085**	-0.019	**0.169**	0.010	**0.083**	**-0.088**	0.046	**0.195**	0.011	-0.037	-0.005	-0.011	-0.017	-0.025	**0.166**	**-0.179**	-0.015	-0.023	**-0.165**	**0.293**														
(27) Firm_size	**-0.087**	**-0.098**	**-0.099**	**0.164**	0.017	0.054	**-0.140**	**0.175**	**-0.060**	**0.150**	-0.077	**0.064**	0.005	**0.835**	**0.489**	**0.854**	-0.052	0.013	**0.309**	**0.306**	**0.368**	**0.536**	**0.196**	**-0.208**	-0.106	-0.057														
(28) Intangibles	-0.041	**0.085**	-0.049	-0.036	-0.019	0.006	**0.144**	0.024	**0.104**	-0.010	-0.049	**-0.066**	**0.118**	0.047	0.035	0.035	0.032	-0.041	**0.083**	0.039	-0.094	0.008	0.008	**-0.148**	**-0.192**	**0.185**	-0.106												
(29) Profitability	0.003	0.011	**-0.102**	**0.084**	-0.047	**0.135**	0.061	0.031	-0.008	-0.013	0.023	-0.013	**0.247**	**0.095**	**0.086**	**0.099**	0.021	-0.006	**0.113**	0.090	**0.105**	0.050	0.048	-0.064	0.044	**0.147**	0.059	**0.094**											
(30) Loss	0.0001	**0.038**	**0.055**	**-0.082**	0.010	-0.031	-0.002	0.015	**0.040**	0.003	-0.013	**-0.044**	**-0.165**	**-0.157**	**-0.151**	**-0.166**	0.002	0.010	**-0.133**	**-0.103**	**-0.197**	**-0.125**	**-0.110**	**0.099**	0.049	**0.092**	**-0.226**	0.013	**-0.365**										
(31) Capex	**0.051**	**0.047**	-0.024	-0.019	-0.021	-0.036	-0.061	**-0.087**	**0.046**	0.014	**-0.072**	0.039	**0.099**	**-0.181**	-0.084	**-0.168**	0.011	**0.058**	**-0.141**	0.015	**-0.471**	**-0.103**	0.026	-0.066	**0.706**	**0.181**	-0.185	**-0.094**	0.075	0.007									
(32) Book_to_Market	-0.007	-0.003	0.002	0.002	0.001	0.012	-0.001	-0.018	0.012	0.007	-0.016	0.002	**0.084**	-0.015	0.007	-0.010	-0.006	-0.001	-0.008	**0.028**	0.045	-0.008	0.021	0.003	0.014	0.023	-0.015	-0.002	-0.006	0.025	0.018							
(33) RandD_Expenses	**-0.056**	0.034	**-0.145**	**0.083**	0.027	0.047	-0.060	-0.068	**0.106**	-0.009	-0.025	**-0.088**	**0.182**	**0.351**	**0.219**	**0.365**	-0.026	-0.014	0.092	**0.126**	**0.224**	**0.225**	**0.224**	**0.148**	0.002	-0.059	**0.405**	-0.062	**0.101**	-0.075	**0.116**	0.010							
(34) AuditBoardCommittee	-0.004	-0.011	0.007	0.001	0.016	-0.016	-0.002	-0.037	0.010	-0.007	-0.024	0.033	-0.048	0.028	-0.046	-0.019	0.013	**-0.167**	0.007	—	—	-0.015	-0.037	0.002	0.031	0.001	0.005	0.012	-0.038	0.015	0.018	-0.001	0.022						
(35) BoardSize	-0.005	0.003	**-0.071**	**0.067**	-0.048	-0.004	0.006	**0.199**	-0.045	**0.077**	-0.060	**0.087**	0.041	**0.366**	**0.279**	**0.384**	0.012	0.050	**0.162**	**0.439**	-0.009	**0.264**	0.050	**-0.147**	**0.086**	0.059	**0.418**	0.024	0.045	**-0.112**	0.014	-0.007	**0.079**	-0.002					
(36) GenderDiversity	**-0.087**	-0.035	-0.011	**0.050**	-0.032	-0.003	**-0.071**	-0.044	**-0.081**	**0.115**	0.004	-0.007	**0.160**	**0.338**	**0.162**	**0.317**	0.006	-0.055	**0.171**	0.067	0.074	**0.174**	0.040	-0.035	-0.053	0.059	**0.273**	0.030	**0.077**	-0.079	-0.072	0.006	**0.208**	0.022	**0.171**				
(37) IndBoard	**-0.067**	**-0.067**	-0.019	**0.078**	-0.0001	**0.152**	0.077	0.066	**-0.076**	0.022	0.041	0.024	**0.101**	**0.201**	**0.117**	**0.187**	0.007	-0.021	**0.190**	0.034	-0.027	**0.157**	-0.007	0.035	**-0.177**	-0.041	**0.184**	-0.101	-0.044	-0.011	**-0.201**	0.015	**0.091**	0.018	-0.005	**0.310**			
(38) Ln_NEmployee	-0.040	-0.028	**-0.169**	**0.167**	-0.025	**0.215**	-0.006	**0.224**	-0.070	**0.104**	-0.034	0.055	**0.203**	**0.703**	**0.465**	**0.726**	-0.001	0.025	**0.339**	**0.437**	**0.184**	**0.439**	**0.169**	**-0.190**	**0.184**	**0.118**	**0.705**	0.026	**0.255**	**-0.238**	**0.115**	-0.004	**0.264**	-0.012	**0.438**	**0.278**	0.069		
(39) Sales_growth	-0.008	**0.024**	-0.008	-0.017	0.004	0.008	-0.003	-0.038	0.018	-0.002	-0.007	-0.013	**0.141**	-0.058	-0.008	-0.057	-0.005	-0.026	0.011	-0.028	0.053	-0.005	-0.013	0.083	-0.020	-0.035	-0.038	**0.062**	-0.034	**-0.123**	0.041	0.006	0.023	-0.015	-0.032	**-0.055**	-0.024	-0.037	
(40) Big_4	-0.002	**-0.089**	-0.030	**0.102**	0.014	0.025	-0.022	0.019	-0.023	**0.095**	-0.052	0.023	**0.122**	**0.408**	**0.296**	**0.404**	-0.049	-0.030	**0.260**	**0.207**	**0.240**	**0.242**	**0.123**	-0.004	-0.004	**0.041**	**0.356**	0.028	**0.118**	**-0.144**	-0.038	0.008	**0.082**	-0.018	**0.178**	**0.168**	**0.150**	**0.316**	-0.024

Table 3: Difference in Means — High-significance Restatements vs Low-significance Restatements

This table reports the univariate comparisons between firms with the most significant restatements and those with other restatements. High-significance restatement is defined as an indicator variable where the restatement affects core transaction processing (i.e., compromising payment or banking details). Significance levels at 1%, 5%, and 10% are denoted by ***, **, and *, respectively.

	Most Sig.	**Low Sig.**	**Diff. (t-stat)**
RESTATEMENT	0.102	0.092	0.009***
			(3.743)
Ln_Tobin's Q	0.548	0.567	-0.019***
			(-3.975)
Ln_NUMBER_OF_RECORDS_LOST	10.027	9.897	0.130**
			(2.038)
Ln_BREACH_COST	4.152	4.298	-0.146
			(-1.445)
Ln_BREACH_COST_USD	12.243	13.651	-1.408***
			(-8.912)
Ln_AUDIT_FEES	14.946	15.182	-0.235***
			(-21.267)
Ln_NON_AUDIT_FEES	12.582	12.762	-0.180***
			(-5.984)
Ln_TOTAL_FEES	15.220	15.450	-0.230***
			(-21.086)
Ln_BENEFITS_FEES	0.283	0.200	0.083***
			(6.335)
Ln_IT_FEES	0.158	0.132	0.027**
			(2.394)
Ln_TAX_FEES	9.260	9.732	-0.472***
			(-9.746)
Ln_TAX_FEES_COMPLIANCE	12.520	12.137	0.383***
			(9.349)
Ln_TAX_FEES_NON_COMPLIANCE	11.036	11.535	-0.499***
			(-4.260)
Ln_AUDIT_RELATED_FEES	9.430	9.946	-0.516***
			(-10.449)
Ln_OTHER_FEES	5.348	5.891	-0.543***
			(-11.215)
CashHolding	0.140	0.121	0.019***
			(15.616)
Tangibility	0.226	0.217	0.009***
			(4.481)
leverage	0.273	0.260	0.013***
			(6.287)
Firm_Size	8.868	9.313	-0.445***
			(-23.284)
Intangibles	0.219	0.183	0.036***
			(19.480)
Profitability	0.070	0.071	-0.001
			(-0.827)
Loss	0.163	0.132	0.031***
			(10.379)
Capex	0.039	0.035	0.004***
			(9.770)
Book_to_Market	4.639	5.385	-0.746
			(-0.706)
RandD_Expenses	1378.655	931.996	446.658***
			(8.568)
AuditBoardCommittee	0.992	0.994	-0.001
			(-1.515)
BoardSize	10.292	10.356	-0.063**
			(-2.120)
GenderDiversity	18.636	19.714	-1.078***
			(-9.798)
IndBoard	78.226	80.217	-1.991***
			(-14.697)
Ln_NEmployee	9.319	9.464	-0.145***
			(-8.910)
Sales_growth	0.064	0.052	0.012***
			(6.654)
Big_4	0.887	0.938	-0.052***
			(-22.521)
Breach_Financial	0.721	0.692	0.029***
			(7.505)
Breach_NotDisclosed	0.885	0.906	-0.021***
			(-8.100)
Breach_Personal	0.497	0.486	0.010**
			(2.428)
Breach_Other	0.897	0.916	-0.019***
			(-7.689)

Table 4: Difference in Means — Most-significant Breaches vs Less-significant Breaches

This table reports the univariate comparisons between firms experiencing the most critical data breaches and those undergoing other incident types. The **Most-Significant Breach** category is an indicator variable equal to one if the incident involved either **Financial** or **Personal** information, and zero otherwise. Significance levels at 1%, 5%, and 10% are denoted by ***, **, and *, respectively.

	Most Sig.	**Less Sig.**	**Diff. (t-stat)**
RESTATEMENT	0.092	0.124	-0.032***
			(-9.998)
Ln_Tobin's Q	0.544	0.594	-0.050***
			(-9.686)
Ln_NUMBER_OF_RECORDS_LOST	9.879	13.476	-3.597***
			(-20.140)
Ln_BREACH_COST	3.554	5.515	-1.962***
			(-19.432)
Ln_BREACH_COST_USD	12.762	12.545	0.217
			(1.429)
Ln_AUDIT_FEES	15.087	14.782	0.305***
			(21.597)
Ln_NON_AUDIT_FEES	12.761	12.179	0.581***
			(15.705)
Ln_TOTAL_FEES	15.361	15.046	0.315***
			(22.602)
Ln_BENEFITS_FEES	0.241	0.314	-0.073***
			(-4.196)
Ln_IT_FEES	0.144	0.172	-0.028**
			(-1.990)
Ln_TAX_FEES	9.493	9.118	0.375***
			(6.602)
Ln_TAX_FEES_COMPLIANCE	12.356	12.436	-0.080*
			(-1.651)
Ln_TAX_FEES_NON_COMPLIANCE	11.497	10.019	1.479***
			(8.433)
Ln_AUDIT_RELATED_FEES	9.882	8.513	1.369***
			(22.872)
Ln_OTHER_FEES	5.584	5.313	0.271***
			(4.787)
CashHolding	0.124	0.172	-0.048***
			(-28.194)
Tangibility	0.232	0.190	0.041***
			(21.516)
leverage	0.281	0.220	0.062***
			(30.958)
Firm_Size	9.203	8.285	0.918***
			(40.933)
Intangibles	0.201	0.231	-0.030***
			(-13.552)
Profitability	0.069	0.075	-0.006***
			(-5.085)
Loss	0.148	0.174	-0.026***
			(-7.019)
Capex	0.038	0.034	0.004***
			(10.555)
Book_to_Market	5.264	3.449	1.815***
			(2.760)
RandD_Expenses	1003.937	1874.437	-870.499***
			(-11.820)
AuditBoardCommittee	0.994	0.990	0.004***
			(3.560)
BoardSize	10.498	9.616	0.882***
			(29.386)
GenderDiversity	19.507	17.095	2.412***
			(17.960)
IndBoard	79.154	77.954	1.200***
			(7.562)
Ln_NEmployee	9.485	8.913	0.572***
			(28.145)
Sales_growth	0.059	0.065	-0.006***
			(-2.610)
Big_4	0.917	0.851	0.066***
			(19.332)
Restate_OutOfPeriod	0.679	0.729	-0.049***
			(-10.963)
Restate_FIN48	0.810	0.799	0.010***
			(2.610)
Restate_Financial	0.532	0.488	0.044***
			(8.752)
Restate_SAB108	0.979	0.984	-0.005***
			(-3.730)

Table 5: Difference in Means — Big-4 vs Non–Big-4

This table reports the univariate comparisons between firms audited by a **Big-4** auditor and those audited by **Non-Big-4** firms. The analysis highlights fundamental operational, financial, and governance differences based on auditor choice. Significance levels at 1%, 5%, and 10% are denoted by ***, **, and *, respectively.

	Big-4	**Non-Big-4**	**Diff. (t-stat)**
RESTATEMENT	0.098	0.100	-0.002
			(-0.462)
Restate_OutOfPeriod	0.676	0.815	-0.139***
			(-25.544)
Restate_FIN48	0.804	0.845	-0.041***
			(-8.121)
Restate_Financial	0.540	0.367	0.173***
			(26.067)
Restate_SAB108	0.980	0.974	0.007***
			(3.151)
Breach_Financial	0.708	0.743	-0.035***
			(-5.847)
Breach_NotDisclosed	0.901	0.801	0.100***
			(18.735)
Breach_Personal	0.485	0.573	-0.088***
			(-13.042)
Breach_Other	0.906	0.882	0.023***
			(5.322)
Ln_Tobin's Q	0.575	0.370	0.205***
			(26.576)
Ln_NUMBER_OF_RECORDS_LOST	10.013	9.577	0.436***
			(4.770)
Ln_BREACH_COST	4.133	4.564	-0.431***
			(-3.481)
Ln_BREACH_COST_USD	12.724	12.386	0.338**
			(2.023)
Ln_AUDIT_FEES	15.202	13.359	1.842***
			(113.127)
Ln_NON_AUDIT_FEES	12.979	9.469	3.510***
			(55.307)
Ln_TOTAL_FEES	15.469	13.672	1.798***
			(115.308)
Ln_BENEFITS_FEES	0.230	0.499	-0.269***
			(-9.197)
Ln_IT_FEES	0.136	0.274	-0.138***
			(-5.810)
Ln_TAX_FEES	9.898	4.890	5.009***
			(66.562)
Ln_TAX_FEES_COMPLIANCE	12.446	10.627	1.819***
			(17.779)
Ln_TAX_FEES_NON_COMPLIANCE	11.445	5.338	6.107***
			(14.845)
Ln_AUDIT_RELATED_FEES	10.057	5.318	4.740***
			(62.165)
Ln_OTHER_FEES	5.756	3.387	2.369***
			(32.209)
CashHolding	0.133	0.136	-0.002
			(-0.990)
Tangibility	0.223	0.226	-0.003
			(-0.879)
leverage	0.272	0.237	0.035***
			(11.906)
Firm_Size	9.280	6.525	2.755***
			(112.331)
Intangibles	0.209	0.189	0.020***
			(6.748)
Profitability	0.075	0.022	0.053***
			(14.727)
Loss	0.136	0.312	-0.176***
			(-28.379)
Capex	0.037	0.042	-0.005***
			(-7.933)
Book_to_Market	5.169	2.378	2.791***
			(5.362)
RandD_Expenses	1370.910	38.617	1332.293***
			(40.949)
AuditBoardCommittee	0.992	0.998	-0.006***
			(-6.736)
BoardSize	10.460	8.477	1.983***
			(42.976)
GenderDiversity	19.556	12.073	7.483***
			(36.456)
IndBoard	79.510	71.309	8.201***
			(30.078)
Ln_NEmployee	9.565	7.510	2.054***
			(79.548)
Sales_growth	0.059	0.077	-0.019***
			(-3.476)

Table 6: Cyber Breach and Restatement

This table reports the results of the logistic panel regression examining the impact of prior-year cybersecurity incidents on the likelihood of aggregate accounting restatements. Column (1) includes baseline financial controls, while Column (2) incorporates the full set of operational and governance control variables. All specifications include firm and year-fixed effects to account for time-invariant characteristics and temporal shocks. Significance levels at 1%, 5%, and 10% are denoted by ***, **, and *, respectively.

	RESTATEMENT	
	Base Controls	Full Controls
	(1)	(2)
Breach_Financial_lag1	0.196***	0.229***
	(0.027)	(0.078)
Breach_Not Disclosed_lag1	0.217***	0.251***
	(0.030)	(0.082)
Breach_Other_lag1	0.254***	0.301***
	(0.040)	(0.087)
Breach_Personal_lag1	0.219***	0.249***
	(0.029)	(0.078)
CashHolding	0.017	0.026
	(0.045)	(0.058)
Tangibility	0.072	0.042
	(0.044)	(0.056)
leverage	−0.027	−0.021
	(0.025)	(0.030)
Firm_Size	−0.013***	−0.020***
	(0.003)	(0.006)
Intangibles	−0.052	−0.084**
	(0.033)	(0.041)
Profitability	0.012	−0.027
	(0.037)	(0.080)
Loss	−0.021	−0.034*
	(0.013)	(0.018)
Capex	0.004	−0.115
	(0.201)	(0.231)
Book_to_Market	−0.00002**	−0.00001
	(0.00001)	(0.00001)
Ln_NEmployee		0.011*
		(0.006)
Sales_growth		−0.048**
		(0.021)
Ln_IT_FEES		0.001
		(0.005)
AuditBoardCommittee		0.036
		(0.047)
BoardSize		0.002
		(0.003)
GenderDiversity		−0.001*
		(0.001)
IndBoard		−0.001*
		(0.0005)
Firm and Year FE	Yes	Yes
Observations	53,788	40,793
Adjusted R^2	0.117	0.129

Table 7: Cyber breaches and Restatement Types

This table reports logistic panel regression results examining the impact of lagged cybersecurity incidents on various categories of reporting corrections. Column (1) focuses on core **Financial** restatements, while Columns (2)–(4) examine technical adjustments (**FIN48**, **Out-of-Period**, and **SAB108**). All specifications include firm and year-fixed effects. Significance levels at 1%, 5%, and 10% are denoted by ***, **, and *, respectively.

	RESTATEMENT			
	Financial	FIN48	Out-of-Period	SAB108
	(1)	(2)	(3)	(4)
Breach_Financial_lag1	1.257***	−0.428***	0.156	0.015
	(0.182)	(0.098)	(0.163)	(0.040)
Breach_NotDisclosed_lag1	1.301***	−0.413***	0.110	0.001
	(0.173)	(0.094)	(0.155)	(0.040)
Breach_Other_lag1	1.262***	−0.370***	0.105	0.004
	(0.167)	(0.091)	(0.144)	(0.038)
Breach_Personal_lag1	1.254***	−0.406***	0.138	0.014
	(0.182)	(0.097)	(0.161)	(0.040)
CashHolding	−0.088	0.252***	−0.219	0.055
	(0.167)	(0.096)	(0.163)	(0.056)
Tangibility	0.031	0.030	−0.067	0.006
	(0.120)	(0.083)	(0.136)	(0.028)
leverage	0.028	0.028	−0.069	0.013
	(0.069)	(0.061)	(0.048)	(0.027)
Firm_Size	−0.026	0.006	0.024	−0.004
	(0.021)	(0.010)	(0.022)	(0.003)
Intangibles	−0.066	0.145*	−0.086	0.007
	(0.121)	(0.082)	(0.128)	(0.033)
Profitability	−0.414**	0.440***	−0.110	0.084
	(0.179)	(0.108)	(0.150)	(0.053)
Loss	−0.004	0.024	−0.021	0.0003
	(0.023)	(0.015)	(0.023)	(0.004)
Capex	−0.120	−0.056	0.283	−0.107
	(0.449)	(0.325)	(0.494)	(0.090)
Book_to_Market	−0.00002	−0.00000	0.00002	0.00000
	(0.00002)	(0.00002)	(0.00004)	(0.00001)
Ln_NEmployee	−0.020	0.030***	−0.011	0.002
	(0.020)	(0.010)	(0.022)	(0.004)
Sales_growth	0.038	−0.022	−0.008	−0.008
	(0.026)	(0.022)	(0.027)	(0.006)
AuditBoardCommittee	−0.094	0.076*	0.043	−0.025
	(0.112)	(0.042)	(0.082)	(0.024)
BoardSize	−0.001	0.002	−0.004	0.003***
	(0.006)	(0.003)	(0.007)	(0.001)
GenderDiversity	−0.001	−0.001	0.001	0.0004
	(0.002)	(0.001)	(0.001)	(0.0004)
IndBoard	−0.003**	0.001*	0.001	0.00003
	(0.001)	(0.001)	(0.001)	(0.0004)
Firm and Year FE	Yes	Yes	Yes	Yes
Observations	40,793	40,793	40,793	40,793
Adjusted R^2	0.489	0.252	0.327	0.335

Table 8: Big_4 Auditors' moderation of Cyber Breach and Restatement Types

This table reports logistic panel regression results examining the moderating effect of **Big_4** auditors on the relationship between lagged cybersecurity breaches and various restatement types. The interaction terms test whether high-quality external assurance attenuates reporting failures following digital shocks. For brevity, the standard firm-level and governance control variables (CashHolding, Tangibility, Leverage, Firm_Size, Intangibles, Profitability, Loss, Capex, etc.) are included in the estimation as in previous tables but are not reported here. All specifications include firm and year-fixed effects. Significance levels at 1%, 5%, and 10% are denoted by ***, **, and * respectively.

	RESTATEMENT			
	Financial	FIN48	Out-of-Period	SAB108
Breach_Financial_lag1	1.453***	−0.329*	−0.207	0.083
	(0.351)	(0.193)	(0.325)	(0.072)
Breach_NotDisclosed_lag1	1.477***	−0.326*	−0.249	0.098
	(0.342)	(0.194)	(0.319)	(0.070)
Breach_Personal_lag1	1.377***	−0.271	−0.182	0.076
	(0.352)	(0.194)	(0.331)	(0.068)
Breach_Other_lag1	1.445***	−0.355*	−0.178	0.088
	(0.354)	(0.203)	(0.326)	(0.073)
Big_4	−0.012	0.047*	−0.037	0.002
	(0.026)	(0.027)	(0.023)	(0.006)
Breach_Fin_lag1 × Big_4	−0.021**	−0.063**	−0.075**	−0.010**
	(0.009)	(0.030)	(0.036)	(0.005)
Breach_NotDisc_lag1 × Big_4	−0.004	0.053	−0.078**	0.030
	(0.042)	(0.036)	(0.038)	(0.020)
Breach_Other_lag1 × Big_4	−0.078	0.063	0.023	−0.007
	(0.053)	(0.045)	(0.053)	(0.008)
Breach_Pers_lag1 × Big_4	0.013	0.009	−0.018	−0.004
	(0.028)	(0.019)	(0.035)	(0.005)
Ln_AUDIT_FEES	−0.019	0.006	−0.003	0.017*
	(0.043)	(0.027)	(0.042)	(0.010)
Ln_NON_AUDIT_FEES	−0.001	0.003	−0.001	−0.001
	(0.004)	(0.002)	(0.004)	(0.001)
Ln_TOTAL_FEES	0.001	−0.017	0.039	−0.023*
	(0.049)	(0.035)	(0.050)	(0.013)
Ln_BENEFITS_FEES	−0.002	0.003	−0.003	0.002
	(0.005)	(0.003)	(0.004)	(0.002)
Ln_IT_FEES	0.002	−0.003	0.0003	0.001
	(0.006)	(0.003)	(0.006)	(0.001)
Ln_TAX_FEES	0.001	−0.003	0.001	0.001**
	(0.003)	(0.002)	(0.003)	(0.001)
Other Controls	Yes	Yes	Yes	Yes
Firm and Year FE	Yes	Yes	Yes	Yes
Observations	40,793	40,793	40,793	40,793
Adjusted R^2	0.490	0.256	0.332	0.041

Table 9: Joint Effect of Cyber Breach and Restatement on Firm Value

This table reports OLS regression results examining the joint effect of lagged cybersecurity breaches and subsequent accounting restatements on firm value ($Ln\_Tobin'sQ$). The reference category for the cybersecurity variables is *Other Breach*. The interaction terms test the signaling dynamics of reporting corrections: whether specific restatements act as corrective signals that mitigate valuation penalties or compounding signals that reinforce systemic weakness. All models include firm-level and governance controls, as well as firm and year-fixed effects. Significance levels at 1%, 5%, and 10% are denoted by ***, **, and *, respectively.

	Ln_Tobins's Q			
	(1)	(2)	(3)	(4)
Breach_Financial_lag1	−1.453***	−1.393***	−1.300***	−1.299***
	(0.465)	(0.461)	(0.483)	(0.479)
Breach_NotDisclosed_lag1	−1.566***	−1.588***	−1.511***	−1.706***
	(0.460)	(0.467)	(0.478)	(0.501)
Breach_Personal_lag1	−1.506***	−1.376***	−1.507***	−1.121**
	(0.463)	(0.460)	(0.482)	(0.473)
Restate_Financial	−0.092			
	(0.096)			
Restate_FIN48		0.127		
		(0.097)		
Restate_OutOfPeriod			0.022	
			(0.112)	
Restate_SAB108				−0.321*
				(0.184)
Breach_Fin × Restate_Fin	0.294***			
	(0.097)			
Breach_NotDisc × Restate_Fin	0.189			
	(0.116)			
Breach_Pers × Restate_Fin	0.238**			
	(0.097)			
Breach_Fin × Restate_FIN48		−0.160		
		(0.103)		
Breach_NotDisc × Restate_FIN48		−0.136		
		(0.109)		
Breach_Pers × Restate_FIN48		−0.288***		
		(0.096)		
Breach_Fin × Restate_OOPA			−0.207*	
			(0.112)	
Breach_NotDisc × Restate_OOPA			−0.143	
			(0.151)	
Breach_Pers × Restate_OOPA			−0.020	
			(0.108)	
Breach_Fin × Restate_SAB108				0.147
				(0.272)
Breach_NotDisc × Restate_SAB108				0.385
				(0.260)
Breach_Pers × Restate_SAB108				−0.120
				(0.188)
Controls	Yes	Yes	Yes	Yes
Firm and Year FE	Yes	Yes	Yes	Yes
Observations	39,256	39,256	39,256	39,256
Adjusted R^2	0.440	0.438	0.338	0.338

Table 10: Audit Fees moderation of Cyber Breaches and Restatement Types

This table reports OLS regression model estimates examining the association between lagged cybersecurity breach information types and various types of restatement. Audit fee ratio is the ratio of audit fees to total fees (total fees include non-audit fees paid to auditors). The models include interactions between breach types and the audit fees to assess whether audit effort moderates post-breach reporting failures. The reference category for the cyber breach variables is *Other Breach*. All regressions include firm-level controls related to liquidity, leverage, investment, profitability, governance, and audit fees. Standard errors are clustered at the firm level. Statistical significance at the 1%, 5%, and 10% levels is denoted by ***, **, and *, respectively.

	RESTATEMENT TYPE			
	Financial	FIN48	Out-of-Period	SAB108
BREACH_Financial_lag1	1.417***	2.695***	0.403	1.125***
	(0.440)	(0.942)	(1.484)	(0.238)
BREACH_NotDisclosed_lag1	−1.007	1.706*	0.868	1.433***
	(1.653)	(1.001)	(1.779)	(0.336)
BREACH_Other_lag1	2.842*	3.054***	1.592	1.196***
	(1.548)	(0.903)	(1.630)	(0.194)
BREACH_Personal_lag1	−0.892	2.510***	0.231	1.151***
	(1.310)	(0.809)	(1.356)	(0.218)
Audit_Fees_Ratio	0.058	−1.437	1.631	−0.252
	(1.376)	(0.936)	(1.463)	(0.262)
BREACH_Financial_lag1 × Audit_Fees_Ratio	−2.462**	−0.428	−1.970*	−0.063
	(1.172)	(0.563)	(1.178)	(0.182)
BREACH_NotDisc_lag1 × Audit_Fees_Ratio	0.552	0.985	−1.238	−0.299
	(1.420)	(0.870)	(1.523)	(0.310)
BREACH_Personal_lag1 × Audit_Fees_Ratio	0.484	0.166	−0.623	−0.027
	(0.692)	(0.438)	(0.688)	(0.125)
Controls	Yes	Yes	Yes	Yes
Firm and Year FE	Yes	Yes	Yes	Yes
Observations	40,723	40,723	40,723	40,723
Adjusted R^2	0.562	0.303	0.400	0.480

Table 11: Cyber Breach Information Types, Severity, and Restatement Types

This table reports panel regression results examining the association between lagged cybersecurity breach information types and accounting restatement. Breach severity is proxied by the logarithm of the number of records lost, and interaction terms test whether severity moderates the effect of each breach type. The reference category for the cyber breach variables is *Other Breach*. Standard errors are clustered at the firm level. All specifications include firm and fiscal year fixed effects. Statistical significance at the 10%, 5%, 1%, and 0.1% levels is denoted by $^{+}$, *, **, and ***, respectively.

	RESTATEMENT TYPE			
	Financial	FIN48	Out-of-Period	SAB108
BREACH_Financial_lag1	0.033^{+}	−0.011	−0.001	−0.021
	(0.020)	(0.019)	(0.005)	(0.017)
BREACH_NotDisclosed_lag1	0.018	0.002	0.002	−0.022
	(0.017)	(0.016)	(0.005)	(0.017)
BREACH_Personal_lag1	0.012	0.012	0.000	−0.024
	(0.019)	(0.018)	(0.006)	(0.019)
Ln_NUMBER_OF_RECORDS_LOST_lag1	0.015*	0.000	0.000	−0.015
	(0.006)	(0.010)	(0.000)	(0.010)
BBREACH_Financial_lag1 × Ln_NUMBER_OF_RECORDS_LOST_lag1	−0.018**	0.004	0.000	0.014
	(0.006)	(0.010)	(0.002)	(0.010)
BREACH_NotDisclosed_lag1 × Ln_NUMBER_OF_RECORDS_LOST_lag1	−0.015*	0.002	−0.001	0.014
	(0.007)	(0.010)	(0.003)	(0.010)
BREACH_Personal_lag1 × Ln_NUMBER_OF_RECORDS_LOST_lag1	−0.013*	−0.002	0.000	0.015
	(0.007)	(0.010)	(0.001)	(0.011)
CashHolding	−0.002	0.001	0.001	0.000
	(0.002)	(0.002)	(0.001)	(0.000)
Tangibility	0.000	0.002	−0.002	0.000
	(0.002)	(0.002)	(0.001)	(0.001)
leverage	0.000	0.000	0.000	0.000
	(0.001)	(0.001)	(0.000)	(0.000)
Firm_Size	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Intangibles	−0.001	0.002	−0.002	0.000
	(0.001)	(0.002)	(0.001)	(0.000)
Profitability	0.000	0.001	−0.001	0.000
	(0.002)	(0.002)	(0.002)	(0.000)
Loss	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Capex	0.010*	−0.012**	0.003	−0.001
	(0.004)	(0.004)	(0.003)	(0.001)
Book_to_Market	0.000^{+}	0.000	0.000***	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Ln_NEmployee	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Sales_growth	−0.001	0.000	0.000	0.000
	(0.001)	(0.001)	(0.000)	(0.000)
AuditBoardCommittee	0.003	−0.001	−0.003*	0.001
	(0.002)	(0.002)	(0.001)	(0.001)
BoardSize	0.000	0.000	0.000	0.000***
	(0.000)	(0.000)	(0.000)	(0.000)
GenderDiversity	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
IndBoard	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Ln_AUDIT_FEES	0.001	0.000	−0.001*	0.000
	(0.001)	(0.001)	(0.001)	(0.000)
Ln_NON_AUDIT_FEES	0.000	0.000	0.000***	0.000^{+}
	(0.000)	(0.000)	(0.000)	(0.000)
Ln_TOTAL_FEES	−0.001	0.000	0.001^{+}	0.000
	(0.001)	(0.001)	(0.001)	(0.000)
Ln_BENEFITS_FEES	0.000	0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
Ln_IT_FEES	0.000	0.000	−0.001^{+}	0.000
	(0.000)	(0.001)	(0.000)	(0.000)
Ln_TAX_FEES	0.000	0.000	0.000*	0.000^{+}
	(0.000)	(0.000)	(0.000)	(0.000)
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
Observations	40,723	40,723	40,723	40,723
Adjusted R^2	0.384	0.342	0.397	0.359

Table A1: Variable Definitions

Variable	Definition
RESTATEMENT	Indicator variable equal to 1 if the firm issued an aggregate financial restatement in a given year, and 0 otherwise. Source: Audit Analytics.
Restate_Financial	Indicator variable equal to 1 if the restatement affects core financial accounts (revenue, assets, expenses), and 0 otherwise. Source: Audit Analytics.
Restate_FIN48	Indicator variable equal to 1 if the restatement relates to uncertain tax positions (FIN 48/ASC 740), and 0 otherwise. Source: Audit Analytics.
Restate_OutOfPeriod	Indicator variable equal to 1 for Out-of-Period Adjustments (OOPA), and 0 otherwise. Source: Audit Analytics.
Restate_SAB108	Indicator variable equal to 1 for misstatement quantification corrections under SEC SAB 108, and 0 otherwise. Source: Audit Analytics.
Breach_Financial	Indicator variable for breaches involving banking or credit data. Source: Audit Analytics.
Breach_Personal	Indicator variable for breaches involving personally identifiable information (PII). Source: Audit Analytics.
Breach_NotDisclosed	Indicator variable for breaches where the compromised data type was not specified. Source: Audit Analytics.
Breach_Other	Indicator variable for breaches involving intellectual property or internal records. Source: Audit Analytics.
Ln_N_RECORDS_LOST	Natural logarithm of the total number of records compromised in a breach. Source: Audit Analytics.
Ln_BREACH_COST	Natural logarithm of the total estimated cost associated with the breach. Source: Audit Analytics.
Most_Significant_Breach	Indicator equal to 1 if the breach involves financial or personal data (PII), and 0 otherwise. These categories represent the highest operational and legal risk.
High-Significance Restatement	Indicator equal to 1 if the restatement affects core financial accounts (e.g., revenue or assets), reflecting a breakdown in fundamental accounting processes.
Ln_Tobin's Q	Market value of assets (Price $\times$ Shares Outstanding) divided by book value of total assets, log-transformed. Source: Compustat.
Firm_Size	Natural logarithm of the book value of total assets. Source: Compustat.
Profitability (ROA)	Earnings before interest and taxes (EBIT) divided by total assets. Source: Compustat.
Loss	Indicator variable equal to 1 if income before extraordinary items is negative, and 0 otherwise. Source: Compustat.
Leverage	Total debt (short-term + long-term) divided by total assets. Source: Compustat.
Tangibility	Net property, plant, and equipment (PP&E) divided by total assets. Source: Compustat.
CashHolding	Cash and short-term investments divided by total assets. Source: Compustat.
Intangibles	Intangible assets divided by total assets. Source: Compustat.
Capex	Capital expenditures divided by total assets. Source: Compustat.
Book_to_Market	Ratio of the book value of equity to the market value of equity. Source: Compustat.
RandD_Expenses	Total Research and Development (R&D) expenditures. Source: Compustat.
Sales_growth	Percentage change in annual sales revenue from year $t-1$ to t. Source: Compustat.
Ln_NEmployee	Natural logarithm of the total number of employees. Source: Compustat.
Big_4	Indicator variable equal to 1 if the firm is audited by a Big 4 auditor, and 0 otherwise. Source: Audit Analytics.
Ln_AUDIT_FEES	Natural logarithm of total fees paid for the annual audit. Source: Audit Analytics.
Ln_NON_AUDIT_FEES	Natural logarithm of fees paid for all non-audit services. Source: Audit Analytics.
Ln_TOTAL_FEES	Natural logarithm of the sum of audit and non-audit fees. Source: Audit Analytics.
Ln_IT_FEES	Natural logarithm of fees paid for technology-related assurance. Source: Audit Analytics.
Ln_TAX_FEES	Natural logarithm of total tax-related service fees. Source: Audit Analytics.
Ln_AUDIT_RELATED_FEES	Natural logarithm of fees for assurance and related services. Source: Audit Analytics.
Ln_BENEFITS_FEES	Natural logarithm of fees paid for employee benefit plan audits. Source: Audit Analytics.
Ln_OTHER_FEES	Natural logarithm of all other fees paid to the auditor. Source: Audit Analytics.
BoardSize	Natural logarithm of the total number of directors. Source: LSEG Workspace.
IndBoard	Percentage of independent directors serving on the board. Source: LSEG Workspace.
GenderDiversity	Percentage of female directors serving on the board. Source: LSEG Workspace.
AuditBoardCommittee	Indicator variable for the presence of a standing audit committee. Source: LSEG Workspace.