# CORPORATE OWNERSHIP PRICE AND INSTITUTIONAL INVESTORS' LEVERAGE OF CYBERSECURITY INCIDENTS

Yasemin Zengin-Karaibrahimoglu [*], Laura Georg Schaffner [**]

[*] Faculty of Economics and Business, University of Groningen, Groningen, the Netherlands
[**] *Corresponding author,* EM Strasbourg Business School, University of Strasbourg, Strasbourg, France
Contact details: EM Strasbourg Business School, University of Strasbourg, HuManiS UR 7308, Strasbourg, France

OPEN ACCESS

**How to cite this paper:** Zengin-Karaibrahimoglu, Y., & Georg Schaffner, L. (2025). Corporate ownership price and institutional investors' leverage of cybersecurity incidents. *Corporate Ownership & Control, 22*(3), 138–152. https://doi.org/10.22495/cocv22i3art11

**ISSN Online:** 1810-3057
**ISSN Print:** 1727-9232

**Received:** 20.06.2025
**Revised:** 03.09.2025; 22.09.2025
**Accepted:** 08.10.2025

**JEL Classification:** D8, M42, O32
**DOI:** 10.22495/cocv22i3art11

## Abstract

Using a data breach incident at a Big Four audit firm, we examine whether companies pay a price for not securing their clients' data. Leveraging a sample of 1,737 firm-year observations of UK-listed firms audited by Big Four auditors during 2015–2019, we apply difference-in-difference (DiD) models to test whether clients of the breached company, as the audit service provider paid lower audit fees post-breach, particularly in the presence of large institutional shareholders. Our findings document that following a data breach, compared to other comparable non-breached companies, the breached company loses its premium for services, particularly for clients with large institutional shareholders. Given companies' dual societal and profit-generating functions, our results suggest that data breaches not only compromise a company's reputation in the capital markets but also erode the trust of their clients, especially in the presence of institutional investors. These findings underscore the economic consequences of data breaches and highlight the critical role of effective control execution in cybersecurity and stakeholder management, thereby preserving market confidence. Our study contributes to the literature by providing novel evidence on reputational spillovers in a non-US setting, highlighting how institutional ownership and service-based trust shape client responses to cybersecurity failures in credence-good industries.

**Keywords**: Corporate Ownership, Company Reputation, Institutional Investors, Cyber-Attacks, Data Breach, Cybersecurity Controls

**Authors' individual contribution**: Conceptualization — Y.Z.-K. and L.G.S.; Methodology — Y.Z.-K. and L.G.S.; Investigation — Y.Z.-K. and L.G.S.; Writing — Original Draft — Y.Z.-K. and L.G.S.; Writing — Review & Editing — Y.Z.-K. and L.G.S.

**Declaration of conflicting interests**: The Authors declare that there is no conflict of interest.

**Acknowledgements:** The Authors thank participants of the AIS, SET, and International Sections, the 45th EAA Conference, and the University of Strasbourg research seminar for valuable feedback. The Authors also thank Partha S. Mohapatra, California State University, and William L. Buslepp, Louisiana State University, for their initial work and ideas for this paper. The research support is provided by the University of Groningen and the University of Strasbourg.

## 1. INTRODUCTION

Cyber-attacks and data breaches have become major issues for businesses worldwide. Cybersecurity risks and resulting breaches are of "fundamental concern to organizations and public policy setters" (Bodin et al., 2018, p. 527). Regardless of the type of attack or the stolen information, data breaches impose substantial direct costs to companies (e.g., malfunctioning internal control systems, legal expenses, operational disruptions, communication costs with stakeholders) and indirect costs (e.g., reputational harm, impairment of brand value) on both businesses and the general public (Rodgers et al., 2019)[1]. The direct global average cost of a data breach in 2024 is $4.88 million, reflecting a 10% increase over the same period ending February 2023 and a 26.4% rise from 2018 (IBM Security, 2024). Given that corporate reputation is a critical intangible asset for competitiveness in the global marketplace (Sarstedt et al., 2013), the indirect costs of data breaches — particularly reputational harm — are considered significant.

Reputational harm might even surpass all other costs, especially for businesses operating in highly regulated industries or those whose stakeholders rely heavily on trust and confidentiality. Recent studies document that data breaches and the quality of control in cybersecurity disclosures are essential components of risk assessment across various sectors (Li et al., 2020; Rosati et al., 2022; Smith et al., 2019; Yen et al., 2018). Following data breaches, companies often face increased scrutiny, higher operational costs, and demands for transparency from stakeholders, which can impact their pricing strategies and market competitiveness (Rosati et al., 2022; Rosati et al., 2019). For instance, Calderon and Gao (2020) find that high-quality cyber risk disclosure is associated with lower costs of capital, suggesting that companies price effective security management into their stakeholder relationships. These studies enhance our understanding of how companies integrate cybersecurity considerations into their corporate governance in response to both internal and client-related incidents.

However, an unanswered question remains in the literature: whether, and under what conditions, companies bear the consequences for cybersecurity incidents. In their recent study using US data from 2014 to 2019, Litt et al. (2023) find that companies experiencing data breach incidents may charge lower fees to clients affected by the breach. While their findings document post-breach client-company relationships in the primary market, they do not address the spillover reputational impact on clients not directly affected by the data breach or the contextual factors that may accelerate a company's response in terms of reduced service fees. Our study aims to fill this void by examining whether corporate owners face consequences for failing to secure the confidentiality of their clients' data and whether contextual factors, such as corporate ownership type in the form of the presence of institutional shareholders, contribute to heightened pressure on companies to assume this responsibility.

Data breaches threaten not only the businesses subject to cyber-attacks but also their stakeholders — including clients, customers, suppliers, and investors. For example, professional standards mandate that audit firms, as service-providing companies, maintain the confidentiality of client information and adopt reasonable procedures to safeguard it (Public Company Accounting Oversight Board [PCAOB], 2004, paragraph 01). Therefore, any damage associated with the companies' reputation not only affects their operations but also has severe impacts on their clients and capital market participants. Companies often charge a premium based on their reputation for providing high-quality products or services (DeFond & Zhang, 2014; Francis, 1984; Palmrose, 1986); thus, any loss of reputation can negatively impact their pricing power and revenues (Boone et al., 2015).

Utilizing the data breach incident that Deloitte, a major consulting and auditing company, experienced in 2017 and a sample of 1,737 firm-year observations from the London Stock Exchange (LSE) between 2015 and 2019, this study addresses two central research questions:

*RQ1: Do companies pay a price for failing to secure their clients' data?*

*RQ2: Is this price incrementally higher when the affected clients have large institutional shareholders in their ownership structure?*

Supporting the reputation hypothesis, our difference-in-difference (DiD) analyses document that following the data breach, a reputation-damaging event, the breached company experienced incrementally lower service fees relative to other non-breached companies. Fees for the breached company's clients, and consequently total revenues from its services, declined by 4%. Our results suggest that, due to potential loss in trust and reputation, to maintain their business relations with their clients, the breached company offers a premium discount to their clients, not necessarily impairing audit service efforts. In other words, given the reputation loss, the breached company is likely to provide a higher or similar level of service quality, with strong efforts, but at a lower price. A considerable impact on its revenue.

Furthermore, our results document that for the breached company, the decrease in service fees depends on its clients' ownership structure and is larger if the client has large and sophisticated institutional shareholders. Our findings remain robust and consistent across alternative pre-post analysis windows (e.g., [-1, +1]), while controlling for variables such as company tenure and client characteristics, incorporating additional controls related to corporate governance structures, independence, and expertise, and considering the influence of foreign shareholding and strategic shareholding.

Our study contributes to the literature in several ways. First, our findings complement those on post-breach reputational damage experienced by companies and adverse market responses by their clients, focusing on different institutional environments (Litt et al., 2023). We provide evidence of the effect of such a data breach in cases where clients were not directly affected but were impacted by the firm's reputation loss. Given that the UK's shareholder-centric corporate governance model places strong emphasis on the role of institutional investors by fostering a different dynamic in client-company relationships compared to the U.S., where regulatory oversight often takes a more prominent role, we illuminate the potential influence of institutional environments on the dynamics of reputational harm following such incidents.

Second, our study extends the findings of Yen et al. (2018) and Rosati et al. (2022), who stated that service fees are higher after the occurrence of

[1] Previous studies examining the economic consequences of data breaches for publicly traded firms document significant negative stock market reactions following news of a data breach (Campbell et al., 2003; Bolster et al., 2010). Other studies show an impact on firms' future performance (e.g., return on assets, future sales, dividends, etc.) (Ko & Dorantes, 2006; Kamiya et al., 2018; Tosun, 2021). A more detailed literature review on market reaction to business data breaches can be found in Richardson et al. (2019).

an information security breach at the client level. Our findings show that this claim is valid only if the breach occurs at the client level. In the case of a data breach at the company level, clients consider the potential impairment of their signal to market participants and are less inclined to pay an additional fee premium. The damage to a company's reputation is likely due to the nature of its services. Since the output of certain services is a credence good where clients are unable to assess the quality even after purchase, it is the lack of they base decisions on trust in the service provider, auditor (Causholli & Knechel, 2012). When trust is compromised, clients may become reluctant to pay a premium. This examination is essential to exercise control among investors because companies in such industries have a unique role by serving dual functions, the societal and profit-generating. Any damage to their reputation may impair not only their business value but also the trust of all their clients, leading to severe consequences in the markets. Given that literature on corporate governance in the supply of service quality and company reputation risk is limited, DeFond and Zhang (2014) stress that reputation incentives have strong theoretical support and intuitive appeal but require empirical validation. Our study empirically supports arguments that clients are willing to pay a price for good service quality. Unlike prior studies that focus on breaches at the client level (Yen et al., 2018; Rosati et al., 2022), we show that when the breach occurs at the service provider level, particularly in credence-good industries like auditing, clients may respond by withholding fee premiums, driven by concerns over reputational contagion.

Third, our findings highlight the importance of large and sophisticated shareholders for businesses from a market perspective. Large institutional shareholders play an important corporate governance role by being not only effective monitoring mechanisms but also significant players affecting strategic management decisions, including the procurement of services (Mitra et al., 2007). Therefore, institutional investors may prevent firms from indirect reputational damages, potentially harmful to those engaging with breached companies, and provide management with an advantage in negotiations with service providers.

Furthermore, we respond to calls by DeFond and Zhang (2014) for empirical work on reputation incentives by providing evidence that reputation-based trust is a key driver in client decision-making under uncertainty. Our findings extend Litt et al. (2023) by illustrating how the institutional context, in our case, the UK's shareholder-centric governance system, amplifies the role of large institutional investors in influencing client behavior. This comparative angle adds to the cross-jurisdictional understanding of reputational dynamics, contrasting with U.S.-centric studies that emphasize regulatory oversight.

Finally, by highlighting the disciplining effect of institutional investors, our study contributes to the growing body of work on the role of ownership structure in shaping firms' responses to reputational threats (Mitra et al., 2007). The evidence that clients with high institutional ownership are more sensitive to breaches at the service company level emphasizes the governance function of sophisticated shareholders in enforcing higher standards of data security and corporate conduct. The presence of institutional investors intensifies the pressure on companies to exercise control over the high standards of data security and transparency, reinforcing the critical role of corporate governance structures in mitigating reputational risks.

## 2. INSTITUTIONAL AND THEORETICAL BACKGROUND

### 2.1. Background: The Deloitte data breach

On September 25, 2017, the Guardian reported that Deloitte had suffered a massive security breach, and the emails of its clients had been compromised. The breach reportedly occurred during Deloitte's email migration and upgrade from an on-site system to Microsoft's cloud software: Office 365 (Schwartz, 2017). The hacker accessed the firm's global email server through an "administrator's account", which did not follow the standard security practice of two-factor authentication. All divisions of Deloitte, including audit, tax, and consulting clients, had material in the company email system that was breached. It is estimated that five million emails could have been accessed by hackers, including plans and designs from across all industries, like pharmaceutical companies, media enterprises, banks, as well as government agencies (Mak, 2017). Hackers had potential access to emails sent and received by 244,000 Deloitte employees (Hopkins, 2017b). Thus, Deloitte failed in its fiduciary duty to place appropriate controls to mitigate the risk of a security breach, and the data breach was essentially an assurance failure.

While the attack occurred between November 2016 and March 2017, the data breach was not publicly disclosed until September 2017. The security breach generated criticisms because Deloitte provides clients advice on how to manage the risks posed by sophisticated cybersecurity attacks in addition to providing auditing and tax services. In fact, Deloitte was ranked the best security consultant in the world in 2012 (Gartner, 2012). While Deloitte initially claimed that the security lapse had only impacted six clients, later reports suggested that the server contained the emails of an estimated 350 clients, including four US government departments, the United Nations, and some of the world's biggest multinationals (Hopkins, 2017a). Deloitte also stated that the firm had been able to establish "precisely what information was at risk". However, internal sources stated that "The hackers had free rein in the network for a long time and nobody knows the amount of the data taken" (Hopkins, 2017b). While Deloitte's data breach is defined more as an operational failure, not directly associated with audit engagements, it puts many large businesses, audited by Deloitte, at risk. This raises an important question: Was Deloitte's reputation compromised by the breach, and if so, what is the price of such a reputation event for Deloitte?

### 2.2. Corporate reputation and service fees: Consequences of data breaches

Corporate reputation is a strategic asset that enhances trust among clients, investors, and other stakeholders. When compromised, it can lead to significant financial and governance challenges, particularly for companies in trust-sensitive industries (Johnson et al., 2014). For instance, reputation allows companies to command premium fees for their services; however, a data breach undermines this advantage by diminishing client confidence and increasing perceived risks (DeAngelo, 1981; Litt et al., 2023).

In industries where services are often credence goods, such as auditing, consulting, or technology, clients rely on reputation as a proxy for quality. Following a data breach, clients may reassess their trust in the company's ability to deliver secure, high-quality services, leading to renegotiations of fees or termination of relationships (Causholli & Knechel, 2012). This dynamic reflects the broader market's reassessment of the company's perceived risk profile and reputation.

The reputation hypothesis suggests that reputational damage directly influences a company's economic outcomes. For instance, firms may face decreased service fees for their services as clients leverage their reduced trust to negotiate better terms. At the same time, they may incur additional costs to restore trust in their controls, such as investing in stronger cybersecurity measures or offering concessions to retain clients. These financial consequences underscore the governance implications for corporate owners of controlling the reputational integrity in a competitive market. This leads to our first research question: whether companies pay a price for not securing their clients' data.

Addressing this question allows us to investigate whether data breaches result in measurable economic consequences, such as reduced service fees, and explore how governance mechanisms, such as stakeholder oversight and control, mitigate or exacerbate these impacts for corporate owners.

### 2.3. The role of institutional investors

Institutional investors are critical actors in corporate governance, serving as both monitors and enforcers of accountability (Majocchi et al., 2013). By holding significant ownership stakes, these investors influence management decisions and ensure alignment with shareholder interests (Baghdadi et al., 2018; Kempf et al., 2017). Their role is particularly pronounced in the aftermath of reputational crises, such as data breaches, where their influence can shape a company's response and recovery strategy.

Institutional investors bring a higher degree of sophistication and vigilance compared to other shareholders, allowing them to monitor and influence key decisions. For example, they can demand stricter cybersecurity measures, advocate for transparency, and negotiate better terms for services in response to reputational damage (Tee et al., 2017) and they can influence management's accounting policy choices, by actively monitoring them (Bushee, 1998; Chung et al., 2002; Mitra et al., 2007; Mitra & Hossain, 2007). The shareholder monitoring mechanism suggests that institutional shareholders, holding a substantial stake in a business, have an economic incentive to monitor the management (Rajgopal & Venkatachalam, 1997). Prior research suggests that institutional ownership improves financial reporting quality, curbs earnings manipulation, and reduces the likelihood of negative outcomes, such as qualified audit reports or diminished investor trust (Rajgopal & Venkatachalam, 1997; Pucheta-Martínez & García-Meca, 2014). Institutional investors are not only sophisticated users of accounting information, but also capable monitors who influence corporate behavior through both explicit governance mechanisms and implicit market-based signals (Kao, 2007). Their monitoring role often extends to strategic decision-making, especially when ownership stakes are sufficiently large to incentivize shareholder activism (Gillan & Starks, 2000). These investors enhance the information environment by demanding timely, accurate, and specific financial disclosures (Ajinkya et al., 2005) and are better positioned than retail investors to detect earnings management (Chung et al., 2002). As a result, firms with strong institutional oversight tend to exhibit higher earnings quality (Mitra & Cready, 2005).

Large institutional shareholders, by virtue of their significant ownership in firms, have both the incentives and power to influence strategic decisions and monitor the activities of the management (Shleifer & Vishny, 1986). Given the significance of their investment by holding a large supply of shares, large institutional shareholders have power against the management because of their 1) legitimate controlling right to have effective control over businesses' operations, and 2) potential direct influence on the share prices of the business via potential bulk selling/buying of the shares on capital markets. Consequently, large institutional investors may influence management's decision regarding the purchase of the audit services using their voting rights and power on the share prices. Empirical evidence shows that institutional blockholder ownership is associated with lower audit fees, consistent with the view that effective monitoring reduces auditors' perceived engagement risk (Mitra et al., 2007). Similarly, Yang et al. (2021) find that when institutional investors are distracted, thus unable to exercise effective oversight, auditors respond by increasing audit fees, reflecting heightened audit risk. Furthermore, auditors are more likely to act independently and prioritize reputation protection when clients are closely monitored by institutional investors, particularly due to the greater perceived threat of litigation in such environments (Velury et al., 2003; Kane & Velury, 2004). Therefore, institutional investors not only improve reporting outcomes but also shape auditor incentives and pricing through their governance influence, information processing capacity, and role in mitigating agency conflicts.

Specifically, after data breaches, institutional shareholders are likely to be concerned about their service-providing company's ability to maintain the IT security within their own firm, as they have high institutional investments. They would be wary of the breached company's competence to sign off on the internal controls for financial reporting, given the fact that the breached company itself could not maintain the IT controls. This decrease in confidence in the breached company may potentially lead large institutional shareholders to use their negotiation power with management to purchase the services from another company. Consequently, the presence of large institutional shareholders may drive the breached company to decrease its service fee premium to keep its current clients. Thus, we suggest that relative to other clients of the breached company, clients with large institutional shareholders are likely to have lower service fees following the data breach. This leads to our second research question: whether companies face incrementally higher financial and reputational consequences for failing to secure client data when their clients have large institutional shareholders in their ownership structure.

## 3. SAMPLE AND RESEARCH DESIGN

### 3.1. Sample

To test our research questions, we use the data breach incident at a Big Four audit firm, as a service providing company. We started our sample selection, including all publicly listed firms on the LSE with available data on the Worldscope database over the period 2015–2019, using an event window of two years around the data breach. In order to test the direct reputation effect of the audit firm in the post-breach period, we chose a sample outside of the US market where clients were not directly impacted by the incident. Our initial sample was 9,810 firm-year observations from 1,964 firms. We eliminated 1,815 firm-year observations because of missing audit firm names. In the second step, we identified firms audited by the Big Four auditors and eliminated 3,050 firm-year observations containing non-Big Four auditors. We further collected data for institutional ownership and all other financial and non-financial (ownership and corporate governance) data from Thomson Reuters EIKON, Worldscope, and Asset4 databases. After eliminating firms with missing data for audit fees (1,064 firm-year observations) and any of the independent and control variables (1,862 firm-year observations), we have a final sample of 1,737 firm-year observations from 421 firms. Table 1 shows our sample selection.

**Table 1.** Sample selection

| *Sample* | *Firms* | *Firm-year observations* |
|---|---|---|
| All companies listed on the LSE between 2015–2019 are available on Thomson Reuters Datastream | 1,964 | 9,810 |
| Firm-year observations with | | |
| (-) Missing audit firm name | | (1,815) |
| (-) Audited by non-Big Four audit firms | | (3,050) |
| (-) Missing audit fee | | (1,346) |
| (-) Missing client-specific firm controls | | (1,862) |
| **Final sample** | **421** | **1,737** |

### 3.2. Empirical models

To examine *RQ1*, we test whether breached companies' clients, relative to clients of other companies, pay incrementally lower audit fees in the year following the data breach. We employ the following difference-in-difference (DiD) model, a modified model of Gutierrez et al. (2018).

$$\begin{gathered}Ln(AuditFee)_t = \beta_0 + \beta_1 Post + \beta_2 Breached\_AF + \beta_3 Post \times Breached\_AF + \\ \beta_4 Client\text{-}specific\ firm\text{-}level\ controls + (Industry\ and\ Year\ indications) + \varepsilon\end{gathered} \qquad (1)$$

where *ln(AuditFee)$_t$* is the natural logarithm of the audit fee paid by the client for the auditing of the financial statements in year *t*. *Post* is an indicator variable that equals 1 for the years 2018 and 2019 and 0 otherwise. In the DiD model, in Eq. (1), we have a treatment sample (UK-listed firms audited by Deloitte) and a control sample (UK-listed firms audited by other Big Four audit firms). Therefore, in Eq. (1), *Breached_AF* is an indicator variable that equals 1 if a firm's financial statements were audited by Deloitte in year *t*, 0 if it is audited by other Big Four audit firms (PricewaterhouseCoopers, Ernst&Young, and KPMG).

In all the empirical models, we control for client-specific firm-level controls. We use *Ln(TotalAssets)* to control for firm size; *ROA* and *Loss* to control for firm performance and identify the companies with negative performance; *MTB* to control for market capitalization and growth opportunities; *Leverage* to control for potential agency cost and financial risk; *CFO*, *Rec*, *Inv*, *SaleVol*, and *Foreign*, to capture the complexity of the audit engagement task, *CG* to control for the quality of corporate governance in the firm[2], *CrossListed* to control for the potential confounding impact of being subject to multiple stock exchange regulations, and *Concentrated_Own* to control for the ownership concentration of the business. Table A.1 in the Appendix defines all variables used in our analyses.

In Eq. (1), our variable of interest is the coefficient of *Post × Breached_AF*, which indicates the difference between the change in audit fees from pre- to post-data breach for breached Big Four audit firm's clients (treatment firms) relative to other Big Four clients (control firms) in the UK. The change in audit fees following the data breach, with $\beta_3 < 0$, indicates an incrementally lower audit fee due to reputation damage following the data breach.

To examine *RQ2*, we use the following DiD model:

[2] Clients' corporate governance quality is an important determinant for auditors in their risk assessment (Bedard & Johnstone, 2004; Cohen et al., 2002). From a risk-view perspective, previous studies show that firms with a weak corporate governance structure have higher audit fees (Bedard & Johnstone, 2004) because auditors perceive the client as riskier due to the lack of strong monitoring and control mechanisms. In contrast, some other studies argued that from a demand perspective, clients with strong corporate governance mechanisms are likely to have higher audit fees, because of demand for higher quality audit services (Carcello et al., 2002). Or alternatively, a strong corporate governance structure may substitute the demand for high-quality external services and consequently, clients with a strong corporate governance structure are more likely to have lower audit fees (Tsui et al., 2001). Although previous studies do not have a consensus regarding the direction of the relation between corporate governance and audit fees, it is well accepted that clients' corporate governance structure is a significant determinant of audit fees (Hay et al., 2006; Hay, 2013). Thus, in all our analyses, we control for the client's corporate governance quality.

$$Ln(AuditFee)_t = \beta_0 + \beta_1 Post + \beta_2 Breached\_AF + \beta_3 ln\big(InstitutionalOwn(\%)\big) + \beta_4 Post \times Breached\_AF + \beta_5 ln\big(InstitutionalOwn(\%)\big) \times Breached\_AF + \beta_6 Post \times ln\big(InstitutionalOwn(\%)\big) + \beta_7 Post \times Breached\_AF \times \ln\big(InstitutionalOwn(\%)\big) + \beta_8 Client\text{-}specific\ firm\text{-}level\ controls + (Industry\ and\ Year\ indications) + \varepsilon \tag{2}$$

where *ln(InstitutionalOwn(%))* is an indicator variable that equals 1 if the percentage of shares held by investment firms is higher than 20%; 0 otherwise. We use a threshold of 20% shareholding because International Accounting Standards (IAS) 28 (International Financial Reporting Standards [IFRS], 2025) states that shareholding greater than 20% is considered a significant influence of investors over the decision-making of the investees and reflects the power of the investors in the financial and operating policies of the invested firms.

In Eq. (2), our variable of interest is the coefficient of *Post × Breached_AF × ln(InstitutionalOwn(%))*, which indicates the difference between the change in audit fees from pre- to post-data breach for breached Big Four audit firm's clients with large institutional shareholders relative to other breached Big Four audit firm's clients. The change in audit fees following the data breach, with $\beta_7 < 0$, indicates an incrementally lower audit fee for the clients due to the leverage of large institutional shareholders.

Finally, we control for the potential impact of industry and year on the audit fees by including industry and year indicators. To mitigate the potential undue influence of extreme values, we winsorize all continuous variables at the 1% and 99% levels. In all our estimations, we use Huber/White/sandwich standard error estimates two-way clustered by the auditor and by the company to correct potential heteroskedasticity and within-cluster correlation.

## 4. RESULTS

### 4.1. Summary statistics

Tables 2a and 2b present the descriptive statistics for our sample. The median audit fee in our sample is £1.097 million. Audit fees paid by breached Big Four audit firm's clients in both pre- and post the data breach are higher than other Big Four. Audit fees in the pre-data breach period summed up to approximately £1.34 million (median audit fees of £1.26 million). On average (median), audit fees paid by breached Big Four audit firm's clients decreased by £130 thousand (£100 thousand) following the data breach. The change in average audit fees presented in Table 2b represents the difference without controlling for other firm-specific characteristics. However, in our regression analysis, after controlling for firm characteristics, the unexplained part of the audit fee — audit fee premium — change is incrementally larger for the breached company's clients. Further, the breached Big Four audit firm's clients constitute 27% of our sample. *InstitutionalOwn(%)* has a mean value of 12%.

Table 3 presents the Pearson correlations. The correlation coefficients ensure that multicollinearity among independent variables is not a severe problem for the variables since the correlation coefficients do not exceed 0.50 for most of the variables. There is a strong correlation between *Ln(TotalAssets)* and *Ln(AuditFee)*. Further, we also test the multicollinearity based on the variance inflation factor (VIF). According to the tolerance values, VIF is 1.46, indicating that multicollinearity is not a concern for our analyses. We used the "vif" command in STATA after running our regression to check for multicollinearity. As a rule of thumb, a variable with VIF values greater than 10 indicates a potential multicollinearity issue. We consider the tolerance values (1/VIF) to check the degree of collinearity. A tolerance value lower than 0.1 is comparable to a VIF of 10.

**Table 2a.** Summary statistics: Full sample (N = 1,737)

| *Variables* | *Mean* | *Std. Dev.* | *p25* | *Median* | *p75* |
|---|---|---|---|---|---|
| *Ln(AuditFee)* | 7.028 | 1.561 | 6.087 | 7.001 | 7.952 |
| *Post* | 0.431 | 0.495 | 0 | 0 | 1 |
| *Breached_AF* | 0.27 | 0.444 | 0 | 0 | 1 |
| *InstitutionalOwn* | 0.119 | 0.323 | 0 | 0 | 0 |
| *Ln(TotalAssets)* | 14.795 | 1.571 | 13.777 | 14.535 | 15.673 |
| *ROA* | 0.057 | 0.106 | 0.022 | 0.055 | 0.098 |
| *Loss* | 0.143 | 0.351 | 0 | 0 | 0 |
| *MTB* | 3.11 | 3.556 | 1.03 | 1.91 | 3.72 |
| *Leverage* | 78.069 | 125.49 | 9.62 | 41.9 | 89.69 |
| *CFO* | 0.098 | 0.159 | 0.036 | 0.082 | 0.128 |
| *Rec* | 0.123 | 0.143 | 0.025 | 0.083 | 0.168 |
| *Inv* | 0.082 | 0.145 | 0 | 0.022 | 0.104 |
| *SaleVol* | 0.105 | 0.114 | 0.039 | 0.072 | 0.129 |
| *Foreign* | 0.697 | 0.46 | 0 | 1 | 1 |
| *CG* | 3.834 | 0.619 | 3.569 | 4.016 | 4.276 |
| *CrossListed* | 0.149 | 0.356 | 0 | 0 | 0 |
| *Concentrated_Own* | 1.975 | 1.332 | 0.751 | 1.735 | 3.255 |

*Note: All variables are described in Table A.1 in the Appendix.*

**Table 2b.** Summary statistics: Pre-post and breached Big Four audit firm versus other Big Four audit firms

| *Breached Big Four* | *Pre (N = 278)* | | | | | *Post (N = 191)* | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Variables*** | ***Mean*** | ***Std. Dev.*** | ***p25*** | ***p50*** | ***p75*** | ***Mean*** | ***Std. Dev.*** | ***p25*** | ***p50*** | ***p75*** |
| *Ln(AuditFee)* | 7.197 | 1.525 | 6.405 | 7.142 | 7.909 | 7.094 | 1.461 | 6.14 | 7.059 | 7.861 |
| *InstitutionalOwn* | 0.129 | 0.336 | 0 | 0 | 0 | 0.126 | 0.332 | 0 | 0 | 0 |
| *Ln(TotalAssets)* | 14.978 | 1.433 | 14.003 | 14.61 | 15.678 | 14.838 | 10.532 | 13.89 | 14.611 | 15.839 |
| *ROA* | 0.057 | 0.078 | 0.025 | 0.054 | 0.089 | 0.039 | 0.103 | 0.019 | 0.044 | 0.089 |
| *Loss* | 0.133 | 0.34 | 0 | 0 | 0 | 0.157 | 0.365 | 0 | 0 | 0 |
| *MTB* | 2.789 | 3.159 | 0.97 | 1.835 | 3.55 | 2.337 | 2.342 | 1.03 | 1.53 | 3.13 |
| *Leverage* | 81.302 | 121.034 | 10.16 | 52.655 | 96.98 | 74.746 | 117.207 | 11.85 | 48.19 | 81.41 |
| *CFO* | 0.081 | 0.09 | 0.034 | 0.069 | 0.11 | 0.076 | 0.069 | 0.034 | 0.071 | 0.113 |
| *Rec* | 0.118 | 0.145 | 0.023 | 0.084 | 0.161 | 0.114 | 0.135 | 0.027 | 0.08 | 0.164 |
| *Inv* | 0.079 | 0.133 | 0 | 0.018 | 0.108 | 0.076 | 0.131 | 0 | 0.013 | 0.1 |
| *SaleVol* | 0.088 | 0.072 | 0.035 | 0.076 | 0.131 | 0.088 | 0.072 | 0.035 | 0.073 | 0.126 |
| *Foreign* | 0.716 | 0.452 | 0 | 1 | 1 | 0.702 | 0.459 | 0 | 1 | 1 |
| *CG* | 3.826 | 0.554 | 3.546 | 3.983 | 4.25 | 3.948 | 0.52 | 3.687 | 4.07 | 4.329 |
| *CrossListed* | 0.198 | 0.399 | 0 | 0 | 0 | 0.199 | 0.4 | 0 | 0 | 0 |
| *Concentrated_Own* | 1.843 | 1.325 | 0.698 | 1.485 | 2.971 | 1.909 | 1.34 | 0.708 | 1.535 | 3.114 |
| ***Other Big Four*** | ***Pre (N = 711)*** | | | | | ***Post (N = 557)*** | | | | |
| ***Variables*** | ***Mean*** | ***Std. Dev.*** | ***p25*** | ***p50*** | ***p75*** | ***Mean*** | ***Std. Dev.*** | ***p25*** | ***p50*** | ***p75*** |
| *Ln(AuditFee)* | 7.047 | 1.596 | 6.075 | 7.024 | 8.122 | 6.897 | 1.56 | 5.961 | 6.813 | 7.905 |
| *InstitutionalOwn* | 0.11 | 0.313 | 0 | 0 | 0 | 0.122 | 0.328 | 0 | 0 | 0 |
| *Ln(TotalAssets)* | 14.852 | 1.616 | 13.778 | 14.608 | 15.728 | 14.615 | 1.58 | 13.486 | 14.399 | 15.497 |
| *ROA* | 0.063 | 0.108 | 0.024 | 0.06 | 0.108 | 0.054 | 0.114 | 0.02 | 0.051 | 0.097 |
| *Loss* | 0.138 | 0.345 | 0 | 0 | 0 | 0.151 | 0.358 | 0 | 0 | 0 |
| *MTB* | 3.412 | 3.88 | 1.05 | 2.15 | 4.04 | 3.15 | 3.611 | 1.03 | 1.89 | 3.68 |
| *Leverage* | 79.526 | 133.619 | 9.48 | 41.73 | 89.86 | 75.735 | 119.833 | 8.89 | 34.99 | 90.76 |
| *CFO* | 0.107 | 0.182 | 0.037 | 0.084 | 0.133 | 0.104 | 0.175 | 0.036 | 0.087 | 0.135 |
| *Rec* | 0.123 | 0.138 | 0.025 | 0.084 | 0.171 | 0.129 | 0.151 | 0.025 | 0.082 | 0.172 |
| *Inv* | 0.087 | 0.154 | 0 | 0.025 | 0.109 | 0.079 | 0.144 | 0 | 0.021 | 0.099 |
| *SaleVol* | 0.105 | 0.112 | 0.039 | 0.069 | 0.126 | 0.117 | 0.14 | 0.041 | 0.073 | 0.132 |
| *Foreign* | 0.699 | 0.459 | 0 | 1 | 1 | 0.684 | 0.465 | 0 | 1 | 1 |
| *CG* | 3.821 | 0.651 | 3.548 | 4.025 | 4.281 | 3.815 | 0.638 | 3.55 | 4.007 | 4.269 |
| *CrossListed* | 0.142 | 0.349 | 0 | 0 | 0 | 0.115 | 0.319 | 0 | 0 | 0 |
| *Concentrated_Own* | 1.993 | 1.339 | 0.742 | 1.773 | 3.287 | 2.04 | 1.322 | 0.829 | 1.833 | 3.276 |

**Table 3.** Correlation matrix

| ***Variables*** | ***(1)*** | ***(2)*** | ***(3)*** | ***(4)*** | ***(5)*** | ***(6)*** | ***(7)*** | ***(8)*** | ***(9)*** | ***(10)*** | ***(11)*** | ***(12)*** | ***(13)*** | ***(14)*** | ***(15)*** | ***(16)*** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ***(1) Ln(AuditFee)*** | 1.00 | | | | | | | | | | | | | | | |
| ***(2) Post*** | **-0.04** | 1.00 | | | | | | | | | | | | | | |
| ***(3) Breached_AF*** | **0.05** | -0.03 | 1.00 | | | | | | | | | | | | | |
| ***(4) InstitutionalOwn*** | **-0.18** | 0.01 | 0.02 | 1.00 | | | | | | | | | | | | |
| ***(5) Ln(TotalAssets)*** | **0.68** | **-0.07** | **0.05** | **-0.19** | 1.00 | | | | | | | | | | | |
| ***(6) ROA*** | **-0.13** | **-0.05** | **-0.04** | **-0.06** | **-0.06** | 1.00 | | | | | | | | | | |
| ***(7) Loss*** | 0.00 | 0.02 | 0.00 | **0.08** | **-0.09** | **-0.61** | 1.00 | | | | | | | | | |
| ***(8) MTB*** | **0.12** | **-0.04** | **-0.09** | **0.04** | **-0.12** | **0.28** | **-0.08** | 1.00 | | | | | | | | |
| ***(9) Leverage*** | **0.27** | -0.02 | 0.00 | 0.00 | **0.24** | **-0.12** | **0.08** | **0.31** | 1.00 | | | | | | | |
| ***(10) CFO*** | -0.02 | -0.01 | **-0.07** | **0.07** | **-0.20** | **0.38** | **-0.17** | **0.45** | -0.02 | 1.00 | | | | | | |
| ***(11) Rec*** | **0.16** | 0.01 | -0.03 | **0.06** | **-0.20** | **0.08** | -0.04 | **0.28** | **0.05** | **0.19** | 1.00 | | | | | |
| ***(12) Inv*** | **-0.04** | -0.02 | -0.02 | **-0.04** | **-0.04** | **0.07** | **-0.07** | 0.03 | **-0.09** | **0.06** | -0.03 | 1.00 | | | | |
| ***(13) SaleVol*** | 0.01 | 0.04 | **-0.09** | **0.11** | **-0.24** | 0.02 | **0.09** | **0.26** | 0.01 | **0.26** | **0.23** | 0.03 | 1.00 | | | |
| ***(14) Foreign*** | **0.52** | -0.02 | 0.02 | -0.04 | **0.15** | **-0.07** | -0.01 | **0.15** | **0.10** | **0.10** | **0.20** | **-0.10** | **0.12** | 1.00 | | |
| ***(15) CG*** | **0.47** | 0.02 | **0.04** | **-0.08** | **0.26** | **-0.06** | -0.01 | **0.10** | **0.15** | **0.10** | **0.18** | **0.13** | **-0.05** | **0.29** | 1.00 | |
| ***(16) CrossListed*** | **0.35** | -0.03 | **0.09** | **-0.07** | **0.39** | **-0.07** | 0.00 | -0.01 | **0.11** | **-0.05** | **-0.08** | **-0.05** | -0.03 | **0.13** | **0.08** | 1.00 |
| ***(17) Concentrated_Own*** | **-0.07** | 0.02 | **-0.05** | **-0.05** | **-0.20** | **-0.09** | **0.09** | 0.02 | -0.02 | -0.01 | 0.04 | 0.04 | **0.13** | 0.02 | **-0.09** | 0.03 |

## 4.2. Results of the pre-post analysis (RQ1)

Table 4, Model 1 presents the on-average change in audit fees for all firms between the pre- and post-data breach periods. We find that the coefficient of *Post* is insignificant, indicating that, on average, there is no impact of the data breach on the average audit fees paid by the clients in the UK.

Table 4, Model 2 presents the estimation results for our *RQ1*, which assesses the average change in audit fees between the pre-and post-data breach periods for breached Big Four audit firm's clients relative to clients of other Big Four audit firms. We find that the coefficient of the interaction term, *Post × Breached_AF*, is negative and significant ($\beta$ = -0.052, p < 0.05). These findings indicate that relative to other Big Four audit firms' clients, the incremental decrease in audit fees of breached clients is approximately 4%. Since we use the natural logarithm of the dependent variable, audit fees, we compute the percentage change in the dependent variable, 4.05%, as ($e^x$-1), where e is 2.71828 and x is -0.052, the coefficient for *Post × Breached_AF* in Table 4, Model 2. Our results indicate that, due to the diminishing reputation, owners of the breached company pay a price for not securing their clients' data, and they potentially offer a discount on their premium to retain their existing relations with clients.

**Table 4.** Pre-post analysis results

| ***DV: lnAuditFee*** | ***Model 1*** | ***Model 2*** |
|---|---|---|
| ***Post*** | 0.038 | **0.055*****
|  | (1.593) | **(2.823)** |
| ***Breached_AF*** |  | **0.151***** |
|  |  | **(2.778)** |
| ***Post × Breached_AF*** |  | **-0.052**** |
|  |  | **(-2.276)** |
| *Ln(TotalAssets)* | 0.639*** | 0.641*** |
|  | (20.497) | (19.542) |
| *ROA* | -0.642*** | -0.627*** |
|  | (-5.877) | (-6.149) |
| *Loss* | 0.079** | 0.081** |
|  | (2.077) | (2.184) |
| *MTB* | 0.027*** | 0.028*** |
|  | (3.373) | (3.307) |
| *Leverage* | 0.000 | 0.000 |
|  | (0.110) | (0.127) |
| *CFO* | -0.016 | -0.005 |
|  | (-0.055) | (-0.018) |
| *Rec* | 1.623*** | 1.611*** |
|  | (4.570) | (4.542) |
| *Inv* | -0.548 | -0.540 |
|  | (-1.446) | (-1.428) |
| *SaleVol* | 0.554* | 0.580* |
|  | (1.758) | (1.766) |
| *Foreign* | 0.848*** | 0.842*** |
|  | (16.662) | (15.620) |
| *CG* | 0.253*** | 0.248*** |
|  | (5.757) | (5.432) |
| *CrossListed* | 0.172*** | 0.155** |
|  | (3.190) | (2.520) |
| *Concentrated_Own* | 0.021 | 0.023 |
|  | (0.790) | (0.914) |
| Constant | -4.025*** | -4.080*** |
|  | (-7.774) | (-7.269) |
| Observations | 1,737 | 1,737 |
| R-squared | 0.769 | 0.770 |
| Industry fixed-effect | Yes | Yes |
| Year fixed-effect | Yes | Yes |

*Note: ***, **, and * denote the significance level at 1%, 5%, and 10%. T-values are presented in parentheses. All variables are described in Table A.1 in the Appendix.*

### 4.3. Role of the institutional shareholders (RQ2)

Table 5, Model 1 presents estimation results for Eq. (2), which assesses the average change in audit fees for the breached audit firm's clients with high institutional shareholding between the pre-and post-data breach periods. The coefficient for the interaction term, *Post × Breached_AF x ln(InstitutionalOwn(%))*, is negative and significant ($\beta$ = -0.208, $p < 0.01$). The evidence suggests that relative to the pre-period, in the post-period, on average, the decrease in audit fees is incrementally larger for breached Big Four audit firm clients with large institutional shareholders compared to other breached audit firms' clients. In other words, the breached audit firm is offering an incrementally higher discount in audit fees if the client has a large institutional shareholder. Our results show that the presence of large institutional shareholders in the ownership structure may influence the strategic decisions of businesses and retain their existing relations with providers.

We further estimate Eq. (1) after partitioning the sample into 1) low, which includes clients with less than 20% institutional shareholding, and 2) high, which includes clients with equal to or more than 20% institutional shareholding[3]. The coefficient of *Post × Breached_AF* is negative and significant in Model 2, for clients with large institutional shareholders. Overall, these findings indicate limited evidence that the incremental decrease in the audit fees in the post-data breach is concentrated among those clients where institutional shareholders are powerful in strategic decision-making. This is consistent with prior evidence that institutional blockholder ownership is negatively associated with audit fees due to reduced audit risk (Mitra et al., 2007) and that effective institutional monitoring mitigates perceived audit risk, leading to lower audit fees (Yang et al., 2021).

[3] To check the robustness of our analysis, we partitioned the sample using an alternative proxy. We compared the strategic (insider) shareholding, foreign shareholding, and institutional shareholding of the firm and created a dummy variable that takes the value of 1 if the institutional shareholding represents the largest shareholding of the group, and 0 otherwise. Our results are statistically similar to the results presented in Table 5, Model 2, and Model 3. Untabulated results show that the coefficient for *Post + Post x Breached_AF* is only significant for the clients with large institutional shareholders.

**Table 5.** The institutional shareholders' role

| *DV: lnAuditFee* | *Model 1* | *Model 2* | *Model 3* |
|---|---|---|---|
| ***Post*** | **0.030**** | **0.225***** | **-0.101***** |
| | **(2.439)** | **(2.756)** | **(-3.376)** |
| ***Breached_AF*** | **0.138**** | **0.501***** | **0.140**** |
| | **(2.161)** | **(3.303)** | **(2.281)** |
| ***Post × Breached_AF*** | -0.029 | **-0.366***** | -0.032 |
| | (-1.059) | **(-5.044)** | (-1.165) |
| ***InstitutionalOwn*** | **-0.355***** | | |
| | **(-4.960)** | | |
| ***Post × InstitutionalOwn*** | **0.174***** | | |
| | **(4.151)** | | |
| ***Breached_AF × InstitutionalOwn*** | **0.164***** | | |
| | **(2.818)** | | |
| ***Post × Breached_AF × InstitutionalOwn*** | **-0.208***** | | |
| | **(-3.306)** | | |
| *Ln(TotalAssets)* | 0.631*** | 0.436*** | 0.636*** |
| | (18.984) | (4.413) | (23.479) |
| *ROA* | -0.704*** | 0.396 | -0.811*** |
| | (-5.143) | (0.770) | (-2.870) |
| *Loss* | 0.090** | 0.249 | 0.056 |
| | (2.238) | (1.552) | (0.821) |
| *MTB* | 0.028*** | -0.034** | 0.035*** |
| | (3.796) | (-2.577) | (5.038) |
| *Leverage* | 0.000 | 0.001*** | -0.000 |
| | (0.221) | (3.143) | (-0.274) |
| *CFO* | 0.033 | 0.042 | 0.316 |
| | (0.115) | (0.231) | (0.632) |
| *Rec* | 1.605*** | 1.416*** | 1.634*** |
| | (4.199) | (7.030) | (3.527) |
| *Inv* | -0.561 | -0.086 | -0.541 |
| | (-1.489) | (-0.186) | (-1.474) |
| *SaleVol* | 0.623* | 0.531** | 0.637* |
| | (1.951) | (2.372) | (1.827) |
| *Foreign* | 0.836*** | 0.628*** | 0.857*** |
| | (16.272) | (4.420) | (12.974) |
| *CG* | 0.246*** | 0.223** | 0.264*** |
| | (5.353) | (2.012) | (4.582) |
| *CrossListed* | 0.154** | -0.654 | 0.209*** |
| | (2.423) | (-1.088) | (3.316) |
| *Concentrated_Own* | 0.017 | 0.056 | 0.016 |
| | (0.667) | (0.498) | (0.539) |
| Constant | -3.879*** | -2.135 | -4.436*** |
| | (-6.978) | (-1.343) | (-8.152) |
| Observations | 1,737 | 206 | 1,531 |
| R-squared | 0.773 | 0.769 | 0.775 |
| Industry fixed-effect | Yes | Yes | Yes |
| Year fixed-effect | Yes | Yes | Yes |

*Note: ***, **, and * denote the significance level at 1%, 5%, and 10%. T-values are presented in parentheses. All variables are described in Table A.1 in the Appendix.*

## 4.4. Additional analyses

### *4.4.1. Alternative windows for the pre-post analysis — [-1, +1]*

In our main analysis, we use an event window of two years around the data breach. We repeat our pre-post analysis to test *RQ1* using a one-year window around the data breach. Untabulated results are consistent with our main results presented in Table 4.

### *4.4.2. Controlling for audit firm tenure and audit opinion*

In our main analyses, we do not control for audit firm tenure and auditor opinion. The association between audit firm tenure, audit opinion, and audit fees is controversial. A qualified audit opinion is a sign of associated risk and issues experienced by the auditors and, consequently, may have consequences on the audit pricing. Similarly, although inconclusive, prior studies argue that due to the "Lowball" effect, audit firms offer a lower fee to attract a new audit client, and therefore, the audit price might be lower at the beginning of the auditor's tenure (Cho et al., 2021). Independent of the underlying reason for the decrease in audit fees, prior literature states that auditor tenure is an important determinant of audit fees (Hay et al., 2006).

To test the sensitivity of our results to the auditor, we repeat our main analyses using audit opinion and auditor tenure. Table 6, Model 1, and Model 3 present our main results after controlling for audit firm tenure and audit opinion. In both models, while the coefficient of audit firm tenure is positive and significant at 1%, the coefficient of audit opinion is insignificant. In line with our results presented in Table 4, Table 6 shows that our variable of interest, *Post × Breached_AF*, remains negative and significant after controlling for audit firm tenure and audit opinion.

### *4.4.3. Controlling for audit committee characteristics*

Abbott et al. (2003) and Carcello et al. (2002) suggest that audit committee (AC) members, who are independent and possess financial expertise, are better able to understand the auditing issues, risks, and the audit procedures proposed to address these issues and risks. Both studies find that audit committee independence and expertise are positively associated with audit fees. Further, Krishnan (2005) finds that companies with independent audit committees and audit committees with financial expertise are less likely to have internal control problems. The findings of previous studies are debatable, but clear that the client's AC structure is also an important element in the determination of the audit fees. We, therefore, controlled our main analysis for AC characteristics, AC independence, and AC expertise. The results presented in Table 6, Model 2, and Model 3 are consistent with our main results presented in Table 4.

**Table 6.** *RQ1* — After controlling for audit firm tenure, audit opinion, and AC characteristics

| ***DV: lnAuditFee*** | ***Model 1*** | ***Model 2*** | ***Model 3*** |
|---|---|---|---|
| ***Post*** | **-0.121***** | -0.039 | **-0.093***** |
| | **(-4.805)** | (-1.561) | **(-3.259)** |
| ***Breached_AF*** | **0.126**** | **0.169***** | **0.144***** |
| | **(2.448)** | **(3.147)** | **(2.889)** |
| ***Post × Breached_AF*** | **-0.034*** | **-0.052**** | **-0.035**** |
| | **(-1.887)** | **(-2.443)** | **(-2.090)** |
| *Ln(TotalAssets)* | 0.633*** | 0.629*** | 0.621*** |
| | (20.724) | (18.229) | (18.809) |
| *ROA* | -0.619*** | -0.584*** | -0.574*** |
| | (-4.832) | (-5.490) | (-4.491) |
| *Loss* | 0.071* | 0.085*** | 0.076** |
| | (1.903) | (2.599) | (2.411) |
| *MTB* | 0.029*** | 0.030*** | 0.031*** |
| | (3.613) | (3.628) | (4.207) |
| *Leverage* | 0.000 | 0.000 | 0.000 |
| | (0.108) | (0.177) | (0.152) |
| *CFO* | -0.035 | -0.033 | -0.061 |
| | (-0.122) | (-0.109) | (-0.209) |
| *Rec* | 1.581*** | 1.566*** | 1.537*** |
| | (4.640) | (4.256) | (4.369) |
| *Inv* | -0.583 | -0.560 | -0.604 |
| | (-1.300) | (-1.371) | (-1.250) |
| *SaleVol* | 0.567* | 0.554* | 0.537* |
| | (1.891) | (1.820) | (1.896) |
| *Foreign* | 0.834*** | 0.822*** | 0.814*** |
| | (20.900) | (19.119) | (26.157) |
| *CG* | 0.292*** | 0.324*** | 0.367*** |
| | (5.551) | (8.428) | (8.319) |
| *CrossListed* | 0.133** | 0.101* | 0.075 |
| | (2.300) | (1.962) | (1.524) |
| *Concentrated_Own* | 0.021 | 0.008 | 0.005 |
| | (0.799) | (0.291) | (0.213) |
| ***AuditOpinion*** | 0.207** | | 0.214** |
| | (2.190) | | (2.392) |
| ***ln(AuditorTenure)*** | 0.103*** | | 0.102*** |
| | (2.731) | | (2.920) |
| ***ln(ACIndependence)*** | | -0.167*** | -0.171*** |
| | | (-4.012) | (-4.434) |
| ***ACExpertise*** | | -0.120 | -0.099 |
| | | (-0.476) | (-0.317) |
| Constant | -4.568*** | -3.657*** | -3.345*** |
| | (-9.067) | (-6.218) | (-4.650) |
| Observations | 1,653 | 1,723 | 1,639 |
| R-squared | 0.774 | 0.767 | 0.772 |
| Industry fixed-effect | Yes | Yes | Yes |
| Year fixed-effect | Yes | Yes | Yes |

*Note: ***, **, and * denote the significance level at 1%, 5%, and 10%. T-values are presented in parentheses. AuditOpinion is an indicator variable that equals 1 if the auditor disclosed a qualified audit opinion in year t; 0 otherwise (Worldscope WC07546). ln(AuditorTenure) is the natural logarithm of the number of years after which the company rotates its statutory auditor (Asset4 ECSLDP061). ln(ACIndependence) is the percentage of independent board members on the audit committee as stipulated by the company (Asset4 CGBFO01V). ACExpertise is an indicator variable that equals 1 if the company has an audit committee with at least one "financial expert" in year t; 0 otherwise (asset 4 CGBFO03V). All other variables are described in Table A.1 in the Appendix.*

### *4.4.4. Controlling for foreign shareholding and strategic shareholding*

The audit fee is not only dependent on the quality of the corporate governance structure but also on the type and magnitude of agency conflicts between the principal and agent (Barroso et al., 2018). In *RQ2*, we claim that the decrease in audit fees of breached companies' clients is larger for firms with higher institutional shareholding. However, previous literature also documents that other types of ownership have a significant association with audit fees (Barroso et al., 2018; Desender et al., 2013; Gotti et al., 2012; Gul & Tsui, 2001; Mitra et al., 2007; Niemi, 2005; Nikkinen & Sahlström, 2004). In case of a data breach, we assume that besides the institutional shareholders, two types of individual shareholders will have strong incentives: 1) foreign shareholders and 2) strategic shareholders. We expect that foreign shareholdings and strategic shareholding by employees and family members bring additional monitoring incentives. We, therefore, controlled our analysis for *RQ2* for foreign shareholding, *ForeignOwn*, and strategic shareholding, *StrategicOwn*. The results presented in Table 7 are consistent with our main results presented in Table 5.

**Table 7.** *RQ2* — After controlling for foreign and strategic ownership

| *DV: lnAuditFee* | *Model 1* | *Model 2* | *Model 3* |
|---|---|---|---|
| ***Post*** | **0.030***** | **0.031**** | **0.031***** |
| | **(3.606)** | **(2.527)** | **(3.596)** |
| ***Breached_AF*** | **0.133**** | **0.143**** | **0.138**** |
| | **(2.055)** | **(2.406)** | **(2.292)** |
| ***Post × Breached_AF*** | -0.029 | -0.029 | -0.029 |
| | (-1.091) | (-1.076) | (-1.104) |
| ***InstitutionalOwn*** | **-0.385***** | **-0.356***** | **-0.385***** |
| | **(-5.150)** | **(-4.778)** | **(-4.986)** |
| ***Post × InstitutionalOwn*** | **0.175***** | **0.160***** | **0.162***** |
| | **(3.893)** | **(4.264)** | **(4.023)** |
| ***Breached_AF × InstitutionalOwn*** | **0.171***** | **0.161***** | **0.168***** |
| | **(2.703)** | **(2.763)** | **(2.664)** |
| ***Post × Breached_AF × InstitutionalOwn*** | **-0.206***** | **-0.201***** | **-0.199***** |
| | **(-3.095)** | **(-3.212)** | **(-3.024)** |
| *Ln(TotalAssets)* | 0.625*** | 0.627*** | 0.621*** |
| | (17.955) | (17.115) | (16.492) |
| *ROA* | -0.676*** | -0.678*** | -0.653*** |
| | (-4.721) | (-5.200) | (-4.707) |
| *Loss* | 0.089** | 0.091** | 0.090** |
| | (2.197) | (2.376) | (2.312) |
| *MTB* | 0.027*** | 0.029*** | 0.028*** |
| | (3.634) | (4.229) | (4.081) |
| *Leverage* | 0.000 | 0.000 | 0.000 |
| | (0.315) | (0.315) | (0.405) |
| *CFO* | 0.027 | 0.017 | 0.013 |
| | (0.096) | (0.062) | (0.046) |
| *Rec* | 1.644*** | 1.623*** | 1.658*** |
| | (4.374) | (4.327) | (4.481) |
| *Inv* | -0.551 | -0.544 | -0.535 |
| | (-1.511) | (-1.510) | (-1.537) |
| *SaleVol* | 0.572* | 0.641** | 0.591* |
| | (1.753) | (2.078) | (1.861) |
| *Foreign* | 0.828*** | 0.832*** | 0.825*** |
| | (15.685) | (17.290) | (16.643) |
| *CG* | 0.239*** | 0.252*** | 0.245*** |
| | (5.508) | (5.127) | (5.219) |
| *CrossListed* | 0.167** | 0.155** | 0.167** |
| | (2.499) | (2.189) | (2.293) |
| *Concentrated_Own* | 0.008 | 0.035 | 0.026 |
| | (0.331) | (0.806) | (0.590) |
| ***ForeignOwn*** | 0.032*** | | 0.031*** |
| | (3.612) | | (3.931) |
| ***StrategicOwn*** | | -0.036 | -0.034 |
| | | (-0.914) | (-0.851) |
| Constant | -3.767*** | -3.841*** | -3.737*** |
| | (-6.574) | (-6.777) | (-6.463) |
| Observations | 1,737 | 1,737 | 1,737 |
| R-squared | 0.774 | 0.773 | 0.774 |
| Industry fixed-effect | Yes | Yes | Yes |
| Year fixed-effect | Yes | Yes | Yes |

*Note: ***, **, and * denote the significance level at 1%, 5%, and 10%. T-values are presented in parentheses. ForeignOwn is the log of the percentage of shares held by investment companies (Datastream NOSHFR). StrategicOwn is the log of the percentage of shares held by strategic owners, families, and employees (Datastream NOSHEM). All other variables are described in Table A.1 in the Appendix.*

## 5. DISCUSSION

Our findings indicate significant insights into the reputational and financial implications of cybersecurity incidents by highlighting the unique dynamics that occur when a service-providing company, an audit firm, rather than a client, experiences a breach. While much prior research has emphasized how client-level breaches lead to higher assurance costs as auditors respond with additional procedures and risk premiums, our evidence points to a contrasting mechanism in the market. Specifically, when the service-providing company itself suffers a data breach, its ability to command fee premiums is diminished, as clients perceive reputational damage and reduced trustworthiness. This dynamic underscores the dual nature of reputational capital in professional services: it not only enables firms to justify premium pricing when intact, but it can also erode quickly when client confidence is undermined.

The concentration of fee reductions among clients with significant institutional ownership further demonstrates how governance structures shape market responses to reputational shocks. Institutional investors, with both the resources and incentives to protect shareholder interests, appear to use their influence to renegotiate or resist premium audit pricing in the aftermath of the breach. This finding aligns with the broader view of institutional investors as active monitors who exert discipline on firms' strategic decisions, extending this role into the domain of service contracting. In the UK's shareholder-centric environment, this monitoring function is particularly salient, suggesting that reputational consequences of service-provider breaches may be amplified in governance systems where ownership is concentrated and shareholder voices carry substantial weight.

Taken together, these results emphasize that reputational damage is not simply a symbolic cost but has tangible contractual and financial implications for companies. They suggest that service-providing companies operate under heightened vulnerability when their credibility as custodians of client information is compromised, potentially eroding one of their key competitive advantages: Trust. Moreover, the findings reveal that clients are not passive in this process. Rather, they actively leverage reputational shocks to alter bargaining dynamics, leading to a redistribution of economic rents in service relationships.

Finally, the robustness of the results across alternative specifications and controls strengthens confidence in the central conclusion that Deloitte's breach materially altered its fee structures. Importantly, the observed effects are distinct from broader ownership and governance variables that often influence audit pricing, suggesting a direct reputational channel. By documenting this, the study highlights the importance of cybersecurity not only for protecting client data but also for safeguarding the economic value of reputational capital in the company's market. This insight carries implications beyond the audit profession, pointing to the need for all service providers in reputation-sensitive industries to recognize that a single breach can reshape client perceptions and contractual outcomes in lasting ways.

## 6. CONCLUSION

Businesses face an omnipresent threat of data security, and while many studies have addressed the economic impact of breaches, our research spotlights the loss of control of the companies' reputation and its ownership structure in shaping these outcomes.

This paper makes three main contributions to the literature. First, it extends prior research on reputational damage from data breaches by showing that when a breach occurs at the service-provider level, clients respond differently than in cases of client-level breaches: rather than paying higher fees, they demand discounts, indicating reputational spillovers in credence-good industries. Second, the study contributes to corporate governance literature by empirically supporting theoretical arguments that reputation incentives drive client decision-making (DeFond & Zhang, 2014), demonstrating that reputational trust is a key determinant of pricing in professional services. Third, the study highlights the role of institutional ownership in amplifying reputational consequences, showing that large shareholders strengthen client bargaining positions and thus influence how reputation loss translates into economic outcomes.

Despite these contributions, the study has several limitations that provide fertile ground for future research. First, our analysis is restricted to Deloitte's UK clients, where extensive media coverage may have magnified reputational consequences. Future work could extend this analysis to other jurisdictions with different media and regulatory environments, allowing for stronger cross-country comparisons. Second, our setting focuses specifically on breaches of confidentiality; subsequent studies should investigate whether breaches of availability or integrity (e.g., ransomware attacks disrupting business continuity (Javers, 2021)) generate distinct reputational or pricing effects. Third, while our quantitative evidence highlights the disciplining role of institutional shareholders, future research could employ qualitative methods, including interviews with institutional investors, boards, and audit committees, to better understand the mechanisms behind shareholder influence in breach settings. Finally, the unique fee transparency of the audit industry enabled our analysis, but future studies should extend this inquiry to other professional service sectors (e.g., law, consulting, IT outsourcing), where trust and reputation also play a central role but fee structures are less transparent.

Taken together, our study underscores the broader societal and market relevance of cybersecurity and reputation management. It highlights the need for firms, particularly in credence-good industries, to strengthen internal controls and transparency, as reputational damage not only undermines immediate revenue streams but also reshapes long-term client and shareholder relationships.

## REFERENCES

Abbott, L. J., Parker, S., Peters, G. F., & Raghunandan, K. (2003). The association between audit committee characteristics and audit fees. *Auditing: A Journal of Practice & Theory, 22*(2), 17–32. https://doi.org/10.2308/aud.2003.22.2.17

Ajinkya, B., Bhojraj, S., & Sengupta, P. (2005). The association between outside directors, institutional investors and the properties of management earnings forecasts. *Journal of Accounting Research, 43*(3), 343–376. https://doi.org/10.1111/j.1475-679x.2005.00174.x

Baghdadi, G. A., Bhatti, I. M., Nguyen, L. H. G., & Podolski, E. J. (2018). Skill or effort? Institutional ownership and managerial efficiency. *Journal of Banking & Finance, 91*, 19–33. https://doi.org/10.1016/j.jbankfin.2018.04.002

Barroso, R., Ben Ali, C., & Lesage, C. (2018). Blockholders' ownership and audit fees: The impact of the corporate governance model. *European Accounting Review, 27*(1), 149–172. https://doi.org/10.1080/09638180.2016.1243483

Bedard, J. C., & Johnstone, K. M. (2004). Earnings manipulation risk, corporate governance risk, and auditors' planning and pricing decisions. *The Accounting Review, 79*(2), 277–304. https://doi.org/10.2308/accr.2004.79.2.277

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy, 37*(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Bolster, P., Pantalone, C. H., & Trahan, E. A. (2010). Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis, 5*(1), 1–13. https://doi.org/10.2202/1932-9156.1081

Boone, J. P., Khurana, I. K., & Raman, K. K. (2015). Did the 2007 PCAOB disciplinary order against Deloitte impose actual costs on the firm or improve its audit quality? *The Accounting Review, 90*(2), 405–441. https://doi.org/10.2308/accr-50867

Bushee, B. J. (1998). The influence of institutional investors on myopic R&D investment behavior. *The Accounting Review*, 305–333. https://ssrn.com/abstract=143834

Calderon, T. G., & Gao, L. (2020). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing, 25*(1), 24–39. https://doi.org/10.1111/ijau.12209

Campbell, K., Gordon, L. A., Loeb, M. P., & 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. https://doi.org/10.3233/JCS-2003-11308

Carcello, J. V., Hermanson, D. R., Neal, T. L., & Riley, R. A., Jr. (2002). Board characteristics and audit fees. *Contemporary Accounting Research, 19*(3), 365–384. https://doi.org/10.1506/CHWK-GMQ0-MLKE-K03V

Causholli, M., & Knechel, W. R. (2012). An examination of the credence attributes of an audit. *Accounting Horizons, 26*(4), 631–656. https://doi.org/10.2308/acch-50265

Cho, M., Kwon, S. Y., & Krishnan, G. V. (2021). Audit fee lowballing: Determinants, recovery, and future audit quality. *Journal of Accounting and Public Policy, 40*(4), Article 106787. https://doi.org/10.1016/j.jaccpubpol.2020.106787

Chung, R., Firth, M., & Kim, J.-B. (2002). Institutional monitoring and opportunistic earnings management. *Journal of Corporate Finance, 8*(1), 29–48. https://doi.org/10.1016/S0929-1199(01)00039-6

Cohen, J., Krishnamoorthy, G., & Wright, A. M. (2002). Corporate governance and the audit process. *Contemporary Accounting Research, 19*(4), 573–594. https://doi.org/10.1506/983M-EPXG-4Y0R-J9YK

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

DeFond, M., & Zhang, J. (2014). A review of archival auditing research. *Journal of Accounting and Economics, 58*(2–3), 275–326. https://doi.org/10.1016/j.jacceco.2014.09.002

Desender, K. A., Aguilera, R. V., Crespi, R., & GarcÍa-Cestona, M. (2013). When does ownership matter? Board characteristics and behavior. *Strategic Management Journal, 34*(7), 823–842. https://doi.org/10.1002/smj.2046

Francis, J. R. (1984). The effect of audit firm size on audit prices: A study of the Australian market. *Journal of Accounting and Economics, 6*(2), 133–151. https://doi.org/10.1016/0165-4101(84)90010-7

Gartner. (2012, May 16). *Market share analysis: Security consulting, worldwide' 2012 report.* https://www.gartner.com/en/documents/2487218

Gillan, S. L., & Starks, L. T. (2000). Corporate governance proposals and shareholder activism: The role of institutional investors. *Journal of Financial Economics, 57*(2), 275–305. https://doi.org/10.1016/S0304-405X(00)00058-1

Gotti, G., Han, S., Higgs, J. L., & Kang, T. (2012). Managerial stock ownership, analyst coverage, and audit fee. *Journal of Accounting, Auditing & Finance, 27*(3), 412–437. https://doi.org/10.1177/0148558X11409158

Gul, F. A., & Tsui, J. S. L. (2001). Free cash flow, debt monitoring, and audit pricing: Further evidence on the role of director equity ownership. *Auditing: A Journal of Practice & Theory, 20*(2), 71–84. https://doi.org/10.2308/aud.2001.20.2.71

Gutierrez, E., Minutti-Meza, M., Tatum, K. W., & Vulcheva, M. (2018). Consequences of adopting an expanded auditor's report in the United Kingdom. *Review of Accounting Studies, 23*, 1543–1587. https://doi.org/10.1007/s11142-018-9464-0

Hay, D. (2013). Further evidence from meta-analysis of audit fee research. *International Journal of Auditing, 17*(2), 162–176. https://doi.org/10.1111/j.1099-1123.2012.00462.x

Hay, D. C., Knechel, W. R., & Wong, N. (2006). Audit fees: A meta-analysis of the effect of supply and demand attributes. *Contemporary Accounting Research, 23*(1), 141–191. https://doi.org/10.1506/4XR4-KT5V-E8CN-91GX

Hopkins, N. (2017a, September 25). *Deloitte hit by cyber-attack revealing clients' secret emails.* The Guardian. https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

Hopkins, N. (2017b, October 10). *Deloitte hack hit server containing emails from across US government.* The Guardian. https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government

IBM Security. (2024). *Cost of a data breach report 2024.* Ponemon Institute. https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Javers, E. (2021, August 11). *A hacker group using Lockbit Ransomware says they have hacked the consulting firm Accenture, CNBC* [Post]. X.com. https://x.com/EamonJavers/status/1425476619934838785

Johnson, W. C., Xie, W., & Yi, S. (2014). Corporate fraud and the value of reputations in the product market. *Journal of Corporate Finance, 25*, 16–39. https://doi.org/10.1016/j.jcorpfin.2013.10.005

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the impact of successful cyberattacks on target firms?* (NBER Working Paper No. 24409). National Bureau of Economic Research. https://doi.org/10.3386/w24409

Kane, G. D., & Velury, U. (2004). The role of institutional ownership in the market for auditing services: An empirical investigation. *Journal of Business Research, 57*(9), 976–983. https://doi.org/10.1016/S0148-2963(02)00499-X

Kao, L. (2007). Does investors' sophistication affect persistence and pricing of discretionary accruals? *Review of Pacific Basin Financial Markets and Policies, 10*(01), 33–50. https://doi.org/10.1142/S0219091507000945

Kempf, E., Manconi, A., & Spalt, O. (2017). Distracted shareholders and corporate actions. *The Review of Financial Studies, 30*(5), 1660–1695. https://doi.org/10.1093/rfs/hhw082

Ko, M., & Dorantes, A. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology and Management, 17*(2), 13–22. https://jitm.ubalt.edu/XVII-2/article2.pdf

Krishnan, J. (2005). Audit committee quality and internal control: An empirical analysis. *The Accounting Review, 80*(2), 649–675. https://doi.org/10.2308/accr.2005.80.2.649

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory, 39*(1), 151–171. https://doi.org/10.2308/ajpt-52593

Litt, B., Tanyi, P., & Weidenmier Watson, M. (2023). Cybersecurity breach at a Big 4 accounting firm: Effects on auditor reputation. *Journal of Information Systems, 37*(2), 77–100. https://doi.org/10.2308/ISYS-2022-006

Majocchi, A., Odorici, V., & Presutti, M. (2013). Corporate ownership and internationalization: The effects of family, bank, and institutional investor ownership in the UK and in continental Europe. *Corporate Ownership and Control, 10*(2–4), 721–732. https://doi.org/10.22495/cocv10i2c4art7

Mak, A. (2017, October 10). *Deloitte hack may have exposed data from major government agencies and companies.* Slate. https://slate.com/technology/2017/10/a-deloitte-security-breach-may-have-granted-hackers-access-to-government-and-corporate-emails.html

Mitra, S., & Cready, W. M. (2005). Institutional stock ownership, accrual management, and information environment. *Journal of Accounting, Auditing & Finance, 20*(3), 257–286. https://doi.org/10.1177/0148558X0502000304

Mitra, S., & Hossain, M. (2007). Ownership composition and non-audit service fees. *Journal of Business Research, 60*(4), 348–356. https://doi.org/10.1016/j.jbusres.2006.10.025

Mitra, S., Hossain, M., & Deis, D. R. (2007). The empirical relationship between ownership characteristics and audit fees. *Review of Quantitative Finance and Accounting, 28*(3), 257–285. https://doi.org/10.1007/s11156-006-0014-7

Niemi, L. (2005). Audit effort and fees under concentrated client ownership: Evidence from four international audit firms. *The International Journal of Accounting, 40*(4), 303–323. https://doi.org/10.1016/j.intacc.2005.09.006

Nikkinen, J., & Sahlström, P. (2004). Does agency theory provide a general framework for audit pricing? *International Journal of Auditing, 8*(3), 253–262. https://doi.org/10.1111/j.1099-1123.2004.00094.x

Palmrose, Z.-V. (1986). Audit fees and auditor size: Further evidence. *Journal of Accounting Research, 24*(1), 97–110. https://doi.org/10.2307/2490806

Public Company Accounting Oversight Board (PCAOB). (2004). *AU Section 9339. Audit Documentation: Auditing Interpretations of Section 339.* https://pcaobus.org/oversight/standards/archived-standards/details/AU9339B

Pucheta-Martínez, M. C., & García-Meca, E. (2014). Institutional investors on boards and audit committees and their effects on financial reporting quality. *Corporate Governance: An International Review, 22*(4), 347–363. https://doi.org/10.1111/corg.12070

Rajgopal, S., & Venkatachalam, M. (1997). *The role of institutional investors in corporate governance: An empirical investigation* (Working paper No. 1436). Stanford University. https://www.gsb.stanford.edu/faculty-research/working-papers/role-institutional-investors-corporate-governance-empirical

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems, 33*(3), 227–265. https://doi.org/10.2308/isys-52379

Rodgers, W., Alhendi, E., & Xie, F. (2019). The impact of foreignness on the compliance with cybersecurity controls. *Journal of World Business, 54*(6), Article 101012. https://doi.org/10.1016/j.jwb.2019.101012

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47*, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review, 31*(3), 701–728. https://doi.org/10.1080/09638180.2020.1856162

Sarstedt, M., Wilczynski, P., Melewar, T. C. (2013). Measuring reputation in global markets — A comparison of reputation measures? Convergent and criterion validities. *Journal of World Business, 48*(3), 329–339. https://doi.org/10.1016/j.jwb.2012.07.017

Schwartz, S. (2017, October 11). *Deloitte reportedly suffered hack during email migration to Office 365.* CIODIVE. https://www.ciodive.com/news/deloitte-hack-email-migration-microsoft-office-365/506946/

Shleifer, A., & Vishny, R. W. (1986). Large shareholders and corporate control. *Journal of Political Economy, 94*(3), 461–488. https://doi.org/10.1086/261385

Smith, T. J., Higgs, J. L., Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems, 33*(2), 177–204. https://doi.org/10.2308/isys-52241

Tee, M., Gul, F. A., Foo, Y. B., Teh, C. G. (2017). Institutional monitoring, political connections and audit fees: Evidence from Malaysian firms. *International Journal of Auditing, 21*(2), 164–176. https://doi.org/10.1111/ijau.12086

The International Financial Reporting Standards (IFRS). (2025). *IAS 28 Investments in Associates and Joint Ventures.* https://www.ifrs.org/issued-standards/list-of-standards/ias-28-investments-in-associates-and-joint-ventures/#about

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis, 76*, Article 101795. https://doi.org/10.1016/j.irfa.2021.101795

Tsui, J. S., Jaggi, B., & Gul, F. A. (2001). CEO domination, growth opportunities, and their impact on audit fees. *Journal of Accounting, Auditing & Finance, 16*(3), 189–208. https://doi.org/10.1177/0148558X0101600303

Velury, U., Reisch, J. T., & O'Reilly, D. M. (2003). Institutional ownership and the selection of industry specialist auditors. *Review of Quantitative Finance and Accounting, 21*(1), 35–48. https://doi.org/10.1023/A:1024855605207

Yang, J., Wu, H., & Yu, Y. (2021). Distracted institutional investors and audit risk. *Accounting & Finance, 61*(3), 3855–3881. https://doi.org/10.1111/acfi.12718

Yen, J.-C., Lim, J.-H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy, 37*(6), 489–507. https://doi.org/10.1016/j.jaccpubpol.2018.10.002

# APPENDIX

**Table A.1.** Variable definition

| *Variable* | *Definition* |
|---|---|
| *Ln(AuditFee)* | The natural logarithm of the auditor fees paid by the firm for the auditing of the financial statements in year *t* (Worldscope WC01801 in US dollars) |
| *Post* | An indicator variable equals 1 for the years 2018 and 2019 and 0 otherwise. |
| *Breached_AF* | An indicator variable that equals 1 if a firm's financial statements were audited by Deloitte in year *t*, 0 if it is audited by other Big Four audit firms (PricewaterhouseCoopers, Ernst & Young, and KPMG). |
| *InstitutionalOwn(20%)* | An indicator variable that equals 1 if the percentage of shares held by investment firms is higher than 20%; 0 otherwise. We computed the variables using the percentage of shares held by investment companies (Datastream NOSHIC). |
| *Ln(TotalAssets)* | The natural logarithm of the total assets at the end of year *t* (Worldscope WC02999 in US dollars). |
| *ROA* | The return on assets at the end of year *t* (Worldscope WC08326) |
| *Loss* | An indicator variable that equals 1 if the firm has a negative net profit in year *t*; 0 otherwise. |
| *MTB* | The market-to-book value of the firm at the end of year *t* (Worldscope WC09704) |
| *Leverage* | The total debt to total capital ratio at the end of year *t* (Worldscope WC03998) |
| *CFO* | Cash flows from operations divided by total assets at the end of year *t* (Worldscope WC04201/WC02999) |
| *Rec* | Receivables divided by total assets at the end of year *t* (Worldscope WC02051/WC02999) |
| *Inv* | Inventories divided by total assets at the end of year *t* (Worldscope WC02101/WC02999) |
| *SaleVol* | The standard deviation of total net sales divided by total assets for each firm at the end of year *t* (standard deviation of (Worldscope WC01001/WC02999) per firm) |
| *Foreign* | An indicator variable that equals 1 if the firm has foreign sales in year *t*; 0 otherwise. We computed the variables using total foreign sales (Worldscope WC08731). |
| *CG* | The natural logarithm of the corporate governance score of the company at the end of year *t*. It captures all systems and processes applied by the firm, which ensures that its board members and executives act in the best interests of its long-term shareholders (Asset4 CGVSCORE) |
| *CrossListed* | An indicator variable that equals 1 if a firm is cross-listed; 0 otherwise. |
| *Concentrated_Own* | The log of the percentage of shares held by insiders (Worldscope WC08021) |