The Effects of Cybersecurity Breach Disclosures on Analyst Forecast Measures

Abstract

This study examines the impact of cybersecurity breach disclosures on financial analysts' forecast outputs. Using a staggered difference-in-differences (DID) design with a propensity score–matched sample, we examine changes in analysts' earnings forecasts and stock recommendations for firms that disclose breach events. Our findings show that analysts revise earnings forecasts downward following breach disclosures, but do not significantly alter their stock recommendations. These results suggest that while analysts incorporate breach-related costs into earnings expectations, institutional frictions and behavioral biases may constrain their willingness to revise recommendations. The effects are robust to alternative specifications and placebo tests.

Keywords: Cybersecurity Breach, Financial Analysts, Earnings Forecasts and Recommendations

1. Introduction

Cybersecurity breach costs continue to escalate, with IBM Security reporting an average of $4.45 million per breach in 2023. Policymakers and investors increasingly emphasize the need for greater transparency around cybersecurity breach disclosures. In response, the Securities and Exchange Commission (SEC) has progressively advanced regulatory guidance. The 2011 framework underscored the importance of disclosing material incidents, while the 2018 update emphasized timely reporting. Most recently, on July 26, 2023, the SEC mandated new rules—effective September 5, 2023—requiring firms to disclose material cybersecurity incidents within four business days of confirming their materiality. These regulations aim to balance investor protection with managerial discretion over disclosure timing.

Despite regulatory efforts, breach disclosures remain a complex issue where firms maintain significant disclosure discretion, and this discretion creates tension. On one hand, voluntary disclosure can increase firm value and signal cybersecurity commitment (Gordon et al., 2010; Chen et al., 2023; Berkman et al., 2018); on the other hand, it may also lead to negative outcomes such as market value losses (Goel & Shawky, 2009; Amir et al., 2018) and heightened stock price crash risk (Cao et al., 2024). Consequently, managers face dilemmas in deciding whether, when, and how to disclose breach incidents. In addition, these disclosures can potentially cause financial damages by drawing investor attention due to the breach events. This complex trade-off raises an important question: how do market intermediaries, particularly financial analysts, interpret and respond to cybersecurity breach disclosures?

Analysts play a vital role in translating corporate information into valuation-relevant information for investors, especially in settings with high information asymmetry (Chen et al., 2010; Livnat & Zhang, 2012; Rubin et al., 2017). Although recent literature has examined how

cybersecurity events affect managers (Xu et al., 2019), auditors (Yen et al., 2018; Richardson et al., 2019; Rosati et al., 2022), lenders (Huang & Wang, 2021), short sellers (Wang et al., 2022), and customers (Janakiraman et al., 2018), less attention has been paid to how financial analysts respond in this context.

While Walton et al. (2021) originally highlighted this as a critical research gap, two recent studies, Chen et al. (2025) and Fleury and Salva (2025), have begun to explore analyst responses to breaches. However, our research focus differs substantially from theirs. Chen et al. (2025) find that breaches increase analyst forecast dispersion and reduce accuracy. Fleury and Salva (2025) show that cyberattacks primarily affect firm value through rising costs rather than reputational damage through analysts' revisions. In contrast, our study investigates whether analysts revise both earnings forecasts and stock recommendations after breach disclosures, and whether these responses are shaped by frictions in how analysts incorporate cybersecurity risks into firm valuations.

Moreover, while prior studies suggest that weak and minimal market reactions to breaches may explain firms' underinvestment in cybersecurity (Hilary et al., 2016; Richardson et al., 2019; Rosati et al., 2022), it remains unclear whether analysts, as informed market intermediaries, also underreact or remain indifferent in their outputs. Hence, we investigate this directly to assess whether analysts meaningfully reflect breach-related costs in their outputs. By focusing explicitly on analysts' forecast and recommendation behaviors, we offer a complementary yet distinct perspective that captures analysts' intermediation role in translating complex and technical disclosures into market signals.

Before testing this empirically, we first address a related question: Do analysts really *care* about cybersecurity breach disclosures? To explore this, we reviewed analyst call transcripts from firms that experienced breach incidents, such as the 2022 Optus data breach

and the 2021 T-Mobile cybersecurity breach. This initial analysis confirms that breach events are a focus point for analysts during the conference calls.[1]

To test our hypothesis, we construct a sample of 704 U.S. firms, comprising 352 breached firms and 352 matched non-breached peers. We observe analyst behaviors over a [-3, +3] year event window centered on the breach year (Kamiya et al., 2021). To address endogeneity and selection concerns, we apply a two-stage empirical strategy. First, we use propensity score matching (PSM) based on pre-breach firm characteristics. Second, we adopt a staggered difference-in-differences (DID) framework to estimate the causal effects of breach disclosures to account for the fact that breaches occur at different times across firms. By relying on the widely used PRC and Audit Analytics datasets, our results remain consistent and comparable with prior research in this field.

Our findings show that analysts significantly lower their earnings forecast estimates following breach disclosures. This suggests analysts do incorporate expected breach-related costs into their forecasts, supporting their role as information intermediaries (Chen et al., 2010; Livnat & Zhang, 2012). These downward revisions likely reflect adjustments for potential legal, operational, and reputational risks associated with breaches (Gordon et al., 2011).

However, we find no evidence that analysts revise their stock recommendations in response to breach disclosures, even when earnings estimates are downgraded. This finding holds even after performing a mediation analysis as a robustness check. We interpret this as

[1] Take the FH1 2023 earnings call transcript of Singapore Telecommunications (the parent company of Optus) as an example. During this call, financial analysts raised concerns regarding the 2022 Optus breach, which resulted in a significant loss of customer subscriptions as users switched to other service providers. This incident provides some evidence that due to the implicit effects from data breaches, analysts appear to put in more effort to understand the breach's consequences. It is a rational assumption that the associated costs such as loss of revenue and remediation, can significantly impact the earnings of breach firms, thus shaping analysts' assessments and predictions of breach firms. Similarly, in the T-Mobile 2022 Q2 earnings call, the CFO highlighted the financial impact on earnings of the 2021 cybersecurity breach, including a $350 million class action settlement and other expenses. These examples shed some light on the fact that analysts incorporate breach incident information in formulating their forecast estimates, as these costs are tied to the firm’s earnings.

evidence of "recommendation stickiness," consistent with prior research showing that analysts are reluctant to issue downgrades due to various factors such as personal opinions, reputational concerns, conflicts of interest, or career incentives (Bradshaw, 2004, 2011; Barniv et al., 2009; Bradley et al., 2017; Lin & McNichols, 1998; Groysberg et al., 2011; Beyer & Guttman, 2011; Barber et al., 2001). Additionally, analysts may strategically delay recommendation changes to avoid frequent revisions, as documented by Bernhardt et al. (2016). Compounding this, managers may strategically underreport or downplay the severity of breach incidents (Kothari et al., 2009; Amir et al., 2018), which can limit the information available to analysts and reduce the perceived need to adjust recommendations. Consistently, this may help explain why prior studies have found minimal investor reactions to breach events (Hilary et al., 2016; Richardson et al., 2019; Rosati et al., 2022).

To understand how these effects evolve, we divide the post-disclosure period into three subsequent years (Kamiya et al., 2021; Cao et al., 2024). This approach allows us to track how analysts' forecasts changed over time. Our analysis reveals that the impact of breach disclosures on analysts' forecasts is most pronounced in the first two years, with diminishing effects in the third year. The results present a very similar pattern to the effects of the 2018 SEC guidance, which appeared to have encouraged breach disclosures to peak in 2019, but the effects slowly diminished between 2020 and 2022.

We also examine the moderating role of the information environment, proxied by analyst coverage. High analyst coverage typically enhances the flow of information, reduces information asymmetry, and improves the overall quality of forecasts. Conversely, low analyst coverage often indicates an opaque information environment (Botosan, 1997; Healy & Palepu, 2001), where limited and unclear disclosures make it challenging for analysts to assess the full impact of events such as breaches. We find that firms with greater analyst coverage see a significant decrease in forecast estimates. This suggests that analysts incorporate the potential

damage from breaches more effectively when the information environments are more transparent. In contrast, firms with fewer analysts show no significant changes, indicating that opaque information environments make breach disclosures harder to evaluate. However, this does not indicate that information environment transparency is a disadvantage for firms, as we find no evidence of changes in analysts' recommendations. Instead, these results suggest that a more transparent information environment helps analysts better estimate the potential costs of breaches and improves the quality of analysts' forecasts, ultimately benefiting the investors.

Finally, we investigate how the information environment affects analyst forecast dispersion. We find that in a high information environment, breach disclosures reduce analyst dispersion, indicating improved information quality and decreased uncertainty. In contrast, there is no significant change in dispersion in a low information environment. These findings align with prior research, suggesting that greater transparency reduces forecast uncertainty. When uncertainty is high (the information environment is low), analysts are more likely to rely on their private information rather than public information, such as breach disclosure (Barron et al., 1998; Barber et al., 2010).

Taken together, this study contributes to the cybersecurity and financial analyst literatures by providing novel evidence on how analysts respond to breach disclosures. We show that while analysts revise earnings forecast estimates in the expected direction, their stock recommendations remain unchanged, highlighting a disconnection between earnings expectations and investment guidance. These findings underscore the complex role analysts play in interpreting breach disclosures and the analysts' behavioral constraints that shape their outputs.

The remainder of the paper is organized as follows: Section 2 reviews relevant literature and develops our hypotheses. Section 3 describes the data and sample construction. Section 4

presents the methodology, empirical results, and robustness checks. Section 5 offers additional analyses. Section 6 concludes.

2. Prior Literature and Hypothesis Development

Cybersecurity Disclosure Regulation and Market Implications

Cybersecurity breaches are often hidden from external stakeholders unless companies voluntarily choose to disclose them, which creates significant information asymmetry. Managers typically have more complete information about the nature and extent of breach incidents and may choose to withhold, delay, or underreport such information, especially if disclosing it could damage the firm's reputation or financial performance (Kothari et al., 2009; Amir et al., 2018).

Recognizing this asymmetry, the SEC has progressively strengthened cybersecurity disclosure regulations to enhance transparency and investor protection. The 2011 guidance emphasized the need for firms to disclose cybersecurity risks and incidents if they were considered material to investors, impacting operations, financial condition, or reputation. However, it did not specify a timeline for reporting breaches, leaving firms with considerable discretion.

In 2018, the SEC expanded upon this guidance, stressing the timeliness of cybersecurity disclosures in response to increasing cyber threats and concerns over underreporting. The 2018 guidance placed a stronger emphasis on ensuring that firms disclose breach incidents promptly. However, firms still retained significant discretion regarding disclosure timing and content.

A significant regulatory change occurred on July 26, 2023, when the SEC introduced new mandatory cybersecurity disclosure rules, effective September 5, 2023. Public firms must now discuss cybersecurity risks and incidents in 10-K reports and disclose material cybersecurity breaches through Form 8-K within four business days of confirming the breach's materiality. The reporting window begins after firms conduct their internal investigation to verify the materiality of the event, rather than from the breach or discovery date. The regulatory

agency recognizes the challenges in evaluating cybersecurity event damages and does not want to discourage voluntary disclosures. Hence, there is currently no time frame for firms to assess the materiality of breach incidents.[2] Consequently, an information gap still exists between firms and stakeholders, as firms express concerns over the ambiguous definition of materiality in breach incidents.[3]

Despite the call for more transparency over cybersecurity breaches and emphasis on the importance of breach disclosures from the SEC, academic evidence remains divided over whether cybersecurity breaches have economically meaningful consequences. Past studies argue that breaches impose significant costs on firms. Breach firms are more likely to face higher loan spreads (Huang & Wang, 2021), increased audit fees (Yen et al., 2018), and have fewer lenders (Sheneman, 2017). Kamiya et al. (2021) find that a successful cyberattack that results in the loss of personal financial information will result in a considerable decline in shareholder wealth.

In addition, Tosun (2021) suggests that breaches reduce daily excess returns and increase trading volume due to selling pressure, impacting firm policies lasting up to five years. Xu et al. (2019) argue that breach firms are more likely to manage earnings. Two studies point out that cybersecurity breach incidents negatively impact the breach firms but positively affect their competitors (Martin et al., 2017; Jeong et al., 2019). Amir et al. (2018) and Foerderer and Schuetz (2022) highlight the role of managerial discretion in withholding information, further complicating market interpretations. Gordon et al. (2011) highlight that while breaches continue to have a significant negative impact on stock prices, investors view the cost of such

[2] SEC, "Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents," May 21, 2024, https://www.sec.gov/news/statement/gerding-cybersecurity-incidents-05212024

[3] Wiley Connect, "Recent Lessons from the SEC On Cyber Reporting: Darned if You Do, Darned if You Don't: Recent Lessons from the SEC On Cyber Reporting," May 23, 2024, https://www.wileyconnect.com/darned-if-you-do-darned-if-you-dont-recent-lessons-from-the-sec-on-cyber-reporting

events as diminishing over time. Overall, this body of literature review highlights the negative impacts of cybersecurity incidents.

Nevertheless, not all research finds strong economic consequences. Hilary et al. (2016) find no significant short- or long-term abnormal returns following breach disclosures, arguing that the costs are immaterial for large firms. Richardson et al. (2019) similarly report minimal effects on stock performance, audit fees, and internal controls and conclude that these factors are why firms are unwilling to invest in cybersecurity. Rosati et al. (2022) observe limited market reactions and changes in audit quality on breach incidents.

These findings raise an important question: if breaches impose material costs, why does the market not react more strongly to breach events? One explanation may lie in the nature of the disclosed information. Campbell et al. (2003) suggested that the economic impact of cybersecurity breaches depends on the specific nature and characteristics of the assets compromised in the breach. Additionally, an information imbalance is likely to exist in cyberattack incidents, and the actual costs of breach incidents are often unknown to outsiders. Managers may strategically underreport or downplay the severity of breach incidents (Kothari et al., 2009; Amir et al., 2018). Hence, ambiguity surrounding breach incidents may create noise rather than transparency, limiting the informativeness of breach disclosures.

The literature on voluntary breach disclosure adds further nuance. On one hand, voluntary disclosure improves transparency and is often rewarded by the market (Gordon et al., 2010; Berkman et al., 2018). Wang et al. (2013) and Brown et al. (2018) find that proactive disclosures are associated with reduced breach likelihood and improved investor confidence. Chen et al. (2023) report that reduced disclosure quality triggers market penalties, highlighting investor demand for consistent transparency.

On the other hand, breach disclosures can result in negative stock price reactions (Campbell et al., 2003; Cavusoglu et al., 2004; Goel & Shawky, 2009), increased crash risk (Cao et al., 2024), and reputational damage. Some studies warn that breach disclosure may accidentally reveal firm vulnerabilities to potential attackers (Ettredge et al., 2018; Li et al., 2018), creating a trade-off between disclosure risk and security risk. These tensions suggest that, while transparency is valued, firms are also exposed to legal, reputational, and operational risks.

Financial Analysts as Information Intermediaries

Financial analysts serve an important monitoring role on behalf of investors (Jensen & Meckling, 1976) and play a critical role in mitigating information asymmetry. As information intermediaries, analysts interpret disclosures, translate technical information, and provide forecasts that signal firm quality to the market (Chen et al., 2010; Livnat & Zhang, 2012; Rubin et al., 2017; Huang et al., 2018). Their role becomes crucial in environments with high information asymmetry, such as those involving cybersecurity incidents (Barth et al., 2002; Barron et al., 2002; Hsieh et al., 2016). Chen et al. (2015) suggest that analysts play a critical governance role in overseeing management. Furthermore, when information extraction costs are high, it increases the demand for analysts' inputs (Bloomfield, 2002). Thus, analysts serve as a proxy for external stakeholders' reactions, translating breach disclosures into meaningful insights. Analysts ' target price revisions and timely forecasts are also valuable, positively influencing market reactions (Brav & Lehavy, 2003; Clement & Tse, 2003). Most importantly, analysts' efforts become particularly significant when managers are likely to withhold information (Huang et al., 2018; Kothari et al., 2009; Amir et al., 2018). Analysts rely on private information when making forecasts (Barron et al., 1998), and both the level and direction of their recommendations help predict stock returns and future earnings surprises, indicating that analysts possess valuable insights not yet reflected in public information (Barber

et al., 2010). Therefore, not only do analysts serve as an important information channel, but analysts' outputs are also essential and valuable to investors when making investment decisions.

Despite this role, analysts' outputs are not without flaws. Analysts face challenges in evaluating disclosures, and past studies have shown limitations in analysts' forecasts (Lin & McNichols, 1998; Hong et al., 2000; Barber et al., 2006; Bradshaw, 2011; Zhang, 2006). Analysts often issue overly optimistic forecasts (Barber et al., 2006) and underreact to adverse or unanticipated news (Easterwood & Nutt, 1999; Rubin et al., 2017). Analysts are likely to herd due to career and reputational concerns (Hong et al., 2000). And analysts with more optimistic forecasts, especially those aligned with their firm's underwriting interests, are more likely to experience favorable career outcomes, suggesting that optimism is often rewarded over accuracy in brokerage firms (Hong & Kubik, 2003). Furthermore, conflicts of interest can impair forecast reliability, such as investment banking relationships (Lin & McNichols, 1998) and compensation incentives (Groysberg et al., 2011).

A separate strand of literature highlights a disconnection between earnings forecasts and stock recommendations. Bradshaw (2004) reveals that analysts' recommendations often fail to align with a fundamental valuation of earnings forecasts. His study employs the residual income model to estimate intrinsic stock values and, surprisingly, discovers a pattern that analysts tend to issue more favorable recommendations for stocks with low intrinsic values and vice versa. This suggests that personal biases may significantly influence analysts' recommendations. Similarly, Barniv et al. (2009), while documenting a positive association between earnings forecasts and future returns following Regulation Fair Disclosure (Reg FD), report findings consistent with Bradshaw (2004), showing an inverse relationship between analysts' recommendations and future returns. This highlights potential misalignment between recommendations and the actual valuation. Two studies observe that analysts are reluctant to revise recommendations. Conrad et al. (2006) find that analysts are generally hesitant to issue

downgrades, and their optimistic bias fluctuates over time rather than remaining constant. Another study further suggests that analysts appear to strategically introduce revision frictions in recommendations to attract profitable retail order flow from investors (Bernhardt et al., 2016). Taking a different approach, while analysts are expected to influence investor beliefs through their recommendations, Loh and Stulz (2011) find that only a small fraction of recommendation changes actually trigger significant market reactions. These further questions whether analyst outputs consistently reflect meaningful firm-specific information, especially in the context of complex events like cybersecurity breaches.

Hypothesis Development

Despite increasing regulatory emphasis on cybersecurity transparency, it remains unclear whether breach disclosures meaningfully influence analyst outputs. We learn from past cybersecurity research that breaches impose both direct and indirect costs on firms, as reflected in declines in shareholder wealth (Kamiya et al., 2021), increased financial constraints (Huang & Wang, 2021), and higher crash risks (Cao et al., 2024). In addition, breach disclosures are often associated with declines in market value (Campbell et al., 2003; Pirounias et al., 2014; Goel & Shawky, 2009). Moreover, financial analysts, as key information intermediaries, are trained with the skillsets in interpreting breach disclosures and translating technical information by providing informative earnings forecasts that incorporate the costs associated with breach incidents following breach announcements (Chen et al., 2010; Livnat & Zhang, 2012; Rubin et al., 2017; Huang et al., 2018).

However, the extent to which these disclosures are reflected in analyst forecasts remains uncertain. A growing body of research highlights several institutional and behavioral limitations that may impair analysts' forecasts. First, past research shows that cybersecurity incidents often lead to little or no reaction in the stock market (Hilary et al., 2016; Richardson et al., 2019), which may cause analysts to view these events as less important. Second, analysts

have been shown to underreact to complex or ambiguous negative news (Easterwood & Nutt, 1999; Rubin et al., 2017), and their forecasts are frequently influenced by conflicts of interest (Beyer & Guttman, 2011; Barber et al., 2001). Moreover, analysts may issue overly optimistic forecasts or fail to incorporate adverse information fully, especially when disclosure quality is low or management underreports the incident (Amir et al., 2018; Kothari et al., 2009).

In addition to this complexity, prior literature shows that analyst earnings forecasts and recommendations do not always align, and that recommendations tend to be more stable over time and influenced by factors beyond just firm fundamentals. Conrad et al. (2006) find stock recommendation changes are "sticky" in one direction. Bradshaw (2004, 2011) points out that recommendations often reflect personal biases and may not always provide meaningful valuation signals. Moreover, analysts appear to strategically introduce revision frictions in recommendations to attract profitable retail order flow (Bernhardt et al., 2016). Furthermore, analysts may refrain from making recommendation changes due to reputational risks, potential conflicts of interest, or a desire to maintain consistency (Groysberg et al., 2011; Bradley et al., 2017; Lin & McNichols, 1998). When faced with complex or ambiguous news like cybersecurity breaches, analysts are also more likely to underreact or delay their response (Easterwood & Nutt, 1999; Rubin et al., 2017).

Likewise, some analysts may view breach incidents as temporary disruptions with limited impact on long-term firm value, especially when companies underreport the severity of the incident (Amir et al., 2018) or when there is little market reaction (Hilary et al., 2016; Richardson et al., 2019). These findings suggest that analysts may not perceive breach events as materially affecting firm value.

This tension between the expected informational role of analysts and the institutional and behavioral frictions they face makes the analysts' outputs to breach disclosures an open

empirical question: Do analysts fully internalize the potential costs of breaches, or do they underreact due to noise, ambiguity, or strategic incentives?

The above discussion leads to the main hypothesis to be tested (stated in alternative form):

H1: *Cybersecurity breach disclosures are associated with downward revisions in analysts' forecast estimates.*

3. Data, Sample, and Descriptive Statistics

Data and Sample Selection

Breach disclosure data are collected from the Privacy Rights Clearinghouse (PRC)[4] and Audit Analytics cybersecurity databases (Li et al., 2018; Richardson et al., 2019). Although firms have discretion in disclosing breaches, the PRC database offers a significant advantage over other data breach datasets. Under State Security Breach Notification Laws, firms are legally required to report these breaches promptly, thereby lessening the issue of underreporting (Kamiya et al., 2021; Chen et al., 2024).

To investigate the hypotheses on the impact of breach disclosures on analysts' forecast measures, the annual consensus earnings forecasts are obtained from the Institutional Broker Estimate System (I/B/E/S) database, and financial information is extracted from Compustat. Table 1 presents the overview of the sample. Panel A of Table 1 shows the selection and development of the sample, and Panel B of Table 1 summarizes the industry distribution of the identified breach firms used in this study. The manufacturing sector represents the largest portion of our sample, with 36.08%, followed by firms in the information sector, with 19.32%. The final sample consists of 3,828 firm-year observations for 704 unique firms in the U.S. (352 treatment and 352 control).

The breach sample period spans from 2005 to 2022 because disclosure data was first available in the PRC dataset in 2005.[5] Following Huang and Wang (2021) and Kamiya et al. (2021), the sample is restricted with an observation window of -3 years and +3 years of the breach disclosure (including the incident year). The observation years for each firm are

[4] The PRC is a non-profit organization based in California that maintains a database with detailed information about cybersecurity incidents in the US. The database is also widely used in accounting and finance literature to examine the economic consequences of data breaches (Richardson et al., 2019; Rosati et al., 2022; Huang and Wang, 2021; Chen et al., 2022; Chen et al., 2024; Kamiya et al., 2021).

[5] The accounting data starts in 2003 because the observation window is [-3 +3] years.

validated to be consecutive. Moreover, governmental, not-for-profit, educational, and financial firms are excluded from the analysis (Mansi et al., 2011; Chen et al., 2015; Huang & Wang, 2021). Breach incidents with ambiguous/missing disclosure dates or company names are manually validated and dropped. Duplicated events are checked and removed. This study employs the fuzzy matching method to merge company names in the PRC database with the U.S. publicly traded company names in Compustat and manually validates matched pairs to obtain CUSIP and GVKEY identifiers.[6] The PRC and Audit Analytics breach databases are merged to increase the breach disclosure sample, and duplicate disclosures in both datasets are dropped. This study includes only the firm's first breach disclosure in the sample because it ensures a precise analysis before potentially expanding to include repeated incidents in future research. The primary breach disclosure data are merged with Compustat and I/B/E/S, ensuring each firm has the accounting and analysts' forecast data. The primary sample is then used for propensity score matching purposes.

Descriptive Statistics and Correlation Matrix

Our study analyzes a matched sample of 352 firms that issued a breach disclosure and 352 comparable control firms from 2005 to 2022. The data reveals an interesting pattern of breach disclosures issued in 2019 following the SEC's 2018 guidance on timely disclosure. Specifically, 2019 saw the highest number of disclosures, with 56 reported incidents, coincident with the SEC's new guidance. However, this heightened reporting activity gradually diminished from 2020 to 2022. Figure 1 tracks the trend of breach disclosures over this period.

To ensure statistical reliability, we winsorized continuous variables at the 1st and 99th percentiles, a standard technique for managing extreme data points. Detailed variable definitions can be found in Appendix A. Table 3 presents the Pearson correlation matrix. The

[6] Fuzzy matching allows us to match the company names across databases without common identifies. It uses a textual search-algorithm that provides a similarity score within a pair of text. It also greatly decreases the time-consuming manual checking process in identifying unstandardized company names in the PRC databases.

correlation coefficients among the independent variables are relatively low, indicating that multicollinearity is not a concern in this study. We employ the variance inflation factors (VIFs) to test for multicollinearity in each of the regression models used to run the test models. The values of all VIFs are below 3; hence, multicollinearity is not a threat to this study.

Table 3 presents the Pearson correlation matrix. The correlation coefficients among the independent variables are relatively low, indicating that multicollinearity is not a concern in this study. This study also employs the variance inflation factors (VIFs) to test for multicollinearity in each regression model used to run the test models. The values of all VIFs are below 3; hence, multicollinearity is not a threat to this study.

Insert Table 3

Analyst Forecast Measures

Analyst data are extracted from I/B/E/S, a historical earnings estimate database containing analyst estimates. This study employs two measures of analysts' forecasts. We test our hypothesis using *MEAN_ESTIMATES* as our first outcome variable, the formula is based on the average EPS estimates. The mean EPS estimate is calculated as follows:

$$\frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

where i is the individual analysts' forecasts and n is the number of earnings estimates

We measure analysts' recommendations using *MEAN_REC* as our second outcome variable. It is the mean recommendation for firm *i* in year *t*. The I/B/E/S maintains a standard set of recommendations with an assigned numeric value corresponding to the matching recommendation text from brokers. The stock recommendation is coded as follows: 1 for "Strong-Buy," 2 for "Buy," 3 for "Hold," 4 for "Underperform," and 5 for "Sell" recommendations (Barber et al., 2006).

Control Variables

This study also includes several control variables that are proven to influence analysts' forecast estimates. Following past literature, this research controls for firm size (*SIZE*), as proxied by the natural logarithm of total assets in US$ million. Prior studies have shown that analysts' estimates positively correlate with firm size (Chen et al., 2022). Furthermore, return on assets (*ROA*) as a control variable is calculated as the net income divided by total assets in Compustat. It is expected that *ROA* is correlated positively with analyst forecast measures. Firm leverage (*LEVERAGE*) is formulated as total liabilities divided by total assets, representing the percentage of total assets funded through debt in a firm. Past literature has suggested *LEVERAGE* to be negatively associated with analysts' forecasts. This study also controls for cashflow (*CASHFLOW*) computed as cashflows from operations for year *t* divided by total assets at the beginning of the year. *CASHFLOW* captures operational performance and positively correlates with analysts' forecasts, as Chen et al. (2015) documented.

Additionally, controlling for sales growth (*SALES_GROWTH)* is relevant to this study, and following Kamiya et al. (2021), it is measured as net sales in period *t* divided by net sales in period *t-1*. It is anticipated that sales growth will be positively correlated with analysts' forecasts because higher growth in sales should increase analysts' estimates of the firm. Per Behn et al. (2008), the firms' financial constraints (*LOSS*) in the given financial year are controlled. *LOSS* is an indicator variable that takes the value of 1 if the firm makes a loss in the fiscal year and zero otherwise. The sign for *LOSS* is anticipated to be negative with analysts' forecasts because firms making losses are more likely to have lower earnings estimates. The Tobin Q ratio (*TOBIN*_Q) is computed as the sum of market capitalization and the book value of debt divided by the book value of total assets. Last, this research controls for analyst coverage (*ANALYST*) as more analysts following increases analysts' forecast quality. Due to

the skewness of the number of analysts following the firm, the natural logarithm of one plus the total number of analysts following the firm has been employed.

4. Methodology and Empirical Results

PSM Sample and Research Design

A potential challenge in this study is that the breach sample may suffer from self-selection bias, which may lead to endogeneity issues. An alternative explanation suggests that breach firms are not randomly selected for treatment. Instead, they are self-selected into the treatment group. Some unique firm characteristics may have caused those firms to be targets of cyberattack incidents. For example, prior studies have found that larger and more profitable firms are more likely to become cyberattack targets. Self-selection bias and omitted variable bias can cause the estimated coefficient to be biased and result in misleading interpretations. Thus, this study employs the propensity score matching (PSM) technique to ensure that the breach firms and the control firms have similar firm-level characteristics to mitigate selection bias (Chen et al., 2015; Wang et al., 2022).

The treatment group consists of firms that have issued breach disclosures. And treatment firms are based on the year before breach disclosures for matching. Since breach disclosures occur at different times, dummy variable *PRE* is assigned the value of one if the period is one year before the breach disclosure and zero otherwise. The control firms are selected from the entire Compustat database, and it is further verified that the potential control firms also have I/B/E/S data.

Additionally, this study ensures that the treatment firms will never be selected as control firms; therefore, the already treated group cannot serve as a control group (Callaway & Sant'Anna, 2021). The matching firm characteristics variables are *ROA*, *SIZE*, *LEVERAGE*, *CASHFLOW*, *SALES_GROWTH*, *LOSS,* and *TOBIN_Q* in the year prior to breach incidents.

These firm characteristics are chosen based on the prior literature. Huang and Wang (2021) suggest that firms with higher *ROA* have a more substantial customer base and therefore

contain more valuable customer information to be a vulnerable target for cyberattack. Kamiya et al. (2021) confirm that *ROA* is associated with breach incidents. The relationship between *LEVERAGE* and the cyber breach is unclear. It has been stated that firms with higher debt may have weaker cybersecurity systems to prevent breach incidents from potential hackers and malware. However, cybercriminals are less incentivized to target firms with higher debts due to less valuable information. (Chen et al., 2015; Huang and Wang, 2021; Rubin et al., 2017; Mansi et al., 2011). There is also a negative association between *CASHFLOW* and breach incidents, as firms experience higher operational risk post-cyberattack incidents (Huang & Wang, 2021; Kamiya et al., 2021). *SALES_GROW*TH is expected to be negatively associated with breach incidents due to reputation costs arising from weakening customer confidence after cyberattacks (Kamiya et al., 2021). Firms' financial conditions (*LOSS*) are included as financially constrained firms are less likely to invest in cybersecurity control systems (Ettredge et al., 2018; Li et al., 2018). Kamiya et al. (2021) suggest that firms with higher *TOBIN_Q* will likely become cyberattack targets.

Prior literature has shown that cyberattacks appear to be clustered in specific industries (Kamiya et al., 2021); this study employs propensity score matching of treatment and control observations in the same industry (based on the 2-digit SIC industry code) and the same financial year (Chen et al., 2023). A first-stage probit regression model is conducted where treatment is regressed on lagged firm characteristics for all companies in the Compustat database between 2005 and 2022. The coefficients are then used to calculate a propensity score for each firm-year (Huang & Wang, 2021; Chen et al., 2022).

The probit model used for the propensity score match is as follows:

$$TREAT_t = \gamma + \gamma_1 ROA_{t-1} + \gamma_2 SIZE_{t-1} + \gamma_3 LEVERAGE_{t-1} + \gamma_4 CASHFLOW_{t-1} + \gamma_5 SALES\_GROWTH_{t-1} + \gamma_6 LOSS_{t-1} + \gamma_7 TOBIN\ Q_{t-1} + \gamma Industry + \gamma Year + \varepsilon \quad (2)$$

Since the propensity score matching method pairs each treated firm with a control firm from the same industry and year, some control firms may be matched to multiple treated firms. Therefore, it is important to manually check for duplicate matches by identifying the corresponding treated firms and removing any duplicate pairs from the sample. Additionally, we ensure that all firms included in the staggered DID analysis have at least one observation in both the pre- and post-breach periods. Breach (treatment) firms are paired using a nearest-neighbor probit matching strategy and caliper matching with a distance of 0.01 (Rosenbaum & Rubin, 1985). This study validates that the treatment and control firms are similar in firm characteristics in the pre-breach disclosure period. The mean comparison table is presented in Table 4.

Following the staggered DID design, this study constructs the following empirical model to examine the effect of cyber breach disclosures on analysts' forecast estimates.

$$Analysts\ Forecast\ Measures_{it} = \alpha + \beta_1 TREAT_{it} * POST_{it} + Controls + Firm\ FE + Year\ FE + \varepsilon_{it} \quad (3)$$

where *i* and *t* index firms and year, respectively. Analyst forecast measures are *MEAN_ESTIMATES* and *MEAN_REC* as the outcome variables. *TREAT* is a dummy variable that takes a value of one if the firm is a breach firm and zero for a control firm. *POST* is a dummy variable that takes a value of one during the post-disclosure period and zero otherwise. Following Huang and Wang (2021) and Fauver et al. (2017), this research employs the firm-fixed effects to capture time-invariant firm-level factors and to control for correlated omitted variables concerns and the year-fixed effects to control year-specific characteristics that are common to all firms in year *t* (Imbens & Wooldridge, 2009). To control for heteroskedasticity, robust standard errors are clustered at the industry levels (Petersen, 2009).

Our research relies on two critical assumptions for the staggered DID model. The first assumption involves the staggered adoption of treatment, which means that once a firm issues

a breach disclosure, it remains in the treatment group throughout the observation period. We verify that treatment firms are never selected as control firms. The second assumption – the parallel trend assumption states that the treatment and control groups are similar in characteristics for valid comparisons. These assumptions are crucial for establishing the credibility of our comparative analysis and ensuring that our findings accurately reflect the impact of cybersecurity breach disclosures.

Using the outcome variable of earnings forecast estimates, the primary coefficient of interest is the interaction term *TREAT* × *POST*, which measures changes in earnings forecasts for breach firms during the post-disclosure period. In our first outcome variable, *MEAN_ESTIMATES*, a negative and statistically significant coefficient for the interaction term would indicate that analysts revise their earnings forecasts downward after breach disclosures, reflecting potential damage caused by the breach incidents. As for our second outcome variable, *MEAN_REC*, a positive and statistically significant coefficient for the interaction term would suggest that analysts downgrade their recommendations following breach disclosures, indicating concern about the stock and a preference for selling. Conversely, an insignificant coefficient would suggest that breach disclosures have no observable impact on analysts' forecast estimates or recommendations.

To ensure robustness, we include control variables that might correlate with analysts' forecast estimates. This comprehensive approach helps isolate the specific impact of breach disclosures on analysts' forecasts and recommendations.

Mean Comparison Test

Table 4 highlights the importance of mean comparison between treatment and control firms before and after propensity score matching. Mean comparison ensures that any observed differences in outcomes can be attributed to the treatment, in this case, breach disclosures,

rather than any pre-existing differences between the groups. Panel A of Table 4 reports the differences in means between treatment and control firms before propensity score matching, where the t-statistics of the matched variables are highly significant. This indicates notable differences in firm characteristics prior to matching.

Panel B of Table 4 presents the mean comparison after propensity score matching, specifically one year before breach disclosures (*t-1*). Here, the t-statistics are no longer statistically significant, suggesting that treatment and control firms exhibit similar firm characteristics in period *t-1*. This outcome confirms the success of propensity score matching, as it balances the observable covariates between the two groups, ensuring comparability and reducing selection bias (Rosenbaum & Rubin, 1985). By achieving balance, the matched sample allows for a more robust estimation of the treatment effects, enhancing the validity of the results.

Insert Table 4

Main Results

Table 5 presents the staggered DID regression results based on Equation (3) to examine the effects of the cyber breach disclosures on analyst forecast measures for the breach firms.

Analyst Earnings Forecasts (*MEAN_ESTIMATES*)

For the results on the outcome variable *MEAN_ESTIMATES* in columns 1 to 3, the coefficient of *TREAT* × *POST* is negative and statistically significant at the 5% level. The interaction term captures the changes in the post-disclosure change in analysts' earnings estimates for the breach firms, and it is economically meaningful, revealing that analysts' estimates have, on average, decreased by 0.29 or 13.5% for the breach firms in the post-

disclosure period.[7] Hence, the findings align with the conclusions drawn in previous studies that suggest the breach disclosures negatively affect the breach firms in valuation (Goel & Shawky, 2009; Amir et al., 2018). Cybersecurity breaches have direct and indirect costs, such as recovery costs, regulatory fines, lawsuits, and reputational costs (Gordon et al., 2011); these events will likely impact firms' earnings.

This result supports the view that analysts serve as effective information intermediaries by incorporating adverse news into their earnings forecasts (Chen et al., 2010; Livnat & Zhang, 2012; Rubin et al., 2017). Analysts' forecasts are particularly valuable in settings characterized by information asymmetry, such as cybersecurity breaches, where managers may have incentives to delay or withhold disclosures (Kothari et al., 2009; Amir et al., 2018). The observed forecast revisions suggest analysts respond to the breach as a negative information event, fulfilling their role in translating complex disclosures into valuation-relevant information (Barth et al., 2002; Brav & Lehavy, 2003).

Control variables in the *MEAN_ESTIMATES* model also behave as expected and are consistent with prior work. *ROA*, *SIZE*, *CASHFLOW*, *SALES_GROWTH*, and *ANALYST* coverage are all positively associated with earnings forecasts, reflecting that larger, more profitable, and better-followed firms are expected to perform better (Chen et al., 2022; Kamiya et al., 2021). Conversely, the *LOSS* indicator is negatively associated with forecasts, suggesting that financial distress leads to more conservative earnings expectations.

[7] We also examine analysts' forecasts within a narrower event window, focusing on the days immediately surrounding the breach disclosure. Using the same model specifications as in Equation (3), we find no statistically significant changes in analyst forecast measures during this short-term period. This result suggests that analysts do not immediately adjust their forecasts in response to breach announcements. However, cybersecurity-related costs often unfold gradually, and the financial implications may not be immediately observable. As such, analysts may revise their forecasts over time as new information becomes available and the impact of the breach becomes clearer.

Analyst Recommendations (*MEAN_REC*)

For the results on the second outcome variable, *MEAN_REC* in columns 4 to 6. The results are not statistically significant, suggesting no difference in analysts' recommendations for breach firms in the post-breach disclosure period. Several explanations are supported by the literature.

First, prior research highlights that valuations and recommendations do not always align. Bradshaw (2004, 2011) shows that analysts' recommendations often fail to align with intrinsic firm valuation and may be influenced by behavioral or institutional biases. Barniv et al. (2009) similarly find that recommendations may diverge from valuation-relevant information. Analysts often exhibit an optimism bias and hesitate to issue downgrades (Conrad et al., 2006). This "stickiness" of recommendations is well-documented, with analysts being more reluctant to revise downward due to career concerns, pressure from institutional clients, or the desire to maintain access to firm management (Hong & Kubik, 2003; Groysberg et al., 2011; Bernhardt et al., 2016).

Second, managers may strategically disclose less severe or immaterial breach incidents while withholding more serious ones (Kothari et al., 2009; Amir et al., 2018), reducing the perceived significance of the breach. Combined with studies showing that many breaches result in minimal market reaction (Hilary et al., 2016; Richardson et al., 2019; Rosati et al., 2022), analysts may conclude that revisions to recommendations are unnecessary. This aligns with Loh and Stulz (2011), who find that only a small fraction of recommendation changes significantly move markets, implying that recommendations may be more sticky and less sensitive to new risk information.[8]

[8] Untabulated mediation analysis following Baron and Kenny (1986) confirms the stickiness of analyst recommendations. We test whether changes in valuation, proxied by the P/E ratio, mediate the relationship between breach disclosures and analyst recommendations. Although breach disclosures are associated with an

In summary, while earnings forecast revisions seem to capture the financial impact of breach disclosures, their recommendations are likely to be limited by organizational pressures, strategic incentives, or the uncertain nature of voluntary breach disclosures.

Control variables in the *MEAN_REC* regression also align with prior findings. *SALES_GROWTH*, *TOBIN_Q*, and *ANALYST* are negatively related to recommendation scores (i.e., implying more favourable ratings), consistent with growth-oriented, well-covered firms receiving more optimistic recommendations. LOSS is positively associated with MEAN_REC, indicating that analysts are more likely to downgrade firms experiencing financial losses.

Insert Table 5

Robustness Test

Parallel trend assumption – Pre-treatment test

To ensure the validity of the staggered DID approach, this study conducts a pre-treatment test to verify the parallel trend assumption. This assumption requires that, in the absence of treatment (i.e., breach disclosures), the treatment and control firms would have followed similar trends over time in analysts' forecast outcomes. Following the approach used in prior literature (Kamiya et al., 2021; Cao et al., 2024), we estimate an extended DID model by adding an interaction term between the treatment indicator and a pre-disclosure period indicator, labeled *TREAT* × *PRE*. This term captures any difference in analyst forecasts between treatment and control firms in the year before the breach disclosure. The regression specification includes firm and year fixed effects and is expressed as follows:

$$MEAN\_ESTIMATES_{it} = \alpha + \beta_1 TREAT_{it} * POST_{it} + \beta_2 TREAT_{it} * PRE_{it} + Controls + Firm\ FE + Year\ FE + \varepsilon_{it} \quad (4)$$

increase in the P/E ratio - suggesting earnings decline without a corresponding drop in stock price—analysts do not adjust their recommendations accordingly. We obtain similar results when using analysts' mean earnings forecasts (*MEAN_ESTIMATES*) as an alternative mediator. In both cases, recommendations remain statistically insignificant, consistent with prior evidence that analysts often ignore valuation signals when revising stock recommendations (Bradshaw, 2004; Barniv et al., 2009; Groysberg et al., 2011).

where *i* and *t* index firms and year, respectively. *PRE* is a dummy variable that takes a value of one if the period is one year before the breach disclosure and zero otherwise. In Equation (4), the two interaction terms are coefficients of interest. The coefficient for *TREAT* × *POST* is expected to remain negative and statistically significant if analysts revise their forecast estimates downward in the post-breach disclosure period. *TREAT* × *PRE* is expected to be insignificant if the parallel trend assumption in the pre-treatment holds. An insignificant coefficient suggests that in the absence of treatment (breach disclosure), the difference in analysts' forecasts between treatment and control groups would have remained constant over time. Therefore, the two groups are comparable. In contrast, if *TREAT* × *PRE* is significant, it suggests that the differences in trends between the two groups exist before the breach disclosure has occurred. The same set of control variables as in Equation (3) has been employed.

Table 6 reports the results of this test. The coefficient on *TREAT* × *POST* remains negative and statistically significant at the 5% level, confirming that breach disclosures are followed by downward revisions in analyst earnings forecasts. More importantly, the coefficient on *TREAT* × *PRE* is statistically insignificant, suggesting that there were no significant differences in analyst forecasts between the two groups in the year before the breach occurred. This provides strong evidence that the parallel trends assumption holds.

Insert Table 6

Further supporting this result, Figure 2 displays the average trends in analysts' mean earnings forecasts for both treatment and control firms across the pre- and post-breach periods. The figure shows that the two groups exhibit similar trends in the years leading up to the breach, with a visible divergence emerging only after the disclosure. Taken together, these findings support the validity of our staggered DID research design and reinforce the interpretation that the observed decline in analyst forecasts is indeed driven by the breach disclosures.

Insert Figure 2

Time-Series Placebo Test

We conduct a time-series placebo test for our DID analysis as an additional robustness check. To do this, we randomly assign a placebo period (three years prior to the actual disclosure year) for each firm and re-run the DID regression using the Equation (3) specification. This test helps identify and rule out pre-existing trends while verifying that any treatment effect occurs after the breach disclosure event. If significant effects are found in the placebo periods, it may indicate that the observed relationship is due to pre-existing trends, not the breach disclosure itself.

As expected, Table 7 presents the results of the time-series placebo test, showing that the interaction term of *TREAT* × *POST* is insignificant across all specifications. This confirms that our DID model is robust and unaffected by pre-existing trends or random noise unrelated to breach disclosures.

Insert Table 7

5. Additional Analysis

Post-Periods Analysis

Our study further breaks down the *POST* period into three subsequent periods in the post-breach disclosures (Kamiya et al., 2021; Cao et al., 2024). This approach analyzes how the effects of breach disclosures on analysts' forecasts differ in each of the three years after the disclosures. Three dummy variables indicate the three years following the breach disclosures. The specification model is as follows:

$$MEAN\_ESTIMATES_{it} = \alpha + \beta_1 TREAT_{it} * POST1_{it} + \beta_2 TREAT_{it} * POST2_{it} + \beta_3 TREAT_{it} * POST3_{it} + Controls + Firm\ FE + Year\ FE + \varepsilon_{it} \quad (5)$$

where *i* and *t* index firms and year, respectively. $POST1$ is a dummy variable that takes a value of one for the first year following the breach disclosure and zero otherwise. $POST2$ is a dummy variable that takes a value of one for the second year following the breach disclosure and zero otherwise. And $POST3$ is a dummy variable that takes a value of one for the third year following the breach disclosure and zero otherwise. The main coefficients of interest are the three interaction terms, which capture the changes in the post-disclosure periods, respectively, in analysts' earnings estimates for the breach firms.

Table 8 reports the results for Equation (5), which reveals that β_1 and β_2 are negative and statistically significant at the 5% level, whereas β_3 is not statistically significant. The results, therefore, further suggest a negative relation between breach disclosures and analysts' earnings estimates. Analyst forecast estimates are reduced by 0.30 for the firms that disclose breach incidents in the first year and 0.31 in the second year.

In summary, the post-period analysis reveals that the downward revision in analysts' earnings forecasts is strongest in the first two years after a breach disclosure, but the effect does

not persist into the third year. These results reinforce the interpretation that while analysts respond meaningfully to breach disclosures, they do not view the associated risks as permanently impairing long-term firm value. Additionally, the results present a very similar pattern to the effects of the 2018 SEC guidance, which appeared to have encouraged breach disclosures to peak in 2019, but the effects slowly diminished between 2020 and 2022.

Insert Table 8

Information Environment and Analysts' Forecasts

This study conducts additional subsample DID analysis to investigate the difference in analysts' forecast estimates for breach firms with high and low transparency information environments. Analyst following is commonly used as a proxy for the information environment because it reflects the extent to which analysts monitor and analyze a firm. Past studies have shown higher analysts following decreases in information asymmetry because analysts act as information intermediaries to the market (Chen et al., 2010; Livnat & Zhang, 2012; Rubin et al., 2017; Huang et al., 2018), and increased efforts in analysts also lead to a more transparent information environment (Cheng & Subramanyam, 2008; Harford et al., 2019). Botosan (1994) highlights that the relationship between voluntary disclosure and the cost of equity capital is conditional on the level of analyst following. Healy and Palepu (2001) also noted that firms with high analyst coverage benefit from greater scrutiny, leading to improved information flow and more accurate forecasts. In addition, firms that disclose more information about their corporate governance tend to attract more financial analysts, which in turn improves the firm's overall information environment (Yu, 2010). Following Botosan (1997), we use the median analyst following as a threshold to divide our sample into high and low information transparency subsamples. The same regression in Equation (3) is employed with the same control variables and fixed effects specification.

The results are depicted in Table 9, where the first two columns report the DID regressions for the high information transparency firms, and the last two columns present the DID regressions for the low information transparency firms. Consistent with Botosan (1997), the interaction term in the high transparency sample is negative and weakly significant at the 10% level. This indicates that firms with a higher number of analysts following are more likely to experience a decrease in forecast estimates in the period following breach disclosures. This suggests that firms with greater analyst coverage benefit from lower information asymmetry, making their breach disclosures more informative.

Although we do not observe a difference in forecast estimates for firms with opaque information environments, it does not indicate that having a more transparent information environment is disadvantageous to breach firms because we do not observe changes in analysts' recommendations for these firms, indicating that analysts may incorporate the potential costs of the breach into their earnings forecasts without adjusting their overall recommendations. These findings imply that financial analysts in high transparency environments have higher-quality information to predict the financial impact of breach incidents in their forecast earnings.

Insert Table 9

Information Environment and Forecast Dispersion

Prior research indicates that higher forecast dispersion—the variability in earnings forecasts—is generally associated with increased uncertainty among analysts (Barron & Brown, 1998; Zhang, 2006). Some studies have argued that firms with more informative disclosures tend to attract more analysts and experience less dispersion in their forecasts (Lang & Lundholm, 1996) because when analysts follow a firm closely, they generate additional information about the firm. However, when the information available or disclosed by the firm is imprecise, forecast dispersion increases as analysts face greater challenges in producing

accurate reports (Roulstone, 2003). Prior studies have shown that when firms temporarily withhold bad news, it results in greater forecast dispersion among analysts (Ali et al., 2019), and this is relevant to our study because firms are more likely to withhold or delay disclosures on breach incidents (Amir et al., 2018). Following Roulstone (2003), our study uses forecast dispersion as a proxy for the quality of information available about the firm. Specifically, we measure forecast dispersion as the standard deviation of earnings forecasts scaled by the mean forecast value. This measure captures the relative spread of forecasts and serves as an indicator of the underlying information uncertainty.

We then explore how high and low information environments affect analyst dispersion. As presented in Table 10, our findings reveal that in a high information environment, forecast dispersion declines following breach disclosures. This suggests that when the overall transparency is high, breach disclosures contribute to a more accurate and comprehensive understanding of the firm, and the quality of information is, therefore, more informative, reducing uncertainty among analysts. These results align with previous studies that uncertainty in analysts' forecasts is more likely to decrease on average when the information environment is more transparent. However, there is no clear evidence of a change in analyst dispersion in a low information environment. These results reveal that when the information environment transparency is low, the additional disclosure of breach information does little to mitigate existing uncertainty among analysts. Thus, the disclosures are not as informative.

Insert Table 10

6. Conclusion

In conclusion, this study examines the effects of cybersecurity breach disclosures on financial analysts' forecast outputs. Motivated by increased regulatory emphasis on breach transparency and the informational role of analysts, this study explores how analysts respond to breach incidents that firms voluntarily disclose. While prior literature offers mixed views on the economic significance of cybersecurity breaches and highlights analysts' limitations in processing complex disclosures, this study adds new empirical evidence by directly linking breach disclosures to analyst behaviors.

This study provides empirical evidence that analysts significantly lower their earnings forecasts for breach firms following disclosures, suggesting that analysts incorporate the anticipated negative financial implications of breach events into their forecasts. And the impacts appear most significant in the first and the second years following breach disclosures and gradually subside in the third year.

Despite decreased earnings forecast estimates for breach firms, this study does not observe a change in the recommendations issued. This supports prior research suggesting that analysts' recommendations do not always align with their earnings forecasts and may not fully reflect fundamental valuations. Furthermore, these findings are consistent with past cybersecurity-related studies, suggesting that market participants often perceive the economic consequences of breach incidents as insufficiently significant.

Overall, this study contributes to the literature on cybersecurity, financial analysts, and voluntary disclosure by providing evidence on how analysts interpret and respond to breach disclosures. It underscores the importance of understanding not only the informational value of breach events but also the institutional context that shapes how such information is processed and transmitted in capital markets.

However, this study acknowledges certain limitations. It only examines voluntary breach disclosures before the 2023 mandatory cybersecurity regulations. Future research could explore how analysts' forecasts and recommendations evolve under the new disclosure rules. Additionally, further investigation into the moderating effects of institutional shareholders and corporate governance, such as internal control weaknesses, could enhance understanding. Future studies may also benefit from analyzing the impact of repeated breach incidents on firms' financial outcomes and analysts' perceptions.

Reference

Ali, A., Liu, M., Xu, D., & Yao, T. (2019). Corporate disclosure, analyst forecast dispersion, and stock returns. *Journal of Accounting, Auditing & Finance*, 34(1), 54-73.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23, 1177-1206.

Barber, B., Lehavy, R., McNichols, M., & Trueman, B. (2001). Can investors profit from the prophets? Security analyst recommendations and stock returns. *The Journal of Finance*, 56(2), 531-563.

Barber, B. M., Lehavy, R., McNichols, M., & Trueman, B. (2006). Buys, holds, and sells: The distribution of investment banks' stock ratings and the implications for the profitability of analysts' recommendations. *Journal of Accounting and Economics*, 41(1-2), 87-117.

Barber, B. M., Lehavy, R., & Trueman, B. (2010). Ratings changes, ratings levels, and the predictive value of analysts' recommendations. Financial Management, 39(2), 533-553.

Barniv, R., Hope, O. K., Myring, M. J., & Thomas, W. B. (2009). Do analysts practice what they preach and should investors listen? Effects of recent regulations. *The Accounting Review*, 84(4), 1015-1039.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of personality and social psychology, 51(6), 1173.

Barth, M., R. Kasznik and M. McNichols (2002), 'Analyst Coverage and Intangible Assets', *Journal of Accounting Research*, Vol. 39, No. 1, pp. 1–34.

Barron, O. E., & Stuerke, P. S. (1998). Dispersion in analysts' earnings forecasts as a measure of uncertainty. *Journal of Accounting, Auditing & Finance*, 13(3), 245-270.

Barron, O. E., Kim, O., Lim, S. C., & Stevens, D. E. (1998). Using analysts' forecasts to measure properties of analysts' information environment. *The Accounting Review*, 421-433.

Barron, O. E., D. Byard, C. Kile and E. Riedl (2002), 'High-Technology Intangibles and Analysts' Forecasts', *Journal of Accounting Research*, Vol. 40, No. 2, pp. 289–312.

Behn, B. K., Choi, J. H., & Kang, T. (2008). Audit quality and properties of analyst earnings forecasts. *The Accounting Review*, 83(2), 327-349.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508-526.

Bernhardt, D., Wan, C., & Xiao, Z. (2016). The reluctant analyst. Journal of Accounting Research, 54(4), 987-1040.

Beyer, A., & Guttman, I. (2011). The effect of trading volume on analysts' forecast bias. *The Accounting Review*, 86(2), 451-481.

Bloomfield, R. J. (2002). The incomplete revelation hypothesis' and financial reporting.

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

Bradley, D., Gokkaya, S., Liu, X., & Xie, F. (2017). Are all analysts created equal? Industry expertise and monitoring effectiveness of financial analysts. *Journal of Accounting and Economics*, 63(2-3), 179-206.

Bradshaw, M. T. (2004). How do analysts use their earnings forecasts in generating stock recommendations?. *The Accounting Review*, 79(1), 25-50.

Bradshaw, M. T. (2011). Analysts' forecasts: what do we know after decades of work?. Available at SSRN 1880339.

Brav, A., & Lehavy, R. (2003). An empirical analysis of analysts' target prices: Short‐term informativeness and long‐term dynamics. *The Journal of Finance*, 58(5), 1933-1967.

Brown, S. V., Tian, X., & Wu Tucker, J. (2018). The spillover effect of SEC comment letters on qualitative corporate disclosure: Evidence from the risk factor disclosure. *Contemporary Accounting Research*, 35(2), 622-656.

Callaway, B., & Sant'Anna, P. H. (2021). Difference-in-differences with multiple time periods. *Journal of Econometrics*, 225(2), 200-230.

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.

Cao, H., Phan, H. V., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis*, 93, 103164.

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

Chen, C., Hartmann, C., & Gottfried, A. (2022). The impact of audit committee IT expertise on data breaches. *Journal of Information Systems*, 36(3), 61-81.

Chen, C. Y., Goh, B. W., Lee, J., & Li, N. (2025). The Effect of Cybersecurity Breaches on Analysts' Earnings Forecasts. European Accounting Review, 1-27.

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187(1), 199-224.

Chen, T., Harford, J., & Lin, C. (2015). Do analysts matter for governance? Evidence from natural experiments. *Journal of Financial Economics*, 115(2), 383-410.

Chen, W., Li, X., Wu, H., & Zhang, L. (2024). The Impact of Managerial Myopia on Cybersecurity: Evidence from Data Breaches. *Journal of Banking & Finance*, 107254.

Chen, W., Zhang, L., Jiang, P., Meng, F., & Sun, Q. (2022). Can digital transformation improve the information environment of the capital market? Evidence from the analysts' prediction behaviour. *Accounting & Finance*, 62(2), 2543-2578.

Chen, X., Cheng, Q., & Lo, K. (2010). On the relationship between analyst reports and corporate disclosures: Exploring the roles of information discovery and interpretation. *Journal of Accounting and Economics*, 49(3), 206-226.

Cheng, M., & Subramanyam, K. R. (2008). Analyst following and credit ratings. *Contemporary Accounting Research*, 25(4), 1007-1044.

Clement, M. B., & Tse, S. Y. (2003). Do investors respond to analysts' forecast revisions as if forecast accuracy is all that matters?. *The Accounting Review*, 78(1), 227-249.

Conrad, J., Cornell, B., Landsman, W. R., & Rountree, B. R. (2006). How do analyst recommendations respond to major news?. *Journal of Financial and Quantitative Analysis*, 41(1), 25-49.

Eames, M., Glover, S. M., & Kennedy, J. (2002). The association between trading recommendations and broker-analysts' earnings forecasts. *Journal of Accounting Research*, 40(1), 85-104.

Easterwood, J. C., & Nutt, S. R. (1999). Inefficiency in analysts' earnings forecasts: Systematic misreaction or systematic optimism?. *The Journal of Finance*, 54(5), 1777-1797.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564-585.

Ettredge, M., & Richardson, V. J. (2003). Information transfer among internet firms: the case of hacker attacks. *Journal of Information Systems*, 17(2), 71-82.

Fauver, L., Hung, M., Li, X., & Taboada, A. G. (2017). Board reforms and firm value: Worldwide evidence. *Journal of Financial Economics*, 125(1), 120-142.

Fleury, A., & Salva, C. (2025) How do Cyberattacks Impact Firms? Available at SSRN: https://ssrn.com/abstract=5175947

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, 36(1), 351-407.

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: a matter of timing?. *Management Science*, 68(10), 7298-7322.

Goel, S., & 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., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 567-594.

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

Groysberg, B., Healy, P. M., & Maber, D. A. (2011). What drives sell-side analyst compensation at high-status investment banks?. *Journal of Accounting Research*, 49(4), 969-1000.

Haislip, J., Lim, J. H., & Pinsker, R. (2017). Do the Roles of the CEO and CFO Differ when it comes to Data Security Breaches?. *Twenty-third Americas Conference on Information Systems*.

Harford, J., Jiang, F., Wang, R., & Xie, F. (2019). Analyst career concerns, effort allocation, and firms' information environment. *The Review of Financial Studies*, 32(6), 2179-2224.

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

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: who cares?. *Georgetown McDonough School of Business Research Paper*, (2852519).

Hong, H., & Kubik, J. D. (2003). Analyzing the analysts: Career concerns and biased earnings forecasts. The Journal of Finance, 58(1), 313-351.

Hong, H., Kubik, J. D., & Solomon, A. (2000). Security analysts' career concerns and herding of earnings forecasts. The Rand journal of economics, 121-144.

Hsieh, C. C., Hui, K. W., & Zhang, Y. (2016). Analyst report readability and stock returns. *Journal of Business Finance & Accounting*, 43(1-2), 98-130.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, *96*(3), 261-286.

Huang, A. H., Lehavy, R., Zang, A. Y., & Zheng, R. (2018). Analyst information discovery and interpretation roles: A topic modeling approach. *Management Science*, 64(6), 2833-2855.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, 96(3), 261-286.

Imbens, G. W., & Wooldridge, J. M. (2009). Recent developments in the econometrics of program evaluation. *Journal of Economic Literature*, 47(1), 5-86.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82(2), 85-105.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, 56(5), 681-695.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & 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.

Kothari, S. P., Shu, S., & Wysocki, P. D. (2009). Do managers withhold bad news?. *Journal of Accounting Research*, 47(1), 241-276.

Lang, M. H., & Lundholm, R. J. (1996). Corporate disclosure policy and analyst behavior. The Accounting Review, 467-492.

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

Lin, H. W., & McNichols, M. F. (1998). Underwriting relationships, analysts' earnings forecasts and investment recommendations. *Journal of Accounting and Economics*, 25(1), 101-127.

Livnat, J., & Zhang, Y. (2012). Information interpretation or information discovery: Which role of analysts do investors value more?. *Review of Accounting Studies*, 17, 612-641.

Loh, R. K., & Stulz, R. M. (2011). When are analyst recommendation changes influential?. The review of financial studies, 24(2), 593-627.

Mansi, S. A., Maxwell, W. F., & Miller, D. P. (2011). Analyst forecast characteristics and the cost of debt. *Review of Accounting Studies*, 16, 116-142.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.

Meckling, W. H., & Jensen, M. C. (1976). Theory of the Firm. Managerial behavior, agency costs and ownership structure, 3(4), 305-360.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, 19(4-5), 257-271.

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.

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

Rosenbaum, P. R., & Rubin, D. B. (1985). Constructing a control group using multivariate matched sampling methods that incorporate the propensity score. *The American Statistician*, 39(1), 33-38.

Roulstone, D. T. (2003). Analyst following and market liquidity. *Contemporary Accounting Research*, 20(3), 552-578.

Rubin, A., Segal, B., & Segal, D. (2017). The interpretation of unanticipated news arrival and analysts' skill. *Journal of Financial and Quantitative Analysis*, 52(4), 1491-1518.

Petersen, M. A. (2009). Estimating standard errors in finance panel data sets: Comparing approaches. *The Review of Financial Studies*, 22(1), 435-480.

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

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, 101795.

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, 35(1), 155-186.

Wang, H. E., Wang, Q. E., & Wu, W. (2022). Short selling surrounding data breach announcements. *Finance Research Letters*, 47, 102690.

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

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems*, 33(3), 267-284.

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.

Yu, M. (2010). Analyst forecast properties, analyst following and governance disclosures: A global perspective. *Journal of International Accounting, Auditing and Taxation*, 19(1), 1-15.

Zhang, X. F. (2006). Information uncertainty and analyst forecast behavior. *Contemporary Accounting Research*, 23(2), 565-590.

Tables and Charts

Table 1 Sample Overview

This table illustrates the overview of the sample used in this study. Panel A presents the sample selection process, and Panel B shows the industry distribution of the breach firms used in this study.

Panel A: Sample Selection Process

Number of PRC breach events	20,161
Less:	
Government, NGO, and educational	(2,901)
Missing disclosure date	(306)
Ambiguous disclosure date	(588)
Duplicated events	(479)
Number of breach events without Compustat data	(15,011)
Financial firms	(316)
Number of PRC breach events remaining	560
Number of Audit Analytics breach events	1,151
Less:	
Number of breach events unmerged with Compustat	(301)
Overlapping events with the PRC database	(358)
Observations from the financial industry	(77)
Number of Audit Analytics breach events remaining	415
Breach events primary sample	975
Less:	
Repeated breach events	(182)
PRC and Audit Analytics unique breach firms	793
Less:	
Number of firms with no I/B/E/S data	(311)
Number of breach firms not matched in propensity score matching	(130)
Number of firms after propensity score matching (352 treatment + 352 control)	**704**
Number of firm-year observations	**3,828**

Panel B: Breach Firms Industry Distribution

Industry Description	**Firms**	**%**
Mining, utilities, and construction	19	5.40%
Manufacturing	127	36.08%
Wholesale, retail, and warehousing	62	17.61%
Information	68	19.32%
Real estate, professional services, and management	48	13.64%
Education and healthcare	8	2.27%
Recreation and entertainment	17	4.83%
Other services and unclassified	3	0.85%
Total	**352**	**100%**

Table 2 Descriptive Statistics

This table presents the descriptive statistics for the matched sample used in this study. There are 352 treatment and 352 control firms, respectively, from 2005 to 2022. Treatment and control firms are matched based on the same industry and in the same fiscal year. The sample is limited to an observation window of -3 years and +3 years of the breach events. This study ensures that firms have at least one observation in the pre- and post-breach periods Panel A reports the descriptive statistics for the whole sample. Panel B shows the descriptive statistics for the treatment and control firm years data, respectively. See Appendix A for variable definitions. To eliminate the outliers, all continuous variables are winsorized at the 1 percent and 99 percent levels.

Panel A: Whole Sample

Variable	N	Mean	S.D.	Min	Max
MEAN_ESTIMATES	3,828	2.147	2.817	-5.310	11.740
MEAN_REC	3,828	2.301	0.506	1	4
ANALYST	3,828	9.926	7.548	1	30
ROA	3,828	0.026	0.131	-2.482	0.326
SIZE	3,828	8.036	1.692	3.111	12.269
LEVERAGE	3,828	0.582	0.237	0.046	2.390
CASHFLOW	3,828	0.095	0.121	-1.574	0.513
SALES_GROWTH	3,828	0.148	0.350	-0.698	2.878
LOSS	3,828	0.224	0.417	0	1
TOBIN_Q	3,828	2.196	1.561	0.659	9.978

Panel B: Treatment Firm Years (352 Treatment Firms)

Variable	N	Mean	S.D.	Min	Max
MEAN_ESTIMATES	1,963	2.209	2.935	-5.310	11.740
MEAN_REC	1,963	2.313	0.491	1	4
ANALYST	1,963	10.736	7.888	1	30
ROA	1,963	0.027	0.119	-0.953	0.326
SIZE	1,963	8.044	1.713	3.111	12.269
LEVERAGE	1,963	0.581	0.230	0.056	2.144
CASHFLOW	1,963	0.093	0.118	-0.855	0.513
SALES_GROWTH	1,963	0.138	0.332	-0.698	2.878
LOSS	1,963	0.227	0.419	0	1
TOBIN_Q	1,963	2.214	1.526	0.659	9.978

Control Firm Years (352 Control Firms)

Variable	N	Mean	S.D.	Min	Max
MEAN_ESTIMATES	1,865	2.082	2.687	-5.310	11.740
MEAN_REC	1,865	2.288	0.521	1	4
ANALYST	1,865	9.075	7.076	1	30
ROA	1,865	0.025	0.142	-2.482	0.326
SIZE	1,865	8.027	1.671	3.168	12.197
LEVERAGE	1,865	0.584	0.245	0.046	2.390
CASHFLOW	1,865	0.097	0.125	-1.574	0.513
SALES_GROWTH	1,865	0.159	0.369	-0.698	2.878
LOSS	1,865	0.221	0.415	0	1
TOBIN_Q	1,865	2.178	1.597	0.659	9.978

Figure 1: Breach Disclosure Trend

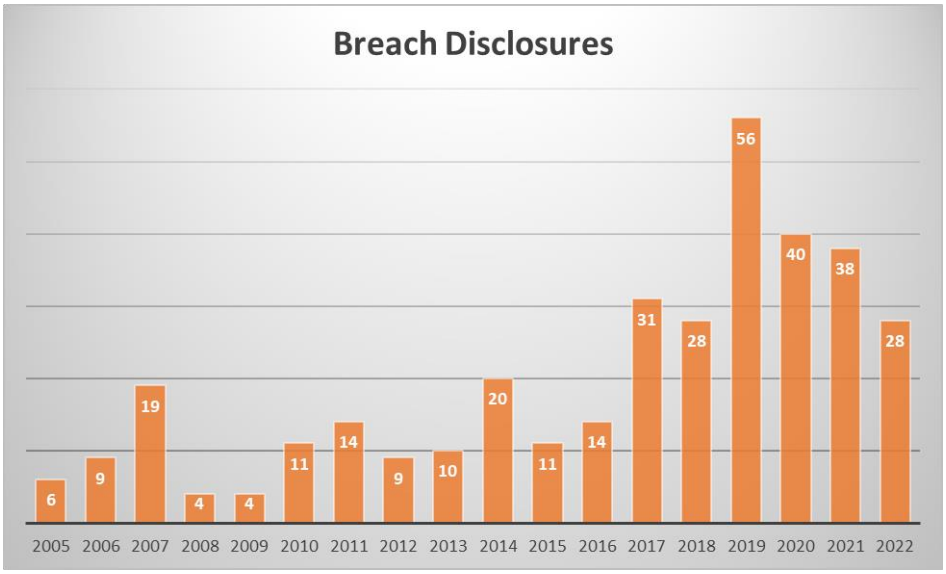

Table 3 Correlation Matrix

This table reposts the correlation matrix of the variables used in this study. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively, based on a two-tailed test. All continuous variables are winsorized at the 1 percent and 99 percent levels to eliminate the outliers.

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
(1) *TREATMENT*	1											
(2) *MEAN_ESTIMATES*	0.0194	1										
(3) *MEAN_REC*	0.0238	0.0167	1									
(4) *LOG_ANALYST*	0.1117***	0.2446***	0.0831***	1								
(5) *ROA*	0.0108	0.4577***	0.0162	0.1558***	1							
(6) *SIZE*	0.0152	0.3537***	0.0899***	0.4098***	0.2567***	1						
(7) *LEVERAGE*	-0.0055	0.0243	0.0540***	-0.0299*	-0.1093***	0.1974***	1					
(8) *CASHFLOW*	-0.0169	0.3575***	0.0742***	0.1902***	0.6627***	0.1866***	-0.0894***	1				
(9) *SALES_GROWTH*	-0.024	-0.0181	-0.2067***	0.0908***	-0.0837***	-0.1064***	-0.0763***	-0.1268***	1			
(10) *LOSS*	0.0079	-0.4712***	0.0333***	-0.1561***	-0.6237***	-0.2814***	0.0735***	-0.4658***	0.0437***	1		
(11) *TOBIN_Q*	0.0068	0.0145	-0.0533***	0.2055***	0.0982***	-0.2249***	-0.1112***	0.1733***	0.2481***	0.0113	1	
(12) *DISPERSION*	-0.0328**	0.0326**	-0.0267	-0.0596***	0.0786***	0.0004	-0.0233	0.0236	-0.0335***	-0.0644***	-0.0073	1

Table 4: Mean Comparison Test - Propensity Score Matching

This table presents the mean comparison test between treatment and control firms before and after the propensity score matching approach. Panel A shows the difference in the means between treatment and control firms before matching. Panel B presents the difference in the means between treatment and control one year before the breach incident after matching. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively, based on a two-tailed test.

Panel A: Differences in Characteristics of Treatment and Control Firms Before Matching

	Mean			Mean comparison	
Variable	**Treated**	**Control**	**Diff.**	**T-statistics**	**p-value**
ROA	0.040	-0.029	0.069***	-24.316	0.000
SIZE	8.169	6.811	1.358***	-58.800	0.000
LEVERAGE	0.582	0.504	0.079***	-23.334	0.000
CASHFLOW	0.109	0.046	0.064***	-23.883	0.000
SALES_GROWTH	0.140	0.187	-0.046***	8.062	0.000
LOSS	0.174	0.318	-0.144***	26.342	0.000
TOBIN_Q	2.269	2.162	0.107***	-5.273	0.000

Panel B: Differences in Characteristics of Treatment and Control Firms After Matching

	Mean			Mean comparison	
Variable	**Treated**	**Control**	**Diff.**	**T-statistics**	**p-value**
ROA	0.027	0.023	0.004	-0.467	0.641
SIZE	7.999	7.951	0.047	-0.376	0.707
LEVERAGE	0.577	0.582	-0.005	0.256	0.798
CASHFLOW	0.097	0.097	0.000	0.035	0.972
SALES_GROWTH	0.147	0.147	0.001	-0.021	0.972
LOSS	0.213	0.216	-0.003	0.092	0.927
TOBIN_Q	2.258	2.234	0.024	-0.195	0.845

Table 5: Relation between Cyber Breaches and Analyst Forecast Measures

This table presents the staggered DID analysis from Equation (3) to investigate cybersecurity breach disclosures' effect on analyst forecast measures. The outcome variables are proxied by *MEAN_ESTIMATES* and *MEAN_REC*. *TREAT* is a dummy variable that takes a value of 1 if the firm is a breach firm and zero otherwise. *POST* is a dummy variable that takes a value of 1 for observations during the post-breach period and zero otherwise. The variable of interest is the interaction term of *TREAT×POST*. Columns 1 to 3 present the results for *MEAN_ESTIMATES* and columns 4 to 6 present the results for *MEAN_REC*. The results are presented without any fixed effects, and with firm- and year-fixed effects, respectively. Robust standard errors are clustered at the industry-level. The t-statistics are reported in parentheses. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively (two-tailed test). The variables are defined in Appendix A.

	(1)	(2)	(3)	(4)	(5)	(6)
VARIABLES	***MEAN_ESTIMATES***			***MEAN_REC***		
TREAT*POST	**0.169***	**-0.249*****	**-0.249*****	**0.009**	**-0.012**	**-0.012**
	[1.902]	**[-3.224]**	**[-2.896]**	**[0.497]**	**[-0.570]**	**[-0.380]**
ROA	4.277***	2.527***	2.527***	-0.045	-0.079	-0.079
	[9.724]	[8.100]	[2.925]	[-0.488]	[-0.924]	[-0.575]
SIZE	0.293***	0.493***	0.493**	0.008	-0.021	-0.021
	[10.510]	[5.155]	[2.651]	[1.390]	[-0.809]	[-0.930]
LEVERAGE	0.487***	-0.302	-0.302	0.075**	0.165**	0.165
	[2.938]	[-1.131]	[-0.879]	[2.146]	[2.265]	[1.574]
CASHFLOW	1.396***	2.116***	2.116**	0.352***	0.050	0.050
	[3.290]	[5.828]	[2.822]	[3.936]	[0.505]	[0.664]
SALES_GROWTH	0.208*	0.507***	0.507*	-0.280***	-0.162***	-0.162***
	[1.834]	[5.586]	[2.000]	[-11.746]	[-6.503]	[-4.001]
LOSS	-1.777***	-1.243***	-1.243***	0.119***	0.089***	0.089***
	[-15.026]	[-14.354]	[-4.266]	[4.763]	[3.747]	[3.449]
LOG_ANALYST	0.302***	0.279***	0.279*	0.067***	-0.043	-0.043*
	[5.060]	[2.942]	[1.983]	[5.357]	[-1.639]	[-2.018]
TOBIN_Q	0.010	0.055*	0.055	-0.009	-0.053***	-0.053***
	[0.379]	[1.660]	[1.562]	[-1.485]	[-5.865]	[-3.322]
Constant	-1.078***	-2.364***	-2.364	2.047***	2.587***	2.587***
	[-4.711]	[-3.061]	[-1.428]	[42.472]	[12.234]	[10.110]
Firm FE	No	Yes	Yes	No	Yes	Yes
Year FE	No	Yes	Yes	No	Yes	Yes
Clustering	No	No	Industry	No	No	Industry
Observations	3,828	3,828	3,828	3,828	3,828	3,828
Adjusted R-squared	0.318	0.787	0.787	0.060	0.505	0.505

Figure 2: Parallel Trend Plot

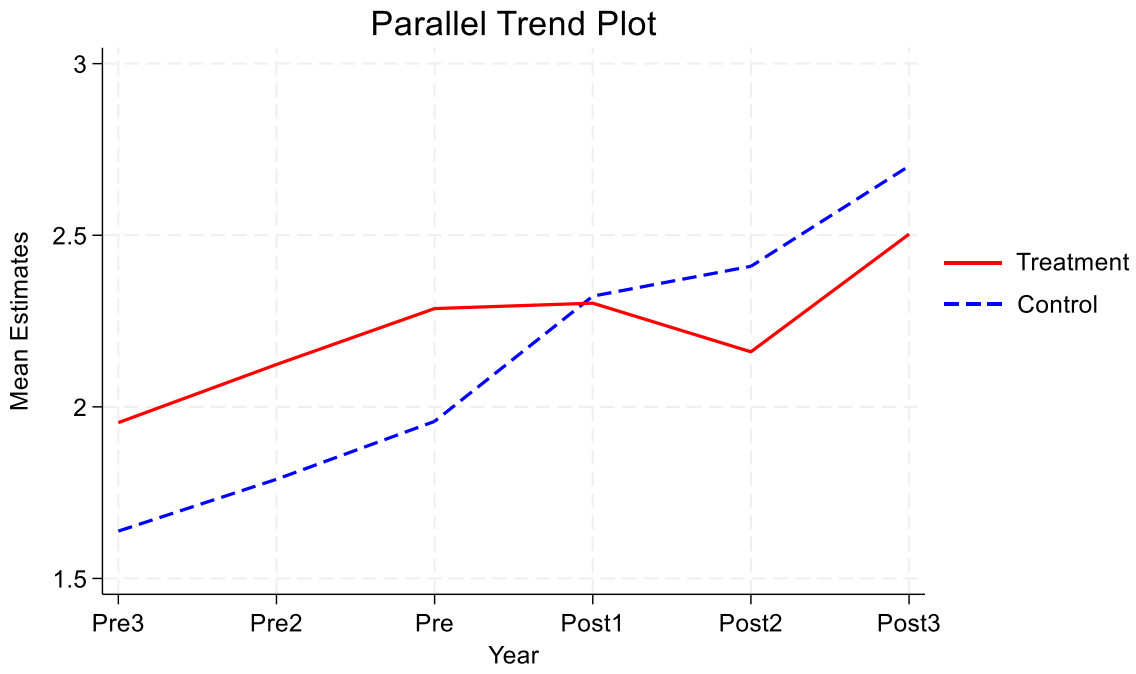

Table 6: Pre-treatment Test

This table presents the results of the effect of cybersecurity breach events on earnings forecast estimates with pre-treatment in Equation (4). The dependent variable is proxied by *MEAN_ESTIMATES. TREAT* is a dummy variable that takes a value of 1 if the firm is a breach firm and zero otherwise. *POST* is a dummy variable that takes a value of 1 for observations during the post-breach period and zero otherwise. *PRE* is a dummy variable that takes a value of 1 for observations one year before the breach incidents and zero otherwise. The variables of interest are the interaction terms of *TREAT*×*POST* and *TREAT*×*PRE*. The results are presented without any fixed effects, and with firm- and year-fixed effects, respectively. Robust standard errors are clustered at the industry-level. The t-statistics are reported in parentheses. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively (two-tailed test). The variables are defined in Appendix A.

	(1)	(2)	(3)
VARIABLES		***MEAN_ESTIMATES***	
TREAT*POST	**-0.381****	**-0.300*****	**-0.300****
	[-2.278]	**[-3.134]**	**[-2.328]**
TREAT*PRE	**-0.000**	**-0.023**	**-0.023**
	[-0.001]	**[-0.195]**	**[-0.229]**
ROA	4.259***	2.527***	2.527***
	[9.711]	[8.097]	[2.923]
SIZE	0.282***	0.494***	0.494**
	[10.053]	[5.156]	[2.650]
LEVERAGE	0.488***	-0.296	-0.296
	[2.954]	[-1.109]	[-0.869]
CASHFLOW	1.370***	2.107***	2.107**
	[3.238]	[5.798]	[2.837]
SALES_GROWTH	0.234**	0.510***	0.510*
	[2.069]	[5.607]	[2.035]
LOSS	-1.803***	-1.247***	-1.247***
	[-15.274]	[-14.383]	[-4.254]
LOG_ANALYST	0.309***	0.276***	0.276*
	[5.165]	[2.912]	[1.943]
TOBIN_Q	0.006	0.055*	0.055
	[0.200]	[1.676]	[1.576]
Constant	-1.295***	-2.417***	-2.417
	[-5.434]	[-3.119]	[-1.478]
Firm FE	No	Yes	Yes
Year FE	No	Yes	Yes
Clustering	No	No	Industry
Observations	3,828	3,828	3,828
Adjusted R-squared	0.322	0.787	0.787

Table 7: Time-series Placebo Test

This table presents the results from the time-series placebo test. The DID specification is based on Equation (3), and the model is re-run using a randomly assigned placebo period of minus three years in breach disclosure events for each individual firm. The outcome variables are proxied by *MEAN_ESTIMATES* and *MEAN_REC*. *TREAT* is a dummy variable that takes a value of 1 if the firm is a breach firm and zero otherwise. *POST* is a dummy variable that takes a value of 1 for observations during the post-breach period and zero otherwise. The variable of interest is the interaction term of *TREAT*×*POST*. Columns 1 to 3 present the results for *MEAN_ESTIMATES*, and columns 4 to 6 present the results for *MEAN_REC*. The results are presented without any fixed effects, and with firm- and year-fixed effects, respectively. Robust standard errors are clustered at the industry-level. The t-statistics are reported in parentheses. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively (two-tailed test). The variables are defined in Appendix A.

	(1)	(2)	(3)	(4)	(5)	(6)
VARIABLES	***MEAN_ESTIMATES***			***MEAN_REC***		
TREAT*POST	**0.047**	**0.074**	**0.074**	**0.040**	**0.031**	**0.031**
	[0.341]	**[0.985]**	**[0.733]**	**[1.181]**	**[1.143]**	**[1.138]**
ROA	4.349***	3.681***	3.681***	-0.068	-0.164	-0.164
	[8.861]	[10.264]	[4.949]	[-0.562]	[-1.269]	[-0.916]
SIZE	0.286***	0.588***	0.588***	0.009	-0.035	-0.035
	[11.118]	[6.307]	[5.384]	[1.344]	[-1.035]	[-0.914]
LEVERAGE	0.457***	-0.204	-0.204	0.050	-0.017	-0.017
	[3.054]	[-0.850]	[-0.876]	[1.350]	[-0.198]	[-0.126]
CASHFLOW	0.827**	2.989***	2.989***	0.446***	0.101	0.101
	[1.966]	[8.778]	[5.637]	[4.303]	[0.827]	[0.707]
SALES_GROWTH	-0.104	0.250***	0.250	-0.296***	-0.135***	-0.135*
	[-0.987]	[3.125]	[1.111]	[-11.350]	[-4.693]	[-1.788]
LOSS	-1.388***	-0.583***	-0.583***	0.127***	0.122***	0.122***
	[-12.048]	[-7.047]	[-4.186]	[4.483]	[4.096]	[4.925]
LOG_ANALYST	0.304***	0.327***	0.327***	0.091***	0.001	0.001
	[5.576]	[3.947]	[3.221]	[6.744]	[0.042]	[0.044]
TOBIN_Q	-0.012	0.076**	0.076	-0.019***	-0.088***	-0.088***
	[-0.470]	[2.188]	[0.975]	[-2.852]	[-7.097]	[-5.286]
Constant	-1.347***	-3.850***	-3.850***	2.053***	2.799***	2.799***
	[-6.279]	[-5.132]	[-4.619]	[38.815]	[10.377]	[9.942]
Firm FE	No	Yes	Yes	No	Yes	Yes
Year FE	No	Yes	Yes	No	Yes	Yes
Clustering	No	No	Industry	No	No	Industry
Observations	3,458	3,458	3,458	3,458	3,458	3,458
Adjusted R-squared	0.311	0.813	0.813	0.071	0.462	0.462

Table 8: Post-periods Analysis

This table presents the staggered DID analysis from Equation (5) to investigate the effect of cybersecurity breach disclosures on analysts' earnings estimates. The dependent variable is proxied by *MEAN_ESTIMATES*. *TREAT* is a dummy variable that takes a value of 1 if the firm is a breach firm and zero otherwise. *POST1* is a dummy variable that takes a value of 1 for the first year following the breach disclosure and zero otherwise. *POST2* is a dummy variable that takes a value of 1 for the second year following the breach disclosure and zero otherwise. *POST3* is a dummy variable that takes a value of 1 for the third year following the breach disclosure and zero otherwise. The main coefficients of interest are the three interaction terms: *TREAT×POST1*, *TREAT×POST2* and *TREAT×POST3*. The results are presented without any fixed effects, and with firm- and year-fixed effects, respectively. Robust standard errors are clustered at the industry-level. The t-statistics are reported in parentheses. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively (two-tailed test). The variables are defined in Appendix A.

	(1)	(2)	(3)
VARIABLES		***MEAN_ESTIMATES***	
TREAT_POST1	**-0.311**	**-0.297****	**-0.297****
	[-1.505]	**[-2.545]**	**[-2.487]**
TREAT_POST2	**-0.396***	**-0.307****	**-0.307****
	[-1.808]	**[-2.448]**	**[-2.098]**
TREAT_POST3	**-0.458***	**-0.266****	**-0.266**
	[-1.949]	**[-1.961]**	**[-1.463]**
ROA	4.244***	2.519***	2.519***
	[9.669]	[8.069]	[4.344]
SIZE	0.282***	0.492***	0.492***
	[10.067]	[5.139]	[3.259]
LEVERAGE	0.490***	-0.291	-0.291
	[2.966]	[-1.089]	[-0.775]
CASHFLOW	1.384***	2.116***	2.116***
	[3.267]	[5.817]	[3.145]
SALES_GROWTH	0.230**	0.510***	0.510***
	[2.033]	[5.608]	[3.018]
LOSS	-1.801***	-1.248***	-1.248***
	[-15.249]	[-14.390]	[-7.759]
LOG_ANALYST	0.308***	0.278***	0.278***
	[5.142]	[2.929]	[2.752]
TOBIN_Q	0.006	0.056*	0.056
	[0.234]	[1.677]	[1.334]
Constant	-1.232***	-2.388***	-2.388*
	[-5.263]	[-3.084]	[-1.935]
Firm FE	No	Yes	Yes
Year FE	No	Yes	Yes
Clustering	No	No	Industry
Observations	3,828	3,828	3,828
Adjusted R-squared	0.321	0.787	0.787

Table 9: Subsample Analysis - High versus Low Information Transparency

This table presents the additional subsample analysis based on the staggered DID analysis from Equation (3) to investigate the effect of breach disclosures on earnings forecast estimates between high and low transparency subsamples. The dependent variable is proxied by *MEAN_ESTIMATES*. The variable of interest is the interaction term of *TREAT×POST* which measures treatment firms in the post-disclosure period. The results are presented without any fixed effects, and with firm- and year-fixed effects, respectively. Robust standard errors are clustered at the industry-level. Columns 1 to 3 present the results in the high information transparency sample, and columns 4 to 6 report the results in the low information transparency sample. The t-statistics are reported in parentheses. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively (two-tailed test). The variables are defined in Appendix A.

	High Transparency				**Low Transparency**		
	(1)	(2)	(3)		(4)	(5)	(6)
VARIABLES	***MEAN_ESTIMATES***				***MEAN_ESTIMATES***		
TREAT*POST	**0.020**	**-0.264****	**-0.264****	***TREAT*POST***	**0.362*****	**-0.154**	**-0.154**
	[0.144]	**[-2.456]**	**[-2.149]**		**[3.243]**	**[-1.365]**	**[-1.117]**
ROA	6.163***	3.336***	3.336**	*ROA*	3.821***	2.337***	2.337*
	[8.024]	[7.430]	[2.696]		[7.512]	[5.409]	[1.956]
SIZE	0.378***	0.859***	0.859**	*SIZE*	0.304***	0.450***	0.450
	[7.975]	[6.001]	[2.817]		[9.517]	[3.357]	[1.367]
LEVERAGE	0.884***	-1.400***	-1.400	*LEVERAGE*	0.091	-0.058	-0.058
	[3.076]	[-2.975]	[-1.530]		[0.486]	[-0.166]	[-0.175]
CASHFLOW	4.440***	4.938***	4.938**	*CASHFLOW*	0.201	0.802*	0.802**
	[5.724]	[7.435]	[2.464]		[0.419]	[1.754]	[2.303]
SALES_GROWTH	0.449**	0.948***	0.948	*SALES_GROWTH*	0.245*	0.243**	0.243
	[2.237]	[6.330]	[1.560]		[1.919]	[2.069]	[1.012]
LOSS	-1.899***	-1.355***	-1.355***	*LOSS*	-1.477***	-1.033***	-1.033***
	[-8.824]	[-9.569]	[-3.369]		[-11.081]	[-9.100]	[-4.271]
TOBIN_Q	-0.037	0.044	0.044	*TOBIN_Q*	0.067*	0.149***	0.149**
	[-0.877]	[0.955]	[1.051]		[1.902]	[2.937]	[2.397]
Constant	-1.483***	-4.593***	-4.593	Constant	-0.639**	-1.852*	-1.852
	[-3.098]	[-3.468]	[-1.740]		[-2.339]	[-1.817]	[-0.783]
Firm FE	No	Yes	Yes	Firm FE	No	Yes	Yes
Year FE	No	Yes	Yes	Year FE	No	Yes	Yes
Clustering	No	No	Industry	Clustering	No	No	Industry
Observations	1,794	1,794	1,794	Observations	2,034	2,034	2,034
Adjusted R-squared	0.292	0.840	0.840	Adjusted R-squared	0.310	0.727	0.727

Table 10: Subsample Analysis – Forecast Dispersion

This table presents the additional subsample analysis to investigate the effect of breach disclosures on analyst dispersions between high and low transparency subsamples. The dependent variable is proxied by *DISPERSION*. The variable of interest is the interaction term of *TREAT×POST* which measures the treatment firms in the post-disclosure period. The results are presented without any fixed effects, and with firm- and year-fixed effects, respectively. Robust standard errors are clustered at the industry-level. Columns 1 to 3 present the results in the high information transparency sample, and columns 4 to 6 report the results in the low information transparency sample. The t-statistics are reported in parentheses. ***, **, and * are significant at 1%, 5%, and 10% confidence levels, respectively (two-tailed test). The variables are defined in Appendix A.

	High Transparency				**Low Transparency**	
	(1)	(2)	(3)		(4)	(5)	(6)
VARIABLES	***DISPERSION***				***DISPERSION***		
TREAT*POST	-0.030*	-0.058**	-0.058**	***TREAT*POST***	-0.061*	-0.051	-0.051
	[-1.862]	[-2.206]	[-2.633]		[-1.943]	[-0.979]	[-1.380]
ROA	0.474***	0.703***	0.703***	*ROA*	0.192	0.275	0.275**
	[5.251]	[6.428]	[4.183]		[1.265]	[1.312]	[2.343]
SIZE	-0.003	0.058*	0.058	*SIZE*	0.006	0.078	0.078
	[-0.577]	[1.666]	[1.023]		[0.682]	[1.275]	[1.320]
LEVERAGE	-0.034	0.144	0.144	*LEVERAGE*	-0.034	0.147	0.147
	[-1.008]	[1.258]	[0.642]		[-0.641]	[0.910]	[1.236]
CASHFLOW	-0.357***	-0.436***	-0.436	*CASHFLOW*	-0.091	-0.079	-0.079
	[-3.919]	[-2.692]	[-1.317]		[-0.666]	[-0.378]	[-0.721]
SALES_GROWTH	-0.016	0.039	0.039	*SALES_GROWTH*	-0.053	-0.099*	-0.099*
	[-0.669]	[1.076]	[1.190]		[-1.519]	[-1.863]	[-1.978]
LOSS	-0.073***	-0.094***	-0.094	*LOSS*	-0.018	0.016	0.016
	[-2.884]	[-2.713]	[-1.240]		[-0.458]	[0.301]	[0.218]
TOBIN_Q	0.014***	0.032***	0.032	*TOBIN_Q*	-0.014	0.002	0.002
	[2.829]	[2.785]	[1.638]		[-1.514]	[0.086]	[0.148]
Constant	0.065	-0.624*	-0.624	Constant	0.084	-0.587	-0.587
	[1.147]	[-1.930]	[-1.009]		[1.055]	[-1.255]	[-1.159]
Firm FE	No	Yes	Yes	Firm FE	No	Yes	Yes
Year FE	No	Yes	Yes	Year FE	No	Yes	Yes
Clustering	No	No	Industry	Clustering	No	No	Industry
Observations	1,779	1,779	1,779	Observations	1,730	1,730	1,730
Adjusted R-squared	0.039	0.087	0.087	Adjusted R-squared	0.005	0.032	0.032

Appendix A

Variables	Definition of variables
MEAN_ESTIMATES	The average EPS estimate for firm *i* obtained from I/B/E/S
MEAN_REC	The average stock recommendation firm *i* obtained from I/B/E/S
ANALYST	The total number of analysts following
LOG_ANALYST	The natural logarithm of one plus the total number of analysts following
ROA	Compustat net income divided by total assets
SIZE	Natural logarithm of total assets
LEVERAGE	The total liabilities divided by total assets
CASHFLOW	Cashflows from operations for year *t*, divided by total assets at the beginning of the year.
SALES_GROWTH	The net sales in period t divided by net sales in period t-1
LOSS	An indicator variable that takes the value of 1 if the firm makes a loss in the fiscal year and zero otherwise
TOBIN_Q	The sum of market capitalization and the book value of debt divided by the book value of total assets
TREAT	A dummy variable that takes a value of one if the firm is a treatment and zero otherwise
POST	A dummy variable that takes a value of one during the post-disclosure period and zero otherwise
POST1	A dummy variable that takes a value of one for the first year following the breach disclosure and zero otherwise
POST2	A dummy variable that takes a value of one for the second year following the breach disclosure and zero otherwise
POST3	A dummy variable that takes a value of one for the third year following the breach disclosure and zero otherwise
PRE	A dummy variable that takes a value of one if the period is one year before the breach disclosure and zero otherwise
DISPERSION	The standard deviation of the analysts' forecast estimates scaled by the mean forecast