

Cyber Attacks and Non-GAAP Earnings Disclosure

Encarna Guillamon Saorin
University Carlos III de Madrid

Yiwei Li
Essex University

Xiaohui Liu
University of Adelaide

Xiu-Ye Zhang
Australian National University

Abstract

We examine whether firms' use of non-GAAP earnings disclosures changes following cyberattacks. Using a large panel of firm-quarter observations, we find that firms are less likely to disclose non-GAAP earnings in attack periods. Cross-sectional tests indicate that this decline is concentrated among firms subject to stronger external monitoring, including higher institutional ownership, greater analyst following, and more independent boards, and among firms with greater financial slack. The effect is also stronger when cyber risks are more likely to persist, including firms with higher ex ante cyber risk and firms experiencing repetitive attacks. Consistent with managerial concerns about scrutiny and legal exposure, the decline is more pronounced for firms with higher-ability CEOs, MBA CEOs, and firms in high-litigation industries. This is further corroborated by the evidence that attacked firms that disclose non-GAAP earnings exhibit weaker subsequent operating performance relative to attacked firms that do not disclose non-GAAP measures. Overall, our findings provide implications for information users that whether or not disclosing the non-GAAP measures may reflect strategic restraint under heightened scrutiny rather than reduced demand for performance explanations.

Key words

Cyber attacks; non-GAAP earnings disclosure; external monitoring; financial constraints

1. Introduction

The growing use of digital technologies has increased firms' vulnerability to cybersecurity threats, which in turn can severely affect stakeholder trust (Amir et al., 2018; Kamiya et al., 2021). Consistent with these concerns, successful cyberattacks carry significant reputational costs, including stock price declines triggered by breaches often exceed the direct financial losses incurred (Gordon et al., 2010; Li et al., 2018). Thus, when a firm suffers a major data breach, investors react not only to remediation expenses or fines, but also to the broader credibility damage inflicted on the firm (Spanos & Angelis, 2016; Berkman et al., 2018). Managers, in turn, face pressure to restore confidence in the aftermath of such events. Indeed, firms that take visible remedial actions following a cyber incident (e.g., strengthening security or leadership changes) tend to mitigate some negative consequences, such as receiving less severe penalties in subsequent financing terms (Huang & Wang, 2021; Smith et al., 2018). This suggests that managers have strong incentives to respond proactively in their communications and disclosures after a cyberattack, aiming to reassure stakeholders and repair the firm's reputation (Gordon et al., 2006; Wang et al., 2013; Curtis et al., 2018).

Cybersecurity breaches have become a recurring negative shock for public firms. Beyond direct remediation expenditures, cyberattacks can disrupt operations, increase uncertainty about future cash flows, and create reputational costs that intensify external scrutiny by investors, analysts, and regulators. These features make cyberattacks a setting in which managers face an acute disclosure tradeoff. Managers have incentives to explain performance implications to outside investors, yet they also face potential costs if discretionary disclosures are perceived as opportunistic or misleading (Healy and Palepu 2001; Verrecchia 2001). Prior evidence indicates that managers do not always fully disclose cyber incidents and that capital markets respond to cyberattack information, consistent with meaningful informational frictions and incentive conflicts in this setting (Amir, Levi, and Livne 2018; Kamiya et al. 2021).

Non-GAAP earnings disclosures are a salient channel through which managers communicate performance in earnings announcements. Non-GAAP reporting is widespread and can be informative when it helps users separate transitory items from recurring performance. At the same time, managers have discretion in defining adjustments and prior research documents that non-GAAP measures can be used strategically, particularly around benchmarks and periods of heightened incentives (Lougee and Marquardt 2004; Kolev,

Marquardt, and McVay 2008; Heflin and Hsu 2008; Doyle, Jennings, and Soliman 2013; Leung and Veenman 2018). Recent work also highlights that regulatory scrutiny and constraints on non-GAAP presentation affect firms' disclosure choices and information environments (Gomez, Heflin, and Wang 2023). Despite extensive evidence on the determinants and consequences of non-GAAP reporting, there is limited evidence on how an operational and reputational shock such as a cyberattack affects managers' propensity to provide non-GAAP earnings.

Our paper examines whether firms change their use of non-GAAP earnings following cyberattacks. Conceptually, cyberattacks can increase the demand for performance explanations, which would predict greater use of non-GAAP measures to isolate breach-related costs. An alternative prediction is that cyberattacks increase perceived litigation and reputational risk, which can make discretionary performance measures more costly when managers anticipate stronger scrutiny over adjustments and classification choices (McVay 2006; Gomez et al. 2023). Under this second view, managers reduce non-GAAP disclosures after a cyberattack to limit exposure to criticism that adjustments are opportunistic or obscure economic performance.

Using a large panel of U.S. firm-quarter observations and a standard set of firm characteristics and fixed effects, we find consistent evidence that firms are less likely to disclose non-GAAP earnings following a cyberattack consistent with managers pulling back on discretionary performance reporting after a cybersecurity breach. We then examine cross-sectional variation to assess whether monitoring and incentives shape the reporting response. Our results show that the post-attack reduction in non-GAAP disclosure is more pronounced when governance and external monitoring are stronger. This pattern is consistent with monitoring limiting managers' use of discretionary non-GAAP reporting in periods when scrutiny is elevated (Kolev et al. 2008; Frankel, McVay, and Soliman 2011; Gomez et al. 2023).

We also show heterogeneity based on firms' financial condition. Specifically, our results suggest that the post-attack reduction in non-GAAP reporting is concentrated among firms with greater capacity to absorb the shock without relying on more aggressive performance presentation. The findings align with evidence that reporting choices reflect both disclosure incentives and the constraints faced by managers in stressed settings (Healy and Palepu 2001; Doyle et al. 2013).

Our robustness analyses reinforce the main inferences. Finally, we investigate whether non-GAAP disclosure after cyberattacks is associated with subsequent operating outcomes. The evidence from our findings is consistent with the interpretation that, conditional on a cyberattack, firms choosing to issue non-GAAP measures have weaker subsequent fundamentals, which aligns with concerns that some non-GAAP adjustments reflect performance pressures rather than purely transitory items (Doyle et al. 2013; Leung and Veenman 2018).

Our study contributes to two core literatures. First, it extends research on non-GAAP reporting by identifying cybersecurity breaches as an economically meaningful shock that affects managers' voluntary performance communication, and by documenting systematic heterogeneity based on monitoring, financial slack, and legal concerns (Kolev et al. 2008; Heflin and Hsu 2008; Gomez et al. 2023). Second, it contributes to the cybersecurity and disclosure literature by providing evidence on how cyberattacks influence earnings announcement disclosure choices, complementing work on underreporting and capital market consequences of cyber incidents (Amir et al. 2018; Florackis et al. 2023; Kamiya et al. 2021). The results also have implications for users assessing earnings announcements in the aftermath of cyber incidents, where the absence of non-GAAP measures may reflect strategic restraint under heightened scrutiny rather than reduced demand for performance explanations.

2. Literature Review and Hypothesis Development

2.1 Non-GAAP Reporting: Dual Perspectives on Managerial Motives

Research on non-GAAP earnings reporting offers two competing perspectives. One view holds that managers use non-GAAP adjustments to communicate more useful information about the firm's core operations by excluding items deemed non-recurring or non-operational. By removing transitory charges (e.g., restructuring costs, one-time write-downs), the resulting pro forma earnings measure can better reflect sustainable profitability and thus improve the informativeness of financial reports. For instance, Bhattacharya et al. (2003) find that market participants perceive non-GAAP "pro forma" earnings to be more persistent and representative of future performance than GAAP earnings. Similarly, firms often justify non-GAAP exclusions as helping users focus on what management considers the true ongoing earnings capacity of the business. In short, under this perspective, non-GAAP disclosures can enhance transparency and aid investors' decision-making by filtering out noise from GAAP results.

In contrast, the opposing view argues that non-GAAP reporting is frequently used opportunistically to mislead or confuse investors. Managers have wide discretion in defining what to exclude as “non-recurring,” and in the absence of uniform standards or audit requirements, some firms might exploit non-GAAP metrics to portray overly optimistic results. Regulators have long cautioned that non-GAAP figures can be misused; for example, the SEC’s 2001 guidance (“Pro Forma Financial Information: Tips for Investors,” Release No. 33-8039) warned that certain pro forma earnings disclosures can be misleading if they lack clear explanation or consistency. In line with this concern, Kolev, Marquardt, and McVay (2008) document that prior to regulatory intervention in 2003, companies often included questionable adjustments in non-GAAP earnings – such as excluding recurring expenses – to boost apparent performance. More recent studies continue to find instances of aggressive non-GAAP reporting. Govindarajan, Srivastava, and Zhao (2021) report that from 2010 to 2019, nearly one-fifth of firms reporting a GAAP net loss managed to turn the loss into a positive profit by using non-GAAP adjustments. High-profile examples underscore this pattern: for the fiscal year 2019, Pinterest disclosed a non-GAAP profit of \$17 million despite a GAAP loss of \$1.36 billion, achieved by excluding certain costs. Such evidence highlights how non-GAAP metrics can serve as a tool for earnings manipulation and impression management (Bhattacharya et al., 2003; Frankel et al., 2011). Thus, the literature presents a dual characterization of non-GAAP reporting – it can improve the relevance of earnings information, but it also carries the risk of obscuring economic reality when used in bad faith.

2.2 Cybersecurity Breaches and Managerial Disclosure Incentives

Cyberattacks represent extreme adverse events that test firms’ reputational capital and stakeholder trust. When companies are victimized by hackers, they often experience sharp declines in investor confidence and face costly aftermaths. Prior studies consistently document severe reputational losses and increased external financing costs following cyber incidents (Huang & Wang, 2021; Liu et al., 2025). For example, Kamiya et al. (2021) find that announcements of successful cyberattacks are associated with significant negative abnormal stock returns, and the loss in shareholder value greatly exceeds the direct out-of-pocket costs of the breaches – indicating substantial reputational damage. Beyond immediate market impacts, cyber incidents can impair a firm’s access to capital. Huang and Wang (2021) show that breached firms subsequently incur higher bank loan spreads and tougher loan contract terms, reflecting lenders’ heightened risk perceptions. Likewise, recent evidence suggests that

firms are less likely to raise equity following a cyberattack, attributable to increased adverse selection and investor wariness post-breach (Liu et al., 2025). Managers themselves may face personal and professional consequences in the wake of a breach, such as leadership turnover or intensified scrutiny from boards and regulators (Huang & Wang, 2021). These repercussions create strong incentives for managers to engage in crisis management aimed at regaining stakeholder confidence. Prior work documents that firms taking more extensive remedial actions after a data breach (for example, improving cybersecurity governance or replacing key executives) tend to lessen the long-term fallout of the breach. In essence, when a cyberattack strikes, managers are under pressure to control the narrative and convince stakeholders that the firm remains fundamentally sound and in command of the situation.

Managers can influence stakeholder perceptions is through financial disclosures. In the context of a cyber crisis, the firm's quarterly earnings announcements and related communications become an important platform to address concerns. Managers must decide whether to acknowledge the costs and disruptions caused by the attack or to downplay them. This is where non-GAAP earnings reporting could play a role. Following a cyberattack, a firm might incur various unusual expenses – for example, investigation and remediation costs, customer notification expenditures, litigation and regulatory penalties, or even lost revenues due to reputational harm. Managers could choose to highlight these impacts in their disclosures, or they might recast these costs as one-time charges that are excluded from an adjusted earnings figure. Because non-GAAP metrics are by definition flexible, managers can use them either to increase transparency (by clearly separating the one-off breach-related losses from the firm's core earnings) or to engage in obfuscation (by opportunistically excluding not just the breach costs but possibly other expenses under the guise of “non-recurring” items). Indeed, managers frequently use non-GAAP earnings to influence investor perception (Bhattacharya et al., 2003; Doyle et al., 2013). A recent real-world example illustrates this phenomenon: in 2024, UnitedHealth Group experienced a significant cyberattack that affected its operations. In reporting its financial results, UnitedHealth presented an adjusted earnings-from-operations figure that explicitly excluded the direct response costs of the cyberattack, labeling those costs as external impacts not reflective of ongoing performance. This disclosure was ostensibly an attempt to reassure investors that aside from the unusual breach-related expenses, the company's core profitability remained intact. The UnitedHealth case underscores how managers can deploy non-GAAP adjustments in the aftermath of a cyber incident – ostensibly to clarify performance by removing the noise introduced by the attack.

At the same time, employing non-GAAP adjustments after a breach is not without risks. Stakeholders may view such exclusions skeptically, worrying that managers are trying to mask the true impact of the incident. The heightened attention from regulators, auditors, and investors on a breached firm could mean any aggressive or unjustified non-GAAP reporting would be quickly noticed and penalized. Thus, cyber crises create a disclosure dilemma for managers: should they use non-GAAP metrics to help tell a “better” earnings story, or should they stick to GAAP results to avoid further credibility loss?

2.3 Competing Theories and Hypothesis Development

Non-GAAP earnings disclosures can either improve the communication of firms’ underlying performance or reflect opportunistic attempts to shape investor perceptions (Healy and Palepu 2001; Verrecchia 2001). Prior research shows that managers are more likely to report non-GAAP earnings when GAAP performance is temporarily depressed and when doing so facilitates meeting or beating salient benchmarks (Lougee and Marquardt 2004; Doyle, Jennings, and Soliman 2013). Applied to cyberattacks, this view implies an information substitution mechanism. If breach-related costs are perceived as unusual and non-recurring, managers may use non-GAAP measures to separate transitory incident costs from recurring operating performance, thereby reducing investor overreaction and supporting valuation.

A competing view emphasizes that cyberattacks increase scrutiny, credibility concerns, and expected litigation and regulatory costs, which can discipline discretionary reporting choices. Cyber incidents are salient reputation shocks that heighten stakeholder skepticism and can trigger regulatory attention and private litigation risk (Skinner 1994; Rogers and Van Buskirk 2009). This disciplining channel is particularly relevant for non-GAAP reporting, where regulators have historically intervened when exclusions appear aggressive or inconsistent (Heflin and Hsu 2008; Kolev, Marquardt, and McVay 2008), and where SEC oversight can alter firms’ incentives to provide prominent non-GAAP performance presentations (Gomez, Heflin, and Wang 2023). In addition, evidence from the cybersecurity literature indicates that cyber risk is economically meaningful, persistent, and priced, which can further limit managers’ ability to credibly characterize breach consequences as purely transitory (Kamiya et al. 2020; Florackis et al. 2023). Consistent with this perspective, managers may avoid discretionary performance measures after a cyberattack to reduce the probability that stakeholders interpret exclusions as obfuscation.

We expect the scrutiny and credibility channel to dominate following cyberattacks in the U.S. setting, leading firms to reduce their reliance on non-GAAP earnings disclosures.

H1 (Conservative Disclosure Hypothesis): Firms are less likely to disclose non-GAAP earnings in periods following a cyberattack.

Our empirical results also motivate cross-sectional predictions consistent with the scrutiny-based mechanism. First, monitoring and governance can amplify the expected costs of discretionary reporting because external parties are more likely to detect and challenge aggressive exclusions. Prior work links monitoring and governance to the quality and use of non-GAAP reporting, including evidence that weaker oversight is associated with more opportunistic exclusions (Frankel, McVay, and Soliman 2011) and that SEC interventions are more likely in settings characterized by complex disclosure choices and active information intermediaries (Gomez et al. 2023). Accordingly, the post-attack reduction in non-GAAP disclosure should be stronger when external monitoring and governance are higher.

Second, we expect financial slack to condition the response. When firms are financially unconstrained, managers have less need to rely on discretionary disclosure to support near-term financing or to manage performance narratives for capital market access. Survey evidence indicates that managers perceive strong market penalties to missing benchmarks and therefore manage reporting and disclosure when incentives are high (Graham, Harvey, and Rajgopal 2005). Following a cyberattack, financially unconstrained firms may be better positioned to accept GAAP-reported consequences without resorting to potentially controversial adjustments, implying a stronger reduction in non-GAAP disclosure among high-slack firms.

Third, cyber risk persistence should matter. If stakeholders view attacks as more likely to recur, or if firms experience repeated attacks, managers face greater difficulty credibly labeling incident-related costs as one-time. Cyber risk measures based on firms' disclosures are strongly related to subsequent realized cyber events, and the market prices this risk (Florackis et al. 2023). This persistence increases skepticism toward exclusions and increases the reputational costs of discretionary reporting, implying a larger post-attack pullback when future attack likelihood is higher or attacks repeat.

Finally, managerial incentives and personal exposure to scrutiny can further shape disclosure choices. Litigation risk affects managers' disclosure behavior (Skinner 1994; Rogers

and Van Buskirk 2009), and managerial characteristics meaningfully influence corporate policies (Bertrand and Schoar 2003). Managers with greater perceived ability or sophistication may be particularly sensitive to the credibility consequences of controversial disclosure after a cyber incident (Demerjian, Lev, and McVay 2012), strengthening the conservative response.

In addition to explaining the average reduction in non-GAAP disclosure, these mechanisms imply that the subset of attacked firms that continue to report non-GAAP earnings may differ systematically. Prior work shows that expenses excluded from pro forma earnings can predict lower future cash flows, indicating that exclusions are not always transitory (Doyle, Lundholm, and Soliman 2003), and that governance is associated with the persistence and quality of non-GAAP exclusions (Frankel et al. 2011). In the cyberattack setting, continued use of non-GAAP reporting may therefore identify firms with weaker underlying fundamentals or more persistent economic effects from the incident. We examine this implication in our analyses of post-attack operating performance.

3. Research Design

3.1 Baseline test of H1

To test whether firms reduce non-GAAP earnings disclosure following a cyberattack, we estimate a firm-quarter model in which the dependent variable, **NonGAAPdum**, equals one when the firm discloses a non-GAAP earnings measure in its periodic earnings communication and zero otherwise. Consistent with the binary nature of the outcome, our primary specifications estimate a limited dependent variable model of the form:

$$\Pr(\text{NonGAAPdum}_{i,t}=1) = F(\beta_1 \text{Attack}_{i,t} + \Gamma'X_{i,t} + \delta_j + \lambda_t) \quad (1)$$

where $F(\cdot)$ is the logistic (or probit) link function, Attack indicator for firm-quarters in the post-incident period (including the quarter of the disclosed cyberattack), $X_{i,t}$ is a vector of time-varying firm controls, δ_j denotes industry fixed effects, and λ_t denotes year-quarter fixed effects. We cluster standard errors at the firm level to account for within-firm serial dependence.

The baseline control set follows the non-GAAP disclosure literature and includes standard determinants of disclosure and performance presentation choices. Prior work documents that non-GAAP reporting is more prevalent among larger firms and among firms

with stronger performance incentives and disclosure demands (Bhattacharya et al. 2003; Doyle, Jennings, and Soliman 2013; Brown, Huffman, and Cohen 2023). We therefore control for firm size, growth opportunities, recent performance, and other firm characteristics used in the main tables. In augmented specifications, we add CEO-level characteristics and incentive measures that capture cross-sectional differences in managerial reporting preferences (Bertrand and Schoar 2003) and equity-based incentives (Core and Guay 2002; Coles, Daniel, and Naveen 2006).

The coefficient of interest is β_1 . Under the conservative disclosure hypothesis, we expect $\beta_1 < 0$, consistent with managers avoiding potentially controversial adjusted performance measures when scrutiny and reputational stakes increase.

3.2 Cross-sectional tests

The baseline model identifies the average effect of cyberattacks on non-GAAP disclosure. Our study investigates whether this effect varies in predictable ways consistent with a scrutiny and credibility mechanism.

3.2.1 Corporate governance and external monitoring

Stronger governance and monitoring can increase the expected costs of discretionary reporting by improving detection and facilitating challenge by boards, investors, and information intermediaries. Prior studies link monitoring to non-GAAP reporting choices and the aggressiveness of exclusions, and they show that regulatory oversight and intermediary attention shape non-GAAP presentation incentives (Frankel, McVay, and Soliman 2011; Christensen et al. 2019; Gomez, Heflin, and Wang 2023). We therefore estimate:

$$\Pr(\text{NonGAAPdum}_{i,t} = 1) = F(\beta_1 \text{Attack}_{i,t} + \beta_2 \text{Monitor}_{i,t} + \beta_3 (\text{Attack}_{i,t} \times \text{Monitor}_{i,t}) + \Gamma' X_{i,t} + \delta_j + \lambda t) \quad (2)$$

where Monitor denotes governance and monitoring proxies (for example, institutional monitoring, analyst scrutiny, and board oversight measures). The incremental effect of cyberattacks under stronger monitoring is captured by β_3 . We predict $\beta_3 < 0$, indicating a stronger post-attack pullback when oversight is higher.

3.2.2 Financial slack

We analyse whether the disclosure response depends on firms' financing capacity. The underlying intuition is that financially unconstrained firms face less pressure to manage performance narratives for near-term capital market access, particularly after a credibility shock. Survey evidence indicates that disclosure choices respond to perceived capital market consequences and benchmarking concerns (Graham, Harvey, and Rajgopal 2005). We operationalize slack using two standard proxies: Altman's Z-score (Altman 1968) and the Whited–Wu index (Whited and Wu 2006), and estimate interaction models that mirror the Table 3 structure.

Specifically, we define an indicator for high slack (or low constraint) and interact it with Attack:

$$\Pr(\text{NonGAAPdum}_{i,t} = 1) = F(\beta_1 \text{Attack}_{i,t} + \beta_2 \text{SlackDummy}_{i,t} + \beta_3 (\text{Attack}_{i,t} \times \text{SlackDummy}_{i,t}) + \Gamma' X_{i,t} + \delta_j + \lambda t) \quad (3)$$

A negative β_3 is consistent with a larger post-attack reduction in non-GAAP disclosure among firms with greater slack.

3.2.3 Managerial concerns

We examine whether heterogeneity in managerial characteristics and exposure to scrutiny conditions the response. Litigation risk is a first-order determinant of disclosure incentives, particularly around negative events (Skinner 1994; Rogers and Van Buskirk 2009). In addition, managerial attributes can shape reporting choices and crisis responses (Bertrand and Schoar 2003). We follow the table design by interacting Attack with proxies for managerial concerns, including measures of managerial ability (Demerjian, Lev, and McVay 2012), CEO background indicators, and a litigation-risk proxy.

The specification parallels the interaction models above. We expect stronger conservative disclosure responses when managers face higher personal exposure to credibility costs and legal risk.

3.3 Robustness tests

3.3.1 Future attack likelihood

A key alternative interpretation is that managers reduce non-GAAP reporting only when cyber costs are expected to be persistent rather than transitory. To evaluate this channel directly, Table 4 Panel A conditions the response on a quantified cyber risk measure that captures the likelihood of future attacks. Prior work shows that cyber risk is economically meaningful, persistent, and priced, implying that stakeholders may be skeptical of attempts to frame cyber consequences as purely one-time (Florackis et al. 2023). The model interacts Attack with an indicator for high cyber risk. This test assesses whether the post-attack reduction in non-GAAP disclosure is stronger when investors have greater reason to expect recurrence.

3.3.2 Repetitive attacks

Our study evaluates whether firms with repeated cyber incidents exhibit a larger pullback in non-GAAP disclosure. Repetition increases the difficulty of credibly characterizing incident-related costs as nonrecurring and increases the reputational risk of exclusions. We estimate the baseline model augmented with a RepetitiveAttack indicator (and associated tests) to separate the average post-attack response from the incremental effect of repeated events.

3.3.3 Entropy balancing

To address concerns that attacked firms differ systematically from non-attacked firms along observable characteristics correlated with non-GAAP disclosure, apply entropy balancing, which reweights control observations so that covariate moments match those of the treated group (Hainmueller 2012). We implement entropy balancing on the baseline covariates and fixed-effects structure, then re-estimate the baseline disclosure model using the implied weights. This approach improves covariate balance without discarding observations and provides a robustness check that the main inferences are not driven by observable differences in the composition of attacked and non-attacked firm-quarters.

3.4 Cyberattacks, non-GAAP disclosure, and future performance

Finally, we examine whether firms' post-attack non-GAAP disclosure choices relate to subsequent operating outcomes. The motivation is that if managers refrain from non-GAAP

disclosure because they anticipate heightened scrutiny and credibility costs, then non-GAAP disclosure after an attack may not signal superior underlying performance, and it may instead reflect atypical reporting incentives. This analysis aligns with the broader literature on the informativeness and credibility of non-GAAP reporting and stakeholders' interpretation of adjustments (Bhattacharya et al. 2003; Christensen et al. 2019).

We estimate linear models of future performance:

$$\text{Perf}_{i,t+1} = \alpha + \beta_1 \text{Attack}_{i,t} + \beta_2 \text{NonGAAPdum}_{i,t} + \beta_3 (\text{Attack}_{i,t} \times \text{NonGAAPdum}_{i,t}) + \Gamma' X_{i,t} + \delta_j + \lambda_t + \varepsilon_{i,t} \quad (4)$$

where $\text{Perf}_{i,t+1}$ is the future performance metric and β_3 captures whether non-GAAP disclosure has different implications for subsequent performance in the post-attack setting.

4. Methodology

4.1 Data and Sample

Our empirical analyses require combining data on corporate cyberattacks with data on firm financial reporting and performance. The cyberattack data are obtained from the Privacy Rights Clearinghouse (PRC) Chronology of Data Breaches, a comprehensive database of publicly reported data breaches in the U.S. The PRC dataset has tracked breaches since 2005 and provides detailed information on each incident. Following the approach of Kamiya et al. (2021) and others, we focus on cyber incidents affecting U.S. publicly traded companies from 2005 onward. The PRC data include key fields such as the date of the breach (and/or the disclosure date), the affected organization's name, the type of breach (e.g., hacking/malware, insider theft, unintended disclosure, etc.), and the number of records compromised. This rich detail enables our severity and type analyses described above. The PRC has documented thousands of breaches over the past two decades; for example, between 2005 and 2017, over 6,300 incidents are recorded, and that number has grown substantially in recent years amid increasing cyber threats.

To construct our sample, we first identify breaches in the PRC data that involve publicly traded companies. The PRC list includes entities across many sectors (retail, healthcare, education, etc.), including private and public firms. We perform a careful matching procedure to link each breach to the correct publicly traded firm in our financial databases. This involves

standardizing company names and using additional information like the firm’s location or industry provided in the breach report. We follow the matching approach of Liu et al. (2025), which entailed fuzzy matching on organization names and manual verification. Specifically, for each breach record, we search for a corresponding firm in Compustat or EDGAR that had the same or similar name and is in the relevant time frame. We cross-check using news articles or the firm’s 8-K disclosures (many firms file an 8-K when a major cyber breach occurs). Through this process, we obtain a list of public-company breaches with confirmed ticker/CIK mappings. Each cyberattack in our final sample is associated with a firm identifier and an event date (or quarter).

Next, for each breached firm, we align the timing of the attack with the firm’s financial reporting periods. For example, if a breach occurred in Q3 2018 (say September 2018), we mark that firm-quarter as an “attack” quarter and look at the *subsequent* earnings announcement (Q3 or Q4 2018) for changes in disclosure. In many tests, we will consider the first earnings report following the breach as the critical one for observing any non-GAAP disclosure change. We also consider multi-quarter windows (e.g., the year following the breach) for persistence of effects.

We then construct a matched control sample of firm-quarters with no cyberattacks. Using the propensity scores or entropy balancing as described, each breached firm-quarter is paired with one or more non-breached firm-quarters in the same calendar quarter (to account for time effects) with similar ex ante characteristics. Key matching variables include: industry (we match within the same industry where possible), firm size, market-to-book, prior-quarter stock return, and prior non-GAAP disclosure frequency. The latter is important – we ensure that the treatment and control firms had a similar likelihood of disclosing non-GAAP *before* the breach, so that any divergence after can be attributed to the breach. The matched control firms serve as the counterfactual for what non-GAAP reporting would look like absent a cyber event.

Financial statement and market data are drawn from standard sources. We obtain accounting variables (assets, earnings, special items, leverage, etc.) from Compustat and stock price/return data from CRSP. These data allow us to compute controls and also the outcomes like earnings surprises and cumulative abnormal returns for event studies. Data on analyst forecasts and coverage come from I/B/E/S. We will use the I/B/E/S *detail* file to get each analyst’s information and the street vs GAAP earnings differences. Governance and ownership

data (board composition, institutional ownership) are sourced from RiskMetrics and Thomson Reuters 13F filings, respectively.

For identifying non-GAAP disclosures, in addition to automated text searches, we use the Bentley et al. (2018) compiled list of non-GAAP EPS, to cross-verify when firms disclosed non-GAAP metrics. Each observation in our dataset will include an indicator for non-GAAP disclosure and possibly a measure of the non-GAAP adjustment magnitude (GAAP earnings minus non-GAAP earnings, when disclosed).

Overall, our sample spans 2005 through 2024, covering the rise of both cybersecurity incidents and extensive non-GAAP reporting. We anticipate hundreds of unique cyberattack events affecting public firms in this period (e.g., Kamiya et al. identified 150 for 2005–2014; with more recent data we expect considerably more). The breadth of the data will also enable us to examine if the phenomena strengthen in the later years when regulation of non-GAAP tightened (post-2016 SEC guidance) or when cyber risk became more salient.

5. Results

5.1. Baseline results

Table 1 presents the baseline results. In column (1), the coefficient on attack is negative and statistically significant (coefficient = -0.287 , $t = -2.82$). In column (2), the negative association persists after adding CEO characteristics (coefficient = -0.255 , $t = -2.02$). Across both specifications, these estimates indicate that firms are less likely to disclose non-GAAP earnings following a cyberattack, consistent with the view that cyber incidents increase external scrutiny and raise the perceived costs of discretionary performance presentation. This interpretation aligns with evidence that cyberattacks generate meaningful reputational and valuation consequences (Kamiya et al. 2021; Amir et al. 2018; Florackis et al. 2023), which can plausibly shift managers toward more conservative disclosure choices.

This pattern is also consistent with the non-GAAP literature emphasizing that non-GAAP reporting is a discretionary communication channel that managers use when they perceive benefits from alternative performance presentation, but whose use and aggressiveness are sensitive to monitoring and regulatory attention (Lougee and Marquardt 2004; Heflin and Hsu 2008; Kolev et al. 2008). Relatedly, prior evidence in settings characterized by heightened

monitoring shows that firms can reduce the incidence of non-GAAP disclosure while improving reporting quality among continuing disclosers (Christensen et al. 2019). Taken together, Table 1 is consistent with cyberattacks acting as an external shock that increases the expected costs of discretionary non-GAAP communication, thereby reducing the propensity to disclose non-GAAP metrics in the baseline specification.

The control variables exhibit several associations that are broadly consistent with prior evidence on the determinants of voluntary non-GAAP disclosure. Firm size is positive and significant in both columns (0.160 and 0.207), indicating that larger firms are more likely to disclose non-GAAP measures. This pattern is consistent with the idea that larger firms face greater investor demand for earnings communication and have more developed disclosure infrastructures (Healy and Palepu 2001; Bentley et al. 2018). Profitability is also positively associated with non-GAAP disclosure (0.395 and 0.941).

While non-GAAP reporting is not confined to profitable firms (Leung and Veenman 2018), prior work indicates that the content and incentives for non-GAAP reporting vary with firms' performance and benchmark pressures (Doyle et al. 2013; Frankel et al. 2011). Column (2) provides additional evidence that CEO attributes correlate with non-GAAP disclosure, but they do not explain away the negative association with cyberattacks. CEO age and CEO tenure load negatively (-0.016 and -0.012). These patterns are consistent with upper-echelons arguments that executives' observable characteristics map into systematic differences in corporate policies (Hambrick and Mason 1984; Bertrand and Schoar 2003) and with evidence that older CEOs tend to implement less risky corporate policies (Serfling 2014). CEO vega is positive and significant (0.046), consistent with higher option-based convexity encouraging risk-taking (Coles et al. 2006), which may extend to discretionary disclosure choices. Importantly, the persistence of the negative attack coefficient after including these CEO controls supports an interpretation centered on the attack shock and the associated shift in the firm's disclosure cost-benefit tradeoff, rather than compositional differences in managerial risk preferences

5.2. Corporate governance

Table 2 examines whether corporate governance proxies moderate the association between cyberattacks and the likelihood of disclosing a non-GAAP measure. The main effect of attack

is economically small and statistically insignificant across specifications (coefficients range from -0.002 to 0.141).

The coefficient on $\text{attack} \times \text{dummy}$ is negative and statistically significant in all four columns, including institutional ownership (-0.395 , $t = -1.82$), analyst following (-0.440 , $t = -2.07$), board size (-0.541 , $t = -2.31$), and board independence (-0.324 , $t = -1.70$). Interpreting these coefficients jointly implies that the post-attack reduction in non-GAAP disclosure is concentrated among firms with stronger monitoring. For example, for firms in the “high” institutional ownership group, the total effect is approximately -0.397 ($-0.002 - 0.395$). For firms with high analyst following, it is approximately -0.392 ($0.048 - 0.440$). The dummy coefficients are positive for several governance proxies, including institutional ownership (0.176 , $t = 3.12$), analyst following (0.207 , $t = 3.11$), and board independence (0.117 , $t = 3.94$), consistent with stronger monitoring being associated with a higher baseline propensity to provide supplemental performance disclosures.

However, the negative interaction terms indicate that these same monitoring mechanisms discipline managers away from discretionary non-GAAP disclosure following a cyber incident, consistent with governance constraining potentially opportunistic reporting choices (Frankel et al. 2011) and with external monitoring by analysts and institutional investors reducing managerial opportunism in financial reporting and disclosure (Yu 2008, Healy and Palepu 2001). This pattern also aligns with evidence that scrutiny affects managers’ incentives to use non-GAAP reporting strategically (Kolev et al. 2008).

5.3. Financial slack

Table 3 tests whether the cyberattack effect on the likelihood of non-GAAP disclosure varies with financial slack, proxied by the Z-score in column (1) and the Whited-Wu index in column (2). Across both specifications, the main effect of attack is statistically insignificant (0.066 , $t = 0.31$ using Z-score; 0.032 , $t = 0.19$ using the Whited-Wu index).

The main result is the interaction term. $\text{attack} \times \text{dummy}$ is negative and statistically significant in both columns (-0.499 , $t = -2.01$ in column 1; -0.382 , $t = -1.86$ in column 2). Economically, these estimates imply that the post-attack reduction in non-GAAP disclosure is concentrated in the high-slack group (for example, the implied effect for the dummy group is

approximately -0.433 in column 1, computed as $0.066 - 0.499$, and -0.350 in column 2, computed as $0.032 - 0.382$).

This pattern is consistent with disclosure incentive frameworks in which managers trade off the potential benefits of discretionary disclosure against credibility and scrutiny costs (Healy and Palepu 2001). In the cyber setting, attacks are associated with reputational and valuation consequences, which can increase perceived costs of discretionary reporting choices (Kamiya et al. 2021; Florackis et al. 2023). For firms with greater slack, the marginal benefit of using non-GAAP to reassure capital providers is plausibly lower because these firms face weaker immediate financing pressure, while the reputational cost of appearing opportunistic may be higher. This interpretation aligns with evidence that managerial reporting choices respond to scrutiny in non-GAAP settings (Kolev et al. 2008; Heflin and Hsu 2008) and with survey evidence that managers value credibility and capital market access when making reporting decisions (Graham et al. 2005). The use of established slack proxies also connects the analysis to the finance literature on external financing constraints and liquidity buffers (Whited and Wu 2006; Opler et al. 1999).

5.4. Managerial incentives

Table 4 examines whether the decline in non-GAAP disclosure following a cyberattack varies with proxies for managerial sophistication and legal exposure. Across the three specifications, the main effect of attack is not statistically distinguishable from zero. The cross-sectional results are concentrated in the interaction terms. Specifically, the coefficient on $\text{attack} \times \text{Dummy}$ is negative and statistically significant when the Dummy captures higher managerial ability (-0.448 , $t = -1.97$), MBA CEO (-0.741 , $t = -2.97$), and high-litigation industry exposure (-0.532 , $t = -2.66$). These estimates indicate that the post-attack reduction in the likelihood of non-GAAP disclosure is more pronounced when managers are plausibly more capable or sophisticated, and when expected legal costs are higher.

This pattern is consistent with the view that cyber incidents increase scrutiny over disclosure choices, and that managers facing stronger reputational and legal incentives avoid potentially controversial exclusions from GAAP earnings. Prior research documents that non-GAAP reporting can reflect managerial discretion used to shape market perceptions and meet earnings benchmarks (Doyle, Jennings, and Soliman 2013) and that monitoring and scrutiny constrain opportunistic non-GAAP choices (Frankel, McVay, and Soliman 2011; Gomez,

Heflin, and Wang 2023). The stronger negative interaction for high managerial ability is consistent with high-ability managers (as commonly proxied using Demerjian, Lev, and McVay 2012) selecting more conservative disclosure responses to avoid credibility losses (Bamber, Jiang, and Wang 2010; Bertrand and Schoar 2003). The stronger effect in high-litigation settings aligns with evidence that litigation risk shapes disclosure incentives and can discipline disclosure behavior around negative events (Skinner 1994; Rogers and Van Buskirk 2009). Consistent with data availability for these managerial proxies, the sample size is 107,434 in column (1) and 150,183 in columns (2) and (3).

5.5. Robustness tests

Table 5 reports two robustness tests that sharpen interpretation of the baseline relation between cyberattacks and firms' propensity to disclose non-GAAP performance (NONGAAPDUM). Panel A conditions the attack effect on an ex ante measure of future cyberattack likelihood (a Cyberrisk indicator). The standalone Attack coefficient is positive but not statistically reliable (0.313, $t = 1.06$), indicating no detectable change in non-GAAP disclosure propensity among firms with *lower* predicted cyber risk. The Cyberrisk dummy is positive and significant (0.181, $t = 4.32$), consistent with higher-risk firms systematically exhibiting greater disclosure complexity and a greater tendency to provide alternative performance measures. This aligns with evidence that firm-level cybersecurity risk is related to observable firm characteristics and predicts subsequent cyberattacks (Florackis, Louca, Michaely, and Weber 2023). The interaction term Attack $\times$ Cyberrisk dummy is negative and marginally significant (-0.601 , $t = -1.79$), implying that the post-attack reduction in non-GAAP disclosure is concentrated among firms with high ex ante cyber risk.

Economically, the implied net effect for high-risk firms is approximately $0.313 - 0.601 = -0.288$, which is close in magnitude to the baseline estimates. This pattern is consistent with the idea that when cyber problems are more likely to persist or recur, managers face weaker justification for portraying cyber-related costs as nonrecurring exclusions. Prior non-GAAP research shows that excluded expenses can be predictive of lower future cash flows and are often not transitory, which raises concerns about classifying such costs as "nonrecurring" (Doyle, Lundholm, and Soliman 2003). It is also consistent with heightened scrutiny of non-GAAP presentation when the exclusions may be viewed as opportunistic or misleading (Gomez, Heflin, and Wang 2023).

Panel B examines whether the baseline effect differs when firms experience repetitive attacks. The coefficient on Attack remains negative and statistically significant (-0.287 , $t = -2.82$), corroborating the main inferences. More importantly, the Repetitive attack indicator is substantially more negative (-0.913 , $t = -3.42$), indicating a materially larger decline in the likelihood of non-GAAP disclosure following repeated incidents. The reported chi-square test p-value of 0.0026 rejects equality, supporting the interpretation that repetitive attacks are associated with a statistically stronger reduction in non-GAAP disclosure propensity.

This evidence is consistent with repetitive attacks serving as a stronger signal of persistent vulnerabilities and ongoing expected costs, increasing reputational and contracting consequences and reducing managers' ability to credibly characterize cyber-related impacts as one-off items. Work in finance documents that successful cyberattacks can impose reputation-related losses that exceed direct out-of-pocket costs and lead firms to adjust policies toward greater risk management (Kamiya, Kang, Kim, Milidonis, and Stulz 2021). Evidence also indicates that the *second* breach can be particularly damaging for firm value (Peng, Zhang, Mao, and Xu 2023), which is consistent with stakeholders penalizing repeated incidents and therefore increasing scrutiny of firms' performance narratives. In the non-GAAP setting, such heightened scrutiny should reduce incentives to rely on alternative earnings metrics when exclusions may be perceived as recurring or strategically motivated (Doyle et al. 2003; Gomez et al. 2023).

Table 6 re-estimates the baseline specification using entropy balancing weights, which reweight control firm-quarters so that the distribution of observable characteristics matches the treated sample. This approach is designed to mitigate concerns that cyberattacked firms differ systematically from nonattacked firms on observables that also predict non-GAAP disclosure (Hainmueller 2012; Rosenbaum and Rubin 1983; Imai and Ratkovic 2014). The results remain consistent with the baseline inference. In column (1), the coefficient on attack is negative and statistically significant (-0.285 , $t = -2.74$). In column (2), after adding CEO characteristics, the coefficient remains negative and marginally significant (-0.219 , $t = -1.75$). These estimates indicate that the lower likelihood of non-GAAP disclosure following a cyberattack is not driven by observable differences between attacked and nonattacked firms, which strengthens a selection-on-observables interpretation of the baseline relation.

Control variables behave in ways consistent with prior non-GAAP evidence. Size is positive and highly significant (0.245 , $t = 11.25$ in column 1; 0.182 , $t = 5.10$ in column 2), and

profitable is also positive and significant (0.231, $t = 5.02$; 0.164, $t = 3.23$). These patterns align with the view that larger and profitable firms are more likely to provide supplemental performance measures as part of their earnings communication strategy (Lougee and Marquardt 2004; Bentley et al. 2018). In the CEO-augmented model, CEO age (-0.008 , $t = -2.58$) and CEO tenure (-0.012 , $t = -2.07$) are negative, while CEO vega is positive (0.049, $t = 3.87$), consistent with executive characteristics and incentives being associated with disclosure choices (Bertrand and Schoar 2003; Coles, Daniel, and Naveen 2006).

Table 7 examines whether cyberattacks and non-GAAP disclosure jointly predict next-period operating outcomes, measured as cash flow, profit margin, and sales growth at $t+1$. The main result is that the interaction $\text{attack} \times \text{nongaapdum}$ is negative and statistically significant across all three performance measures. Specifically, the coefficient on $\text{attack} \times \text{nongaapdum}$ equals -0.259 ($t = -1.82$) for future cash flow, -0.002 ($t = -2.99$) for future profit margin, and -0.055 ($t = -1.70$) for future sales growth.

These estimates imply that, among attacked firms, those that disclose non-GAAP earnings exhibit weaker subsequent operating performance than attacked firms that do not disclose non-GAAP metrics.

The main effect of attack is positive for future cash flow (0.424, $t = 2.69$) but is not statistically significant for future profit margin or sales growth. This pattern indicates that the adverse future-performance association is not a generic post-attack effect. It is concentrated in the subset of attacked firms that choose to issue non-GAAP disclosures. Interpreted in the context of the non-GAAP literature, these findings are consistent with non-GAAP disclosures being used in settings where managers anticipate weaker subsequent fundamentals and where excluded items may not be transitory. Prior research shows that expenses excluded from pro forma or non-GAAP earnings can predict lower future performance, which is inconsistent with the notion that exclusions are purely nonrecurring (Doyle, Lundholm, and Soliman 2003). Related evidence indicates that managers define non-GAAP earnings in ways that can be strategically aligned with capital market incentives such as meeting or beating benchmarks (Doyle, Jennings, and Soliman 2013), and that scrutiny and concerns about opportunistic presentation are central in non-GAAP reporting settings (Kolev, Marquardt, and McVay 2008; Gomez, Heflin, and Wang 2023). At the same time, cyberattacks are associated with persistent economic and reputational consequences (Kamiya et al. 2021; Florackis et al. 2023), so the negative interaction is consistent with cyber-related costs and operational disruption being

more persistent for the firms that choose to rely on non-GAAP communication following an incident.

Finally, the coefficients on *nongaapdum* itself vary across outcomes, including -0.021 ($t = -2.56$) for cash flow, 0.003 ($t = 12.40$) for profit margin, and -0.052 ($t = -11.13$) for sales growth. The interaction results remain the key inference because they isolate how non-GAAP disclosure in the post-attack setting relates to subsequent performance, beyond average differences across disclosers and nondisclosers.

6. Conclusion

Our study examines whether firms adjust non-GAAP earnings disclosure following cyberattacks. We find that firms are less likely to disclose non-GAAP earnings in attack periods, consistent with cyber incidents increasing the expected costs of discretionary performance presentation. This reduction is concentrated among firms subject to stronger monitoring and oversight, including higher institutional ownership, greater analyst following, and more independent boards. The reduction is also more pronounced among firms with greater financial slack and in settings in which expected scrutiny and legal exposure are higher, including firms led by higher-ability CEOs, MBA CEOs, and firms operating in high-litigation industries. These patterns are consistent with monitoring and credibility concerns constraining managers' use of discretionary non-GAAP communication after a negative shock (Kolev et al. 2008; Frankel et al. 2011; Gomez et al. 2023).

Our robustness tests support the main inferences. The decline in non-GAAP disclosure is stronger when cyber risks are more likely to persist, including firms with higher ex ante cyber risk and firms experiencing repetitive attacks, consistent with stakeholders viewing cyber-related consequences as less transitory and therefore treating exclusions more skeptically (Doyle et al. 2003; Florackis et al. 2023; Kamiya et al. 2021). Results are robust to entropy balancing, which mitigates concerns that observable differences between attacked and nonattacked firms drive the findings (Hainmueller 2012). Finally, attacked firms that disclose non-GAAP earnings exhibit weaker subsequent operating performance relative to attacked firms that do not disclose non-GAAP measures. This evidence is consistent with non-GAAP disclosure in the post-attack setting identifying firms with less favorable future fundamentals and with exclusions that are not purely transitory (Doyle et al. 2003; Doyle et al. 2013).

Overall, the evidence indicates that cyberattacks shift managers' disclosure tradeoffs toward more conservative non-GAAP use, particularly when monitoring and legal exposure are high and when cyber risks appear persistent. These findings extend research on non-GAAP reporting by identifying cybersecurity breaches as an operational and reputational shock that alters voluntary performance communication, and they complement evidence that cyber incidents have economically meaningful capital market consequences (Amir et al. 2018; Kamiya et al. 2021; Florackis et al. 2023). An implication for users is that the absence of non-GAAP disclosure after a cyberattack may reflect strategic restraint under heightened scrutiny. Conversely, continued non-GAAP disclosure in the post-attack period is associated with weaker subsequent performance, which warrants careful evaluation of the nature and persistence of excluded items.

References

- Abdel-Meguid, A., Jennings, J. N., Olsen, K. J., & Soliman, M. T. (2021). The impact of the CEO's personal narcissism on non-GAAP earnings. *The Accounting Review*, 96(3), 1–25.
- Altman, E. I. (1968). Financial ratios, discrimination analysis and the prediction of corporate bankruptcy. *The Journal of Finance*, 23(4), 589–609.
- Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), 1177–1206.
- Bamber, L. S., Jiang, J., & Wang, I. Y. (2010). What's my style? The influence of top managers on voluntary corporate financial disclosure. *The Accounting Review*, 85(4), 1131–1162.
- Bentley, J. W., Christensen, T. E., Gee, K. E., & Whipple, B. C. (2018). Disentangling managers' and analysts' non-GAAP reporting. *Journal of Accounting Research*, 56(4), 1039–1081.
- Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity breaches and the market value of corporate disclosures. *Journal of Accounting and Public Policy*, 37(6), 508–526.
- Bertrand, M., & Schoar, A. (2003). Managing with style: The effect of managers on firm policies. *The Quarterly Journal of Economics*, 118(4), 1169–1208.
- Bhattacharya, N., Black, E. L., Christensen, T. E., & Larson, C. R. (2003). Assessing the relative informativeness and permanence of pro forma earnings and GAAP operating earnings. *Journal of Accounting and Economics*, 36(1–3), 285–319.
- Black, E. L., Christensen, T. E., & Steffen, T. D. (2017). Has the regulation of non-GAAP disclosures influenced managers' use of aggressive earnings exclusions? *Journal of Accounting, Auditing & Finance*, 32(2), 209–240.
- Brown, N. C., Huffman, A. A., & Cohen, S. (2023). Accounting complexity and disclosure complexity. *The Accounting Review*, 98(6), 37–71.
- Christensen, T. E., Pei, H., Pierce, S. R., & Tan, L. (2019). Non-GAAP reporting following debt covenant violations. *Review of Accounting Studies*, 24(2), 629–664.
- Coles, J. L., Daniel, N. D., & Naveen, L. (2006). Managerial incentives and risk-taking. *Journal of Financial Economics*, 79(2), 431–468.
- Core, J. E., & Guay, W. R. (2002). Estimating the value of employee stock option portfolios and their sensitivities to price and volatility. *Journal of Accounting Research*, 40(3), 613–630.
- Curtis, M. B., Jenkins, J. G., & Bedard, J. C. (2018). Consumer behavior following a data breach. *Managerial Auditing Journal*, 33(4), 425–435.
- Demerjian, P., Lev, B., & McVay, S. (2012). Quantifying managerial ability: A new measure and validity tests. *Management Science*, 58(7), 1229–1248.
- Doyle, J.T., Lundholm, R.J. & Soliman, M.T. 2003. The Predictive Value of Expenses Excluded from Pro Forma Earnings. *Review of Accounting Studies* 8, 145–174
- Doyle, J. T., Jennings, J. N., & Soliman, M. T. (2013). Do managers define non-GAAP earnings to meet or beat analyst forecasts? *Journal of Accounting and Economics*, 56(1), 40–56.
- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cyber risk and firm value. *Review of Financial Studies*, 36(1), 1–37.
- Frankel, R., McVay, S., & Soliman, M. T. (2011). Non-GAAP earnings and board independence. *Review of Accounting Studies*, 16(4), 719–744.
- Gomez, R., Heflin, F., & Wang, K. (2023). Securities and exchange commission regulation and non-GAAP income statements. *The Accounting Review*, 98(2), 149–175.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2006). The impact of the Sarbanes–Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5), 503–530.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in the market reaction? *Journal of Computer Security*, 19(1), 33–56.

- Govindarajan, V., Srivastava, A., & Zhao, R. (2021). Mind the GAAP. *Harvard Business Review* (online).
- Graham, J. R., Harvey, C. R., & Rajgopal, S. (2005). The economic implications of corporate financial reporting. *Journal of Accounting Research*, 43(1), 3–73.
- Guest, N. M., Kothari, S. P., & Pozen, R. C. (2022). Why do large positive non-GAAP earnings adjustments predict abnormally high CEO pay? *The Accounting Review*, 97(6), 297–326.
- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research: A systematic literature review. *Managerial Auditing Journal*, 34(7), 808–834.
- Hainmueller, J. (2012). Entropy balancing for causal effects: A multivariate reweighting method to produce balanced samples in observational studies. *Political Analysis*, 20(1), 25–46.
- Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review*, 9(2), 193–206.
- 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.
- Heflin, F., & Hsu, C. (2008). The impact of the SEC’s regulation of non-GAAP disclosures. *Journal of Accounting and Economics*, 46(2–3), 349–365.
- Huang, H. H., & Wang, C. (2021a). Do banks price firms’ data breaches? *The Accounting Review*, 96(3), 261–286.
- Huang, Y., & Wang, H. S. (2021b). The impact of cybersecurity breaches on corporate financing. *Journal of Financial Economics*, 140(2), 561–582.
- Imai, K., & Ratkovic, M. (2014). Covariate balancing propensity score. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 76(1), 243–263.
- Johnson, M. F., Kasznik, R., & Nelson, K. K. (2001). The impact of securities litigation reform on the disclosure of forward-looking information by high technology firms. *Journal of Accounting Research*, 39(2), 297–327.
- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). What is the impact of successful cyberattacks on target firms? *Journal of Financial Economics*, 142(2), 887–917.
- Kolev, K., Marquardt, C. A., & McVay, S. E. (2008). SEC scrutiny and the evolution of non-GAAP reporting. *The Accounting Review*, 83(1), 157–184.
- Kyung, H., Lee, H. A., & Marquardt, C. A. (2019). The effect of investors’ access to management earnings forecasts on analysts’ earnings forecasts. *Journal of Accounting and Economics*, 67(1), 175–201.
- Leung, E., & Veenman, D. (2018). Non-GAAP earnings disclosure in loss firms. *Journal of Accounting Research*, 56(4), 1083–1137.
- Li, J., No, W., & Wang, K. (2018). SEC’s cybersecurity disclosure guidance and information security risk disclosure. *Journal of Accounting and Public Policy*, 37(6), 489–507.
- Liu, X., Luo, J., & Yawson, A. (2025). Equity offering following cyberattacks. *Journal of Corporate Finance*, 91, 102710.
- Lougee, B. A., & Marquardt, C. A. (2004). Earnings informativeness and strategic disclosure: An empirical examination of “pro forma” earnings. *The Accounting Review*, 79(3), 769–795.
- McVay, S. E. (2006). Earnings management using classification shifting: An examination of core earnings and special items. *The Accounting Review*, 81(3), 501–531.
- Opler, T., Pinkowitz, L., Stulz, R., & Williamson, R. (1999). The determinants and implications of corporate cash holdings. *Journal of Financial Economics*, 52(1), 3–46.
- Peng, J., Mao, J., Xu, X., & Zhang, H. (2025). Repeated data breaches and executive compensation. *Applied Economics Letters*, 32(8), 1111–1120.
- Pinsker, R. E., Smith, T. J., & Higgs, J. L. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems*, 33(2), 177–204.

- Rogers, J. L., & Van Buskirk, A. (2009). Shareholder litigation and changes in disclosure behavior. *Journal of Accounting and Economics*, 47(1–2), 136–156.
- Rosenbaum, P. R., & Rubin, D. B. (1983). The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70(1), 41–55.
- Serfling, M. (2014). CEO age and the riskiness of corporate policies. *Journal of Corporate Finance*, 25, 251–273.
- Skinner, D. J. (1994). Why firms voluntarily disclose bad news. *Journal of Accounting Research*, 32(1), 38–60.
- Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216–229.
- U.S. Securities and Exchange Commission. (2001). Cautionary advice regarding the use of “pro forma” financial information in earnings releases (Release No. 33-8039; 34-45124; FR-65).
- Verrecchia, R. E. (2001). Essays on disclosure. *Journal of Accounting and Economics*, 32(1–3), 97–180.
- Wang, J., Kannan, K., & Ulmer, J. (2013). The association between the disclosure of information security risk and the cost of capital. *Information Systems Research*, 24(2), 201–218.
- Whited, T. M., & Wu, G. (2006). Financial constraints risk. *Review of Financial Studies*, 19(2), 531–559.
- Yu, F. (2008). Analyst coverage and earnings management. *Journal of Financial Economics*, 88(2), 245–271.
- Zhang, T., Kwack, S. Y., Si, Y., & Tian, G. (2023). Non-GAAP reporting following going-concern opinions. *Accounting & Finance*, 63(3), 3217–3252.

Table 1. Baseline results

	(1)	(2)
	nongaap~m	nongaap~m
attack	-0.287*** (-2.82)	-0.255** (-2.02)
btm	0.002 (0.06)	0.093* (1.85)
salegrowth	0.007 (0.17)	0.056 (0.84)
size	0.244*** (11.28)	0.180*** (5.09)
profitable	0.233*** (5.08)	0.174*** (3.51)
roa	-1.302 (-1.39)	-3.817*** (-2.84)
CEO_age		-0.008*** (-2.66)
CEO_tenure		-0.012** (-2.09)
female		0.060 (0.81)
CEO_delt~n		-0.001 (-0.10)
CEO_vega~n		0.046*** (3.72)
_cons	-2.961*** (-23.34)	-2.420*** (-7.73)
year quarter fe	yes	yes
industry fe	yes	yes
N	150183	66544
pseudo R~q	0.175	0.150

Table 2. Corporate governance

	(1)	(2)	(3)	(4)
	insitutional owners	analyst following	board size	board independence
attack	-0.002 (-0.02)	0.048 (0.30)	0.141 (0.67)	-0.068 (-0.44)
Dummy	0.176*** (3.12)	0.207*** (3.11)	0.016 (0.56)	0.117*** (3.94)
attack*dummy	-0.395* (-1.82)	-0.440** (-2.07)	-0.541** (-2.31)	-0.324* (-1.70)
btm	0.049 (1.29)	0.091** (2.18)	0.013 (0.32)	0.016 (0.38)
salegrowth	0.001 (0.02)	-0.015 (-0.30)	0.010 (0.23)	0.014 (0.31)
size	0.200*** (7.06)	0.174*** (5.39)	0.235*** (5.00)	0.236*** (11.35)
profitable	0.414*** (9.55)	0.423*** (8.60)	0.242*** (10.86)	0.237*** (5.02)
roa	-2.248** (-2.13)	-2.369* (-1.91)	-1.429 (-1.51)	-1.390 (-1.46)
_cons	-2.921*** (20.46)	-2.638*** (14.95)	-2.955*** (23.13)	-2.991*** (23.64)
year quarter fe	yes	yes	yes	yes
industry fe	yes	yes	yes	yes
N	126409	113470	136210	136210
pseudo	0.180	0.162	0.176	0.177

Table 3. Financial slack

	(1) Z-SCORE	(2) WW-INDEX
attack	0.066 (0.31)	0.032 (0.19)
dummy	-0.341*** (-5.85)	-0.061 (-1.40)
attack*dummy	-0.499** (-2.01)	-0.382* (-1.86)
btm	0.070 (1.35)	0.063 (1.47)
salegrowth	0.046 (0.75)	0.089 (1.48)
size	0.208*** (5.87)	0.203*** (5.60)
profitable	0.247*** (4.52)	0.172*** (3.45)
roa	-3.187*** (-3.24)	-4.155*** (-3.83)
_cons	-2.817*** (-10.11)	0.929*** (10.68)
year quarter fe	yes	yes
industry fe	yes	yes
N	67276	79285
Pseudo R ² q	0.149	0.144

Table 4. Managerial concerns

	(1) Managerial ability	(2) MBA CEO	(3) litigation dummy
attack	-0.099 (-0.62)	0.006 (0.07)	-0.104 (-0.92)
Dummy	0.003 (0.09)	-0.172** (-2.39)	0.490*** (2.73)
attack*dummy	-0.448** (-1.97)	-0.741*** (-2.97)	-0.532*** (-2.66)
btm	0.009 (0.21)	-0.001 (-0.02)	0.019 (0.57)
salegrowth	-0.025 (-0.50)	0.006 (0.15)	-0.008 (-0.19)
size	0.264*** (11.78)	0.254*** (11.87)	0.249*** (11.15)
profitable	0.230*** (4.27)	0.231*** (5.07)	0.247*** (4.93)
roa	-1.881** (-2.41)	-1.333 (-1.42)	-1.066 (-1.12)
_cons	-3.116*** (-26.49)	-3.013*** (-23.70)	-3.005*** (-21.44)
year quarter fe	yes	yes	yes
industry fe	yes	yes	yes
N	107434	150183	150183
pseudo R~q	0.167	0.177	0.181

Table 5. Robustness tests

Panel A. likelihood of the future cyber attacks	
attack	0.313 (1.06)
Dummy	0.181*** (4.32)
attack*dummy	-0.601* (-1.79)
btm	0.022 (0.49)
salegrowth	0.004 (0.09)
size	0.239*** (10.18)
profitable	0.217*** (4.49)
roa	-1.601 (-1.62)
_cons	-2.620*** (-18.08)
year quarter fe	yes
industry fe	yes
N	99516
pseudo R ²	0.172

Panel B. Repetitive attacks

	(1)	(2)
attack	-0.287***	
	(-2.82)	
repetitive attack		-0.913***
		(-3.42)
btm	0.002	0.002
	(0.06)	(0.06)
salegrowth	0.007	0.008
	(0.17)	(0.17)
size	0.244***	0.244***
	(11.28)	(11.29)
profitable	0.233***	0.233***
	(5.08)	(5.07)
roa	-1.302	-1.303
	(-1.39)	(-1.39)
_cons	-2.961***	-2.962***
	(-23.34)	(-23.34)
p-value of chi-test		0.0026
year quarter fe	yes	yes
industry fe	yes	yes
N	150183	150183
pseudo R~q	0.175	0.176

Table 6. Robustness test: EntropyBalance

	(1)	(2)
attack	-0.285*** (-2.74)	-0.219* (-1.75)
btm	0.007 (0.17)	0.099** (2.00)
salegrowth	0.009 (0.19)	0.063 (0.89)
size	0.245*** (11.25)	0.182*** (5.10)
profitable	0.231*** (5.02)	0.164*** (3.23)
roa	-1.403 (-1.51)	-3.967*** (-2.95)
CEO_age		-0.008*** (-2.58)
CEO_tenure		-0.012** (-2.07)
female		0.074 (1.02)
CEO_delt~n		-0.002 (-0.20)
CEO_vega~n		0.049*** (3.87)
_cons	-3.004*** (-24.10)	-2.396*** (-7.41)
year quarter fe	yes	yes
industry fe	yes	yes
N	150183	66544
pseudo R~q	0.176	0.151

Table 7. Cyberattacks and non-GAAP disclosures and company future performance

	future performance _t+1 (1) cash flow	future performance _t+1 (2) profit margin	future performance _t+1 (3) sales growth
attack*dummy	-0.259* (-1.82)	-0.002*** (-2.99)	-0.055* (-1.70)
attack	0.424*** (2.69)	-0.001 (-0.99)	0.036 (1.15)
dummy	-0.021** (-2.56)	0.003*** (12.40)	-0.052*** (-11.13)
btm	-0.004 (-1.31)	0.001** (2.32)	-0.061*** (-7.28)
salegrowth	-0.002 (-1.26)	0.002*** (4.54)	0.431*** (13.93)
size	0.035*** (7.60)	0.001*** (5.74)	0.005** (2.21)
profitable	0.002 (0.76)	0.000 (1.03)	0.004 (0.65)
roa	-0.094*** (-3.00)	0.198*** (21.37)	0.038 (0.33)
_cons	-0.187*** (-6.24)	-0.008*** (-4.69)	0.447*** (9.57)
N	126427	126104	150214
R2_adj	0.122	0.294	0.195