

How do cyberattacks impact firms?

Axel Fleury^a, Carolina Salva^a

^a University of Neuchatel, Institute of Financial Analysis, Rue A.-L. Breguet 2, 2000 Neuchâtel, Switzerland

This draft: January 2026

Abstract

We study the economic consequences of cyberattacks on firms using analysts' forecast revisions. Cyberattacks trigger economically significant downward revisions in expected cash flows and price targets. These revisions operate mainly through higher expected costs rather than revenue declines, indicating that cyberattacks are operational and organizational shocks rather than reputational shocks. Revenues and demand remain stable, while firms internalize substantial new costs that persist beyond the short term. Industry and temporal analyses show that reputational concerns have weakened over time as firms improve cyber resilience. Our findings challenge the view that reputational damage is the primary consequence of cyberattacks and instead identify cost-side effects as the dominant channel.

JEL classification: G14, G32

Keywords: Cyberattacks, Reputation, Firm value, Analyst forecasts, Risk management

* Contact information: Axel Fleury, axel.fleury@unine.ch (corresponding author). Carolina Salva, carolina.salva@unine.ch.

Acknowledgements: We thank participants at the SFI Research Days 2025, and the University of Neuchatel Research Day 2024, for their helpful comments and suggestions.

Declaration of Interest statement: The authors declare no competing financial interests or personal relationships that could have influenced the work reported in this paper.

1 Introduction

Cyberattacks represent one of the most severe and likely disruptions to firm operations.¹ Managers and boards consistently rank cyber risk among their most significant concerns, reflecting both the high frequency of attacks and their potentially large economic consequences. In response, firms devote substantial resources to prevention, including investments in cybersecurity infrastructure, internal controls, and governance frameworks.² Nevertheless, successful attacks occur even at well-protected firms, placing the economic consequences at the center of concern for investors, managers, and other stakeholders. Understanding how cyberattacks impact firm fundamentals is therefore critical for evaluating firm value, designing effective post-incident responses, and assessing the economic relevance of cyber risk.

Despite the increasing frequency of cyberattacks, existing empirical evidence provides a limited and potentially incomplete account of their firm-level consequences. Much of the literature emphasizes reputational damage as the primary channel through which cyberattacks impact firms. Negative stock market reactions to cyberattacks or subsequent performance drops are often interpreted as indicators of reputational harm (Akey et al., 2023; Kamiya et al., 2021). This interpretation, however, rests largely on indirect evidence and often relies on specific attack types or narrow samples. Moreover, it is not obvious that reputational concerns dominate the economic consequences firms face following a cyberattack.³ Cyberattacks can generate substantial direct and indirect costs including remediation efforts, operational disruptions, legal and regulatory expenses, and sustained increases in security and compliance spending, that may persist well beyond the initial event. Distinguishing between reputation-driven and cost-driven channels is therefore essential for understanding how cyberattacks affect firm fundamentals and for guiding how firms should respond once an attack occurs.

To this end, we study how cyberattacks affect investors' expectations using analysts' consensus forecast revisions at a monthly frequency. Analysts' forecasts are commonly viewed as informative proxies for investors' expectations about firms' future performance, making them well suited for examining how

¹ Survey evidence is consistent with cyberattacks representing a first-order risk to firms. In a PwC survey of CEOs, 53% report that cybersecurity and data privacy breaches pose a significant threat to stakeholder trust, and cybersecurity ranks among the top three disruptive risks firms expect to manage, alongside regulatory change and business model transformation. Cybersecurity is also identified as the most likely disruptive event in the near term, with approximately 60% of respondents expecting to experience such an incident (PwC, *Staying the Course towards True North: State of the Internal Audit Profession Study*, 2017).

² Consistent with this emphasis in prevention, survey evidence highlights firms' focus on preparedness and mitigation. In PwC's *Risk in Review* survey, executives report that a central challenge in managing cyber risk is identifying and implementing policies to mitigate the operational and financial impact of cyberattacks (PwC, *Risk in Review*, 2017).

³ Survey evidence suggests that firms themselves emphasize cost-based consequences following cyberattacks. In the World Economic Forum's *Global Cybersecurity Outlook 2024*, based on a survey of 199 business and cyber leaders from 49 countries, respondents identify direct operational disruption and direct financial losses as their primary concerns following a cyberattack, whereas brand and reputational damage receive substantially less emphasis.

expectations evolve around a discrete event (Bouchaud et al., 2019; Abarbanell et al., 1995; Trueman, 1994). This approach offers two key advantages. First, the higher frequency of forecast data compared to reported annual data allows us to more closely link changes in expectations to the timing of cyberattacks, which alleviates concerns that results are driven by unrelated confounding events. Second, it allows us to examine how the effects of cyberattacks vary across forecast horizons and to gain insight into their short and longer-term implications. We combine this approach with a novel cyberattack dataset, the CISSM Cyber Attacks Database from the University of Maryland, which provides international coverage and classifies cyberattacks into distinct types. This broader scope allows us to move beyond case-specific analyses and assess the consequences of cyberattacks across a range of incidents.

We show that cyberattacks have economically significant consequences for firm value, but that these effects operate primarily through cost channels rather than revenue channels. Following a cyberattack, firms experience negative stock returns and, consistently, downward revisions in analysts' stock price targets. Analysts revise expected cash flows downward, with stronger adjustments concentrated in the short term and no significant effects at longer horizons. Importantly, we find no evidence of downward revisions in sales forecasts, suggesting that cyberattacks do not, on average, lead to reputational damage or demand contraction. Instead, analysts significantly revise EBIT forecasts downward, consistent with firms facing higher operating, recovery and remediation costs. These findings challenge the prevalent view that reputational damage is the primary consequence of cyberattacks. Instead, they suggest that cyberattacks represent operational and organizational shocks that force firms to internalize new costs while revenues and customer demand remain largely stable. As a result, the adverse impact of cyberattacks on firm value is driven primarily by cost-side effects rather than by reputational damage.

While our main results provide average effects, they may mask important variations over time, across industries, and between different types of cyberattacks. To address this, we examine how the consequences of cyberattacks vary temporally and cross-sectionally. We find that downward sales forecast revisions occur primarily in earlier cyberattacks and in industries particularly sensitive to privacy and data security. This suggests that reputational damage was a greater concern in the past and in certain industries. In contrast, reputational damage from cyberattacks is limited in recent years and outside of highly sensitive industries as we do not find evidence of sales declines. Nevertheless, the costs associated with cyberattacks remain a persistent concern across all time period, industries, and attack types, reinforcing the notion that the financial burden imposed on firms is a primary consequence of cyberattacks.

Our findings of limited reputational damage align with the view that firms are increasingly equipped to manage cyberattacks insuring minimal disruption. Firms can prepare to mitigate reputational harm through proactive risk management, well-defined protocols, and protective policies. Using the MSCI Privacy & Data Security Management Score as a proxy for cyberattack readiness, we find evidence that firms effectively mitigate reputational damage when they are prepared to manage cyberattacks. We find that preparedness effectively offsets the negative impact on expected sales. Analysts revise sales forecasts downward following a cyberattack, but this effect is mitigated for firms with higher scores, with similar offsetting effects in recent periods and non-sensitive industries, where we previously found limited reputational damage. We also provide evidence that firms' overall readiness has improved in recent years and in non-sensitive industries showing greatest gains. Additionally, we explore an alternative channel in which firms successfully mitigate reputational damage by being reactive and providing sufficient ex-post efforts. We proxy ex-post efforts using the change in operating expenses in the year of the cyberattack and find that firms with the lowest efforts tend to suffer reputational damage, while those with high efforts successfully mitigate reputational damage and even observe beneficial effects on their reputation.

Finally, we conduct several robustness tests to confirm our findings. First, we examine whether analysts can assess the implications of cyberattacks by analyzing forecast errors in cyberattack years. We find no significant increase in forecast errors, indicating that analysts accurately incorporate the impact of cyberattacks by adjusting cost projections rather than anticipating reputational damage. We also rule out the possibility that analysts primarily focus on forecasting earnings and are less responsive in updating revenue forecasts. Second, we validate our results by analyzing firms' actual performance following cyberattacks. While we detect no significant changes in actual sales, we find evidence of rising costs and capitalized expenses, as well as increased investments as part of their recovery process. This further reinforces our conclusion that cyberattacks primarily affect firms through higher costs rather than reputational harm. Last, we rule out the possibility that changes in sample composition drive our results by showing that the proportion of cyberattacks in sensitive and non-sensitive industries remains stable over time.

This paper contributes to the literature on the impact of cyberattacks on firms by deepening the understanding of the channels through which they affect firm valuations. Existing studies primarily focus on stock price reactions to data breaches, interpreting negative market responses and revenue declines as evidence of reputational damage as the primary consequence of cyberattacks.⁴ [Brogi et al. \(2018\)](#) find significant declines in market returns following data breach announcements. This finding

⁴ Cyberattacks may also impact firm value through the cost of capital. [Sheneman \(2017\)](#) shows that cybersecurity breaches increase firm's cost of debt, as post-breaches loans carry significantly higher spreads, highlighting the economic impact of cyberattacks on financing costs. [Havakhori et al. \(2021\)](#) find that firms experience a significant reduction in their cost of capital after disclosing cybersecurity improvements.

is further supported by [Akey et al. \(2023\)](#), [Kamyia et al. \(2021\)](#) and [Crosignani et al. \(2023\)](#). The prevailing view in this literature is that the deterioration in firm value is largely attributed to reputational damage, particularly through customer churn and firms' subsequent efforts to rebuild their reputation by investing in ESG initiatives ([Akey et al., 2023](#)). [Kamiya et al. \(2021\)](#) reinforce this argument by estimating reputational harm as the difference between total shareholder losses from negative market reactions and identified direct costs, concluding that reputational damage exceeds direct costs. They also observe sales declines in certain cases, further supporting the reputational damage hypothesis. Similarly, [Crosignani et al. \(2023\)](#) document that customers of firms affected by the NotPetya cyberattack tend to terminate their relationships with these firms in the medium term.⁵ Moreover, existing studies often focus on specific types of cyberattacks and case studies, which may limit the generalizability of their findings. Direct empirical evidence linking reputational damage to firm valuation remains scarce, with most studies relying on indirect measures such as market reactions.⁶

In contrast to existing studies, our research leverages a global dataset and includes recent incidents providing timely insights and a broader perspective on the economic consequences of cyberattacks on firms. Our empirical set up enables us to specifically examine the channels through which cyberattacks impact firm value. We challenge the prevailing view that reputational damage is the primary consequence of cyberattacks, showing instead that firms are primarily affected by the financial burden of recovery. Our findings indicate that cyberattacks primarily impact firm value through increased costs rather than reduced sales, and these costs are not necessarily incurred to prevent sales losses.⁷ Additionally, we explore the specific contexts in which reputational damage may occur and provide evidence suggesting that firms' proactive measures, such as risk management efforts, may help mitigate reputational harm.

Finally, we contribute more generally to the literature on the performance of financial analysts by providing new insights into how analysts incorporate information on cyberattacks into their forecasts. While existing research primarily focuses on analysts' responses to traditional firm-specific and macroeconomic events, our study examines their ability to process and integrate information on cybersecurity events.

The rest of the paper is organized as follows. Section 2 presents the data used in the study and provides summary statistics on cyberattacks. Section 3 describes the methodology and examines the impact of

⁵ [Akey et al. \(2023\)](#), [Bana et al. \(2023\)](#) and [Kamiya et al. \(2021\)](#) focus specifically on data breaches in the US. [Crosignani et al. \(2023\)](#) study specifically the NotPetya cyberattack.

⁶ Another strand of the literature examines firms' cybersecurity risk and asset pricing or its influence on the cost of capital. [Florackis et al. \(2023\)](#) develops a cybersecurity risk measure for U.S. firms, showing that high-risk companies outperform in normal times but underperform during periods of elevated cyber risk.

⁷ [Bana et al. \(2023\)](#) provide evidence that companies often respond to a cyberattack by investing in human capital, such as hiring cybersecurity professionals, as well as legal and public relations staff following a cyberattack.

cyberattacks on firms. Section 4 conducts a temporal and cross-sectional analysis. Section 5 explores how firms build resilience by preparing for potential cyberattacks, and investigate firm’s reactivity. Section 6 implements a series of robustness tests. Finally, Section 7 briefly concludes.

2 Data

2.1 Cyberattack events

Data on cyberattacks come from the CISSM Cyber Attacks Database of the University of Maryland (Harry & Gallagher, 2018). This database collects publicly available information on cyberattacks occurring worldwide from relevant sources, starting in 2014, and is updated monthly. Data are collected using a mixed-method approach of web scraping automation and manual review by researchers, who make the final decision on whether an event should be included in the database. Each cyberattack is classified according to the taxonomy of Harry & Gallagher (2018) into three categories: disruptive, exploitative, and mixed cyberattacks. Disruptive cyberattacks impede the target organization's normal operations. Exploitative cyberattacks illicitly access or exfiltrate sensitive information such as personally identifiable information, classified information, or financial data. Mixed cyberattacks incorporate both disruptive and exploitative elements. In this study, we consider cyberattacks from January 2014 to June 2023.

Victims of cyberattacks listed in the CISSM Database are not necessarily publicly listed firms; various other entities, such as government organizations and universities, are also included. As a first step, we retain only publicly listed firms. To do this, we compare all organization names to common company names in the LSEG Eikon database (previously Refinitiv Eikon), which provides financial data. Since organization names from CISSM are not necessarily displayed the same way as in LSEG Eikon, we perform fuzzy name matching. The identification follows the methodology of De Nederlandsche Bank (Nijhuis, 2022), which involves preprocessing company names by removing capital letters, non-ASCII characters, punctuation, legal business suffixes, and common words. Using a combination of Cosine Similarity, Discounted Levenshtein, String Subsequence Kernel Similarity, and Token Sort algorithms, company names from the CISSM database are matched with those in LSEG Eikon, with a score ranging from 0 to 100. As a threshold, we retain only matches with a score of 95 or higher. We then manually check the matches to ensure the company names from both databases truly correspond. Finally, if a company is targeted by multiple cyberattacks, we retain only the first recorded event for that firm. This process results in the identification of 483 public firms being cyberattacked from January 2014 to June 2023.

Table 1 presents the distribution of the 483 cyberattacks across years, industries, and types. The frequency of cyberattacks has been increasing since 2014, with a spike in 2020. The most frequently

targeted industries in the sample are industrials, information technology, consumer discretionary, and financials. Exploitative events are the most common type of cyberattack, accounting for 48.28% of the sample.

-Insert table 1 here-

2.2 Analysts' consensus forecasts

Data on analysts' forecasts come from the LSEG I/B/E/S Estimates database. We retrieve monthly analyst consensus forecasts for earnings per share (EPS), revenues, gross profit, and EBIT, issued at 1-year, 2-year, and 3-year horizons from January 2014 to December 2023. We also gather monthly forecasts for long-term EPS growth and 12-month price targets.⁸ The monthly consensus forecasts are computed by I/B/E/S as the statistical average of all outstanding individual broker estimates as of the third Friday of each month. Additionally, we collect the number of analysts covering each firm and earnings announcement dates. Finally, we gather the corresponding actual values for EPS, revenue, and EBIT. Each item is denominated in U.S. dollars using daily currency exchange rates for monthly forecasts and end-of-fiscal year exchange rates for actual values to ensure comparability among firms in our international sample as in [Derrien et al. \(2022\)](#).

I/B/E/S organizes forecast data using a rolling structure tied to fiscal periods, where fiscal year forecasts are categorized as FY1, FY2, FY3, and so on, based on their relative position to the forecast issue date. This structure defines forecast horizons (short, medium, long-term) relative to the time remaining until the fiscal year-end, rather than aligning forecasts with a specific fixed fiscal year-end to form a single time series. While this structure is convenient for capturing the most up-to-date forecasts at a given point in time, it does not allow us to track the evolution of forecasts for a fixed fiscal year over time. To address this, we restructure the data by matching forecasts to their corresponding fiscal years using the forecast date and fiscal period. We then align them chronologically to construct a time series of forecasts for each fiscal year.

2.3 Firm characteristics and stock market data

We collect firm financial statement data at an annual frequency from 2014 to 2023 from LSEG Eikon for the following items: total assets, total debt, total equity, actual revenues, EBIT, net income, EPS, cost of goods sold, operating expenses, R&D expenses, SG&A expenses, unusual expenses, intangibles and capital expenditures (capex). Each item is denominated in U.S. dollars using end-of-fiscal-year exchange rates. Additionally, we retrieve the Privacy & Data Security Management Score from MSCI

⁸ Long term growth of EPS is defined by I/B/E/S as “an estimate of the compound average rate of EPS growth analysts expect over a period of three to five years”

for each firm at a yearly frequency.⁹ This score evaluates a firm's ability to manage its exposure to cyber risks, including its capacity to address data breaches and the extent of its information security management system certifications. We use this score as a proxy for the firm's readiness against cyberattacks. If readiness mitigates the economic consequences of cyberattacks, firms with higher scores should experience smaller adverse effects following an attack. To prevent any look-ahead bias, we merge financial statement data and MSCI scores with monthly consensus forecasts using the latest available financial statement data as of the forecast date. For example, a forecast made in March 2015 is merged with the firm's financial statement data and MSCI scores from 2014, as the 2015 data would not yet be available at the time of the forecast.

We also collect stock market data, specifically stock prices and market capitalization, from LSEG Eikon. We retrieve closing stock prices and market capitalization at a monthly frequency, converting them into U.S. dollars using daily exchange rates. Prices are adjusted for stock splits and dividends. Stock market data are then merged with monthly consensus forecasts at the firm and year-month level.

2.4 Propensity Score Matching

To build a comparison group for our sample of cyberattacked firms, we select a control firm with no cyberattacks for each victim firm using propensity score matching. We compute propensity scores based on the prediction of a logit model of *Cyberattacked* (a dummy variable equal to 1 if a firm experienced a cyberattack during a year and 0 otherwise) on *leverage*, *size*, and *stock performance*, variables used in the propensity score matching of [Kamiya et al. \(2021\)](#). To alleviate the influence of outliers, we winsorize each matching variable at the 1% and 99% levels. We then perform one-to-one matching for each cyberattacked firm using nearest neighbor matching based on data from the year prior to the cyberattack. Additionally, we require the control firm to belong to the same industry as the cyberattacked firm, as classified by the Global Industry Classification Standard (GICS). This process results in 483 cyberattacked firms matched with 483 control firms.

[Table 2](#) presents the results of the propensity score matching, showing the differences in the means of the variables used for matching between the cyberattacked firms and the control group in the year prior to the cyberattack. Using T-tests and Wilcoxon z-tests, the results indicate no significant differences between the two groups for the matching variables.

-Insert table 2 here-

⁹ MSCI defines its Privacy & Data Security Management Score as follows: “*The Privacy & Data Security Management Score evaluates the company’s ability to manage its exposure to risks on this Key Issue*”. The full details of this score are included in the official [factsheet](#) produced by MSCI.

3 The impact of cyberattacks on firms: Analysts' forecast revisions

We examine analysts' consensus forecast revisions at a monthly frequency following a cyberattack. Analysts' consensus forecasts are commonly viewed as informative proxies of investors' expectations (Bouchaud et al., 2019; Abarbanell et al., 1995; Trueman, 1994). Using forecast revisions rather than realized firm outcomes offers two key advantages. The higher frequency of the data allows us to more precisely identify both the magnitude and the timing of the response to a cyberattack. Then, it enables us to examine how the effects of cyberattacks vary across forecast horizons. If cyberattacks impact firms' expected cash flows, these effects should be reflected in analysts' forecast revisions.

3.1 Methodology

We investigate how analysts adjust their forecasts following a cyberattack. To do so, we employ dynamic difference-in-differences regressions to analyze monthly changes in analysts' consensus forecasts in the months following the cyberattack. Specifically, we estimate the following regression:

$$Revision_{i,t} = \alpha + \sum_{m=1}^3 \beta_m month_{i,t+m} + controls_{i,t} + \gamma_{Firm} + \gamma_{Time \times Industry} + \varepsilon_{i,t} \quad (1)$$

The dependent variables are monthly revisions in analysts' consensus forecasts for EPS, revenues, gross profit, EBIT, long-term EPS growth, and price targets. Alternatively, we also use monthly stock returns to assess the market's reaction to a cyberattack. For EPS, revenues, gross profit, and EBIT, we estimate separate regressions for 1-year, 2-years, and 3-years forecast horizons to examine how the impact of a cyberattack evolves over time and to capture the term structure of the response.

Revisions to analysts' forecasts for EPS, revenues, gross profit, EBIT, long-term EPS growth and price target forecasts are computed following Derrien et al. (2022). For the EPS consensus forecast, $F_t EPS_{i,p}$, issued for firm i in month t for year p , the forecast revision is defined as the change in EPS forecast from month $t-1$ to t , scaled by the absolute value of the forecast in $t-1$ and multiplied by 100. This scaling expresses the revision as a percentage while avoiding the influence of negative values. Precisely, we compute EPS forecast revisions as $\Delta F_t EPS_{i,p} = \frac{F_t EPS_{i,p} - F_{t-1} EPS_{i,p}}{|F_{t-1} EPS_{i,p}|} \times 100$. Following the same logic, revenue forecast revisions are computed as $\Delta F_t Revenues_{i,p} = \frac{F_t Revenues_{i,p} - F_{t-1} Revenues_{i,p}}{|F_{t-1} Revenues_{i,p}|} \times 100$, gross profit forecast revisions as $\Delta F_t Gross Profit_{i,p} = \frac{F_t Gross Profit_{i,p} - F_{t-1} Gross Profit_{i,p}}{|F_{t-1} Gross Profit_{i,p}|} \times 100$ and EBIT forecast revisions as $\Delta F_t EBIT_{i,p} = \frac{F_t EBIT_{i,p} - F_{t-1} EBIT_{i,p}}{|F_{t-1} EBIT_{i,p}|} \times 100$. Long-term EPS growth forecast revisions are computed as $\Delta LTG_{i,t} = LTG_{i,t} - LTG_{i,t-1}$, as long-term growth is

already expressed in percentage. Price target revisions is $\Delta PriceTargets_{i,t} = \frac{PriceTarget_{i,t} - PriceTarget_{i,t-1}}{PriceTarget_{i,t-1}} \times 100$. Finally, monthly stock returns are computed using monthly closing stock prices as $Returns_{i,t} = \frac{Close Stock Price_{i,t} - Close Stock Price_{i,t-1}}{Close Stock Price_{i,t-1}} \times 100$. To alleviate the impact of outliers, all variables are winsorized at the 1% and 99% levels.

Our main independent variables are the three indicator variables $month_{i,t+1}$, $month_{i,t+2}$ and $month_{i,t+3}$. $Month_{i,t+m}$ equals 1 for the respective three consecutive months following a cyberattack event for a firm, and 0 otherwise. These three variables allow us to capture how analysts revise their expectations following a cyberattack. As I/B/E/S updates consensus forecasts on the third Friday of each month and not at the end of the month, we exclude the month of the cyberattack itself.

Additionally, we include a set of control variables to control for firm and forecast characteristics. Firm-level controls include firm size, book-to-market ratio, and leverage (Kong et al., 2021; Ramelli et al., 2021; Charitou et al., 2019; Loh & Stulz, 2018; To et al., 2018; Clement et al., 2011; Barth & Hutton, 2004). Firm-level variables are winsorized at the 1% and 99% levels. We control for size, as larger firms often have different financial characteristics and performance drivers than smaller firms, which can significantly affect forecast revisions. Note that size is not time invariant and therefore not fully subsumed by firm fixed effects. Size is computed as $Size_{i,t} = \ln(Total\ assets_{i,t})$ using our yearly firm financial statement data. The book-to-market ratio provides insights on the valuation and growth prospects of a firm. Controlling for the book-to-market ratio accounts for differences in valuation and growth expectations. Growth firms typically exhibit greater volatility in their performance due to their reliance on uncertain future prospects, whereas value firms generally have more stable and predictable expectations. The book-to-market ratio is computed as $Book - to - market_{i,t} = \frac{Book\ Value\ Equity_{i,t}}{Market\ Capitalization_{i,t}}$. Finally, controlling for leverage accounts for the extent to which a firm's capital structure influences its earnings performance and for variations in leverage that might affect forecast revisions. For instance, firms with higher leverage might exhibit greater earnings volatility, as fixed interest payments must be made regardless of business performance. Analysts may revise their earnings estimates more frequently and more significantly for highly leveraged companies to reflect this volatility. Leverage is computed as $Leverage_{i,t} = \frac{Total\ Debt_{i,t}}{Total\ Equity_{i,t}}$.

We also control for forecast characteristics. We include the following additional controls: analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates. Analyst coverage refers to the number of analysts following a firm. Firms with extensive analyst coverage tend to benefit from a broader range of perspectives, increased information processing and dissemination, and enhanced market visibility. Incorporating analysts'

coverage controls for potential differences in forecast revisions due to disparities in information and visibility. Earnings surprise provides valuable insights into a firm's ability to meet, fail or exceed forecasts and expectations. A positive earnings surprise can result in an upward forecast revision while a negative earnings surprise can lead to downward revisions. The earnings surprise is computed as the difference between the actual earnings of year p and the last forecast issued for that year in month T , scaled by the absolute value of the last forecast issued and multiplied by 100. Specifically, it is computed as $EPSsurprise_{i,t} = \frac{EPS_{actual_{i,p}} - F_T EPS_{i,p}}{|F_T EPS_{i,p}|} \times 100$. Earnings surprise is winsorized at the 1% and 99% levels. The time until the end of the forecast period helps us mitigate the tendency for analysts to refine their estimates as the earnings announcement date approaches, thereby acknowledging that the forecast just preceding the earning announcement (actual earnings) typically exhibits greater precision. The earnings announcement date is a dummy that equals 1 for months with earnings announcements and 0 otherwise. With this dummy variable, we control for analysts' tendency to revise their expectations when new information is released by the firm. Finally, forecast data are collected in U.S. dollars for comparability purpose as in [Derrien et al. \(2022\)](#). However, equity analysts typically issue forecasts in the reporting currency of the firm. When calculating analysts' revisions, our goal is to isolate the changes driven by shifts in analysts' beliefs, rather than by fluctuations in exchange rates. To address this, we account for exchange rate changes, which we compute as $\Delta FXRate = \ln\left(\frac{Exchange\ rate_{i,t}}{Exchange\ rate_{i,t-1}}\right) \times 100$. Changes in exchange rates are winsorized at the 1% and 99%.

Finally, we include *Firm* and *Time x Industry* fixed effects to control for unobserved firm specific time invariant characteristics and time-varying industry-specific factors. Standard errors are clustered at the firm level to account for within-firm correlation.

[Appendix A](#) presents the definition and construction of all variables used in the paper. [Table 3](#) reports the summary statistics of the variables employed in our main analysis. All variables are winsorized at the 1% and 99% levels, except for analysts' coverage, time until the end of the forecast period and earnings announcement dates. Note the negative mean monthly forecast revisions for EPS, revenues, gross profit, EBIT and long-term growth. This pattern is consistent with the well-documented tendency of financial analysts to issue optimistic forecasts that are subsequently revised downward as the earnings announcement date approaches (e.g. [Richardson et al., 2004](#)).

-Insert table 3 here-

3.2 Main results

To evaluate the impact of cyberattacks on firms, we begin by examining analysts' revisions of earnings forecasts as well as the effect of a cyberattack on firm value. Specifically, we look at EPS revisions at FY1, FY2 and FY3 horizons, long-term growth, price targets revisions as well as stock returns.

-Insert table 4 here-

Table 4 shows that a cyberattack triggers negative forecast revisions of EPS at FY1, FY2 and FY3 horizons compared to revisions in the absence of a cyberattack. Analysts revise their forecasts two months after a cyberattack, with revisions being stronger at shorter horizons. For FY1 forecast revisions, there are negative adjustments in the three months following a cyberattack, resulting in a cumulative downward revision of 2.66% (-0.42% -1.23% -1.01%). This cumulative forecast revision is about 2.5 times higher than the average EPS forecast revision (2.66/|-1.08|). It is only two months after the cyberattack that the negative forecast revisions of -1.23% for FY1, -1.47% for FY2, and -0.85% for FY3 become statistically significant. Note that the cumulative downward revision decreases with the time horizon. We don't observe any significant revisions of long-term EPS growth. Price targets are also revised downwards starting in month 1 (-0.05%) but with significant adjustments of -0.59% in month 2. Consistently, we also observe significant negative stock returns after a cyberattack. We observe cumulative negative stock returns of -1.37% (-0.42% -0.95%) two months after the cyberattack. Interestingly, market returns are about two times larger than analysts' revisions of price targets.

Our findings indicate that firms are expected to be hurt after a cyberattack resulting in lower future cash flows and lower firm value. We also observe that the impact is expected to be short lived. In terms of economic magnitude, we observe stronger revisions compared to other types of negative events. Comparing our results to those in Derrien et al. (2022) for other negative events, a cyberattack impacts expected EPS as much as a credit rating downgrade.¹⁰ Price target downward revisions are three times larger than a negative ESG news. Thus, cyberattacks are events that bring a substantial negative impact on firms. Our findings align with recent research, which confirms that cyberattacks have a significant negative impact on firms (Akey et al., 2023; Crosignani et al., 2023; Kamiya et al., 2021; Brogi et al., 2018).

¹⁰ Derrien et al. 2022 report revisions of EPS at FY1, FY2 and FY3 following a list of negative events on firms. Comparing the EPS revisions found from cyberattacks to their list, the magnitude is as big as a credit rating downgrade, which is the second most impactful event of their list.

3.3 Sales versus cost revisions

Existing studies argue that cyberattacks primarily cause reputational damage and revenue loss, while collateral costs are often considered less significant [Kamiya et al. \(2021\)](#). Compared to prior research, our set up enables us to directly examine the channels through which a cyberattack impacts cash flows and firm value. Specifically, we investigate whether downward revisions of expected cash flows are driven by lower expected sales due to reputational loss with customers or by higher costs incurred by firms to mitigate the attack. To address this, we evaluate forecast revisions of revenues, gross profit, and EBIT following a cyberattack at FY1, FY2 and FY3 horizons.

-Insert table 5 here-

[Table 5](#) presents the results. Interestingly, we don't find evidence of significant downward changes in expected sales at any given horizon. A similar observation is made for gross profit, which is reasonable since the costs of goods sold is unlikely to be directly impacted by a cyberattack. In contrast, we observe significant downward revisions in EBIT one to two months after a cyberattack for FY1, FY2 and FY3, with revisions ranging from -0.75% to -0.84%. These findings suggest that cyberattacks lead to changes in analysts' earnings expectations driven by the anticipation of higher costs rather than expectations of lower sales. This evidence implies that cyberattacks have limited reputational damage with customers but instead result in adverse effects for firms, primarily through higher associated ex-post costs. Thus, cyberattacks reduce future cashflows through higher costs rather than lower sales. Furthermore, we are confident that the absence of downward revisions in sales is not due to stale forecasts, as [Derrien et al. \(2022\)](#) document negative revisions in analysts' consensus sales forecasts following ESG-related bad news about firms, indicating that analysts pay attention to sales forecasts and update them if necessary.

Our results are somewhat surprising given the widely held perception that cyberattacks primarily harm firms' reputations. Contrary to this belief, our findings indicate that cyberattacks mainly reduce future cashflows through higher costs rather than through reputational damage with clients. However, these are average effects that may mask important trends over time, differences across firms and industries or between different types of cyberattacks. Next, we explore three key dimensions to gain additional insights.

4 Temporal and cross-sectional analysis

This section explores how the consequences of cyberattacks vary over time and cross-sectionally. First, we examine whether the impact of cyberattacks has evolved over time, reflecting changes in cybersecurity practices, or stakeholder perceptions. Second, we investigate how the effects vary across

industries with differing levels of exposure to cyber risk. Third, we analyze whether specific types of cyberattacks lead to differential cost or reputational outcomes.

4.1 Analysts' forecasts revisions over time

Cyberattacks have increased in frequency over time, with the number of incidents more than doubling since the onset of the COVID-19 pandemic.¹¹ This rise reflects the growing sophistication of threat actors and the increased difficulty of preventing cyberattacks, driven by firms' growing reliance on software, the Internet of Things, and the rising complexity of code.¹² For firms, the question is no longer if a cyberattack will occur, but when it will happen.¹³ In this environment, stakeholders may increasingly perceive cyberattacks not as signals of firm specific failure or fragility, but rather as inevitable events that reflect broader industry or societal challenges. Such a shift in perception is likely to mitigate the reputational consequences of cyberattacks and, in turn, their impact on customer demand. In that case, we would expect that the impact of cyberattacks on expected sales may have diminished over time. However, even if reputational effects on sales weaken over time, we expect that cyberattacks continue to generate substantial new costs. We, therefore, expect the cost impact of cyberattacks to persist over time, even as their effect on expected sales diminishes. To evaluate our hypotheses, we adjust our model and test for analysts' revisions on forecasted sales and EBIT for cyberattacks occurring during two distinct periods: 2014 to 2018, representing the first half of our sample, and 2019 to 2023, representing the latter half.

-Insert table 6 here-

Table 6 presents the results. For cyberattacks occurring in the early subperiod, we find significant downward revisions in sales forecasts at FY1 and FY3, with decreases of -0.33% and -0.34% , respectively. These results are consistent with analysts anticipating reputational damage during this period. We also observe significant downward revisions in EBIT forecasts at FY2 and FY3, with decreases of -1.05% and -1.54% , suggesting short- to medium-term cost effects. In contrast, for cyberattacks occurring in the later subperiod, we find no evidence of revisions in sales forecasts, suggesting that reputational concerns have largely dissipated. However, we continue to observe significant downward revisions in EBIT forecasts within one to two months after the cyberattacks,

¹¹ "Rising Cyber Threats Pose Serious Concerns for Financial Stability", IMF 2024, reported that cyberattacks have more than doubled since the pandemic.

¹² "Cyber Risk Is Growing. Here's How Companies Can Keep Up" Harvard Business Review, Michael Chertoff, 2023. Ensuring everything is patched against cyberattacks has become practically impossible due to firms' growing reliance on applications, the increasing number of Internet of Things devices, and the complexity of codebases with large amounts of lines of codes.

¹³ "The Global Cyber Threat", IMF 2021, states that a major cyberattack threatening the financial stability is not a question of if, but when. "A matter of when not if: Why is it crucial for businesses to protect themselves from cyberattacks?", Euro news 2023, is arguing the same question on businesses.

particularly at FY1, suggesting that analysts still expect cyberattacks to impose short-term cost-related impacts despite the lack of reputational damage.¹⁴

Our findings suggest that reputational damage with customers was anticipated in earlier cyberattacks, consistent with the evidence in [Kamyia et al. \(2021\)](#) and [Akey et al. \(2023\)](#), who study cyberattacks over the 2005-2017 period. In contrast, for more recent cyberattacks, reputational damage seems limited. Nevertheless, cyberattacks continue to impose significant short-term costs, reinforcing the view that the financial burden imposed on firms remains a critical concern.

4.2 Analysts' forecast revisions by industry

Research, media and public discourse frequently emphasize the loss of customer trust and brand damage following cyberattacks, especially in some industries such as finance, healthcare, information technology and telecommunications.¹⁵ Certain industries may be more vulnerable to reputational damage from cyberattacks due to their greater reliance on private information and the sensitive nature of the data they handle. As a result, customer responses and cyberattack induced costs may vary across industries. To examine this heterogeneity, we differentiate between sensitive and non-sensitive industries. We identify sensitive industries using the MSCI ESG Industry Materiality Map. Specifically, we classify as sensitive the three industries for which the Privacy & Data Security component receives the highest weight in the MSCI S score: Communication Services, Financials, and Information Technology.¹⁶ All other industries are categorized as non-sensitive.

-Insert table 7 here-

[Table 7](#) reports analysts' revisions to sales and EBIT forecasts for FY1, FY2, and FY3 horizons following cyberattacks in sensitive and non-sensitive industries. In sensitive industries, we document significant downward revisions in sales forecasts at the FY1 and FY2 horizons, with declines of -0.38% and -0.41%, respectively. Short-term EBIT forecasts are also significantly reduced by -1.43% at FY1. In contrast, for non-sensitive industries, we find no significant downward revisions in sales forecasts. However, EBIT forecasts are significantly revised downward at the FY1, FY2, and FY3 horizons. These findings suggest that cyberattacks affect customer demand only in sensitive industries, where the nature of the business plays a critical role. At the same time, in both industry groups, cyberattacks impose a financial burden through higher costs, as reflected in the consistent negative revisions to EBIT forecasts. Finally, we verify that these findings are not driven by changes in sample composition over time. As

¹⁴ Unreported tests, we find no significant effects on long-term growth forecasts in either period.

¹⁵ Some sources discussing reputational damage in the industries mentioned: Finance: [WEF](#), Healthcare: [WEF](#), IT: [Deloitte](#), Telecommunications: [Deloitte](#).

¹⁶ MSCI defines the Privacy and Data Security component as follows: "Companies are evaluated on the amount of personal data they collect, their exposure to evolving or increasing privacy regulations, their vulnerability to potential data breaches, and their systems for protecting personal data"

shown in Section 6.3, the share of cyberattacks occurring in sensitive industries remains relatively stable throughout the sample period.

These results can be illustrated with an example. A cyberattack on a bank, where sensitive data such as personal account details and passwords are compromised, would likely result in a significant loss of trust in the institution. In contrast, a cyberattack on a retailer, where personal information about purchases is stolen, may not necessarily lead to a comparable loss of trust. While reputational damage can occur, it is more likely when the context and nature of the business matters. However, in both cases, firms are likely to incur new costs to address internal issues and mitigate the impact caused by the cyberattack.

4.3 Analysts' forecast revisions by type of cyberattack

Finally, our sample categorizes cyberattacks into three types: exploitative, disruptive, and mixed, each characterized by distinct objectives and mechanisms. We investigate whether the effects of cyberattacks differ across types, focusing on exploitative and disruptive attacks, which are the most clearly differentiated. We expect exploitative cyberattacks to be more likely to result in reputational damage, as their primary objective is the theft of sensitive information, while also imposing significant additional costs on firms. In contrast, we expect disruptive cyberattacks to primarily affect firms through higher costs, as their main goal is to impair the firm's operations. To test these hypotheses, we estimate separate regressions of analysts' revisions to sales and EBIT forecasts for each cyberattack type.

-Insert table 8 here-

Table 8 presents the results by cyberattack type. Focusing on analysts' revisions to sales forecasts, we find no evidence of negative revisions across any type of cyberattack. This finding suggests that no specific type of cyberattack is expected to adversely affect sales or, consequently, to generate reputational damage with customers. Turning to EBIT forecast revisions, we document significant negative effects following both exploitative and disruptive cyberattacks. Exploitative cyberattacks are associated with a downward revision of -1.48% at the FY1 horizon, consistent with short-term impacts. Disruptive cyberattacks generate significant negative revisions to EBIT forecasts ranging from -1.43% to -2.18% at FY2 and FY3 horizons, suggesting short to medium-term cost effects. Overall, these results indicate that cyberattack type does not influence customer reactions, as reflected in the absence of negative sales forecast revisions across attack types.

5 Building cyber resilience: how firms mitigate reputational damage?

5.1 Firm's readiness against cyberattacks

Our findings of limited reputational damage are consistent with the view that firms are increasingly equipped to navigate cyberattacks with minimal disruption. Firms can mitigate reputational damage by proactively preparing for such events, for example, through effective risk management, well-defined protocols and protective policies. Many firms have established response plans that can be quickly implemented in the event of a cyberattack. This ensures a quick and efficient recovery. These measures not only reduce operational disruptions and mitigate costs but also reinforce stakeholder confidence, preventing significant reputational harm.

To test this channel, we use the MSCI Privacy & Data Security Management Score as a proxy for firms' readiness to manage cyberattacks. This score evaluates a firm's ability to address cyberattack-related risks, including its incident response plan for data breaches and its information security management system certifications.¹⁷ The score ranges from 0 to 10, with 0 indicating the weakest risk management measures against cyberattacks and 10 representing the best practices.

We focus on analysts' revisions of sales and EBIT forecasts, and extend our baseline regression model by including the MSCI Privacy & Data Security Management Score as an interaction term with our indicator variables, as follows:

$$\begin{aligned} Revision_{i,t} = & \alpha + \sum_{m=1}^3 \beta_m month_{i,t+m} + \sum_{m=1}^3 \beta_m month_{i,t+m} \times MSCI\ Score_{i,t} + controls_{i,t} \\ & + \gamma_{Firm} + \gamma_{Time \times Industry} + \varepsilon_{i,t} \end{aligned} \quad (2)$$

We estimate this regression on the full sample, as well as across the different time-period and industry-specific subsamples previously examined where we do not observe reputational damage. This approach allows us to evaluate whether a firm's readiness to manage cyberattacks effectively mitigates reputational damage to customers, potentially explaining the absence of such damage in our findings.

-Insert table 9a, 9b and 9c here-

Table 9a presents summary statistics for the MSCI Privacy & Data Security Management Score of cyberattacked firms, categorized by year, period and by industry sensitivity. We find that, on average, cyberattacked firms are better prepared in the later period compared to the earlier period. Firms in

¹⁷ All components included in this score is described in the official [factsheet](#) produced by MSCI.

sensitive industries tend to be better prepared than those in non-sensitive industries. Further, these differences in average scores are statistically significant at the 99% level, as confirmed by both a t-test and a Wilcoxon z-test (Table 9b). Overall, these results suggest that firms have improved their ability to navigate cyberattacks over time.

Table 9c presents the results of analysts' forecast revisions in relation to firms' readiness against cyberattacks. Analyzing the full sample, we observe significant downward revisions in sales forecasts two and three months after a cyberattack, with FY1 and FY2 forecasts decreasing by -0.74% and -0.98%, respectively. This suggests that, in the absence of any readiness against cyberattacks, firms suffer reputational damage. Turning to the interaction terms with our MSCI score, we find significant positive coefficients of 0.17 two and three months after a cyberattack for FY1 and FY2 forecasts. These findings indicate that a firm's readiness effectively mitigates reputational damage, as the downward revisions in sales forecasts are, on average, offset by stronger cyber resilience (average MSCI score of $4.98 \times 0.17 = 0.85$ percentage points in FY1 and FY2). Turning to analysts' revisions of EBIT, we observe similar results from our base indicators, where firms tend to suffer in the absence of readiness, with revisions ranging from -6.01% to -1.39%. The larger downward revisions in EBIT indicate that firms incur additional costs beyond reputational damage when unprepared. We also find similar results from our interaction terms, where downward EBIT revisions tend to be mitigated as a firm's cyberattack readiness improves, suggesting that readiness is indeed also effective in reducing costs. These pattern holds across the 2019–2023 and non-sensitive industries subsamples, where no reputational damage was previously observed, further supporting that view that the absence of reputational damages in our results can be attributed to firms' readiness against cyberattacks. This also indicates that the lack of reputational damage in these subsamples is not only attributable to a shift in perception over time or an irrelevant industry context, with readiness being of importance as well in these settings.

Overall, our findings suggest that firm's readiness against cyberattacks is effective in mitigating reputational damage, which may explain why we do not observe reputational harm in general from our previous results. Our subsamples analysis further indicates that neither the shift in perception of cyberattacks over time nor the industry context alone is sufficient to explain the absence of reputational damage, with firm's readiness still playing a part in these settings. While firm readiness appears also effective in mitigating the costs incurred by cyberattacks, it may not be as effective as in reducing reputational damage, as cost effects remain of significance in our main results. Alternatively, offsetting cost may just be more challenging than mitigating reputational damage in the context of cyberattacks. Finally, firm's are increasingly improving their readiness over time, which may also contribute to the evolving effect of cyberattacks on reputational damage.

5.2 Alternative channel

Our results are also consistent with alternative interpretations. They support the view that firms can limit the reputational impact of a cyberattack by responding swiftly and implementing transparent, prompt remediation measures -that is, by efficiently restoring trust. This reactivity, however, may lead to higher ex-post costs as firms take steps to mitigate the impact of the cyberattack. Other expected ex-post costs may include legal settlements and penalty fees imposed on cyberattacked firms. For instance, the credit rating firm Equifax had to pay over \$1 billion in penalties following a data breach occurring in 2017.¹⁸

To measure firm reactivity, we examine changes in actual operating expenses, during the year of the cyberattack. We compute the change in operating expenses by taking the difference between operating expenses at the beginning and end of the cyberattack year. We then categorize changes in operating expenses into five quintiles, where quintile 1 includes firms with the smallest changes and quintile 5 includes those with the largest changes. We predict that firms with larger changes in these metrics experience less reputational damage, reflected in lower decline in sales. As the change in operating expenses in the year of the cyberattack is not directly observable by analysts when the cyberattack occurs, we shift our analysis from analysts' forecasts to firms' actuals. We adjust our model from Section 3 and apply it to firms' actuals as follows:

$$\Delta Sales_{i,t} = \alpha + \sum_{p=0}^2 \beta_p \text{Cyberattack Year}_{i,t+p} + \text{controls}_{i,t} + \gamma_{\text{Firm}} + \gamma_{\text{Time} \times \text{Industry}} + \epsilon_{i,t} \quad (3)$$

The dependent variable $\Delta Sales$ represents the annual percentage change in actual sales from year $t-1$ to t , computed as $\Delta Sales_{i,t} = \frac{Sales_{i,t} - Sales_{i,t-1}}{|Sales_{i,t-1}|} \times 100$. Our main independent variables are the three indicators: $\text{Cyberattack Year}_i$, $\text{Cyberattack Year}_{i,t+1}$, and $\text{Cyberattack Year}_{i,t+2}$. $\text{Cyberattack Year}_{i,t+p}$ equals 1 for respectively the year of the cyberattack, one year after, and two years after, and 0 otherwise. We control for firm size, the book-to-market ratio, and leverage, constructed in the same way as in Section 3. Finally, we incorporate *firm* and *time x industry* fixed effects to control for unobserved firm-specific, time-invariant characteristics and time-varying, industry-specific factors. Standard errors are clustered at the firm level.

-Insert Table 10 here-

¹⁸ "Rising Cyber Threats Pose Serious Concerns for Financial Stability", IMF 2024, mentions that the credit reporting agency Equifax had to settle more than \$1 billion in penalties after a data breach in 2017.

[Table 10](#) presents the results for this channel. We find that firms with low efforts, as observed in quintiles 1 and 2, tend to experience a decline in sales in the year of the cyberattack, while firms with high efforts, as observed in quintiles 3 to 5, may even see an increase in sales. These results may also explain why we sometimes observe positive revisions in sales by analysts in prior results, indicating that high efforts following a cyberattack can even have beneficial effects on a firm's reputation.

Overall, while our results do not establish causality, they show an association suggesting that firms that respond proactively to cyberattacks and make efforts to mitigate their impact tend to offset reputational damage and may even strengthen client confidence.

6 Robustness tests

It is possible that our empirical approach has limitations in detecting reputational damage or that our results are influenced by sample composition. This could occur, for instance, if analysts primarily focus on forecasting earnings and are less responsive in updating revenue forecasts, or if they find it challenging to predict the outcomes of cyberattacks. In the first case, the impact of a cyberattack on revenues may not be fully captured through analysts' forecasts. But do analysts update revenue forecasts? Evidence suggests that they do when an event justifies such revisions. For example, [Derrien et al. \(2022\)](#) show that analysts adjust revenue expectations following ESG incidents, indicating that they pay attention to revenue forecasts and update them when necessary.

In the second case, if analysts find it challenging to predict the outcome of a cyberattack, they are likely to make larger forecast errors. As a result, any observed outcome may not accurately represent the true impact that firms experience. To address this, in section 6.1, we examine whether analysts make larger forecast errors in years when a cyberattack occurs. In Section 6.2, we further investigate the direct impact of cyberattacks on firms' realized performance by analyzing actual revenues, margins, costs, and capitalized expenses. This approach allows us to assess whether the observed outcomes align with our findings from analysts' forecast revisions and provides additional insight into the nature of costs increases triggered by a cyberattack.

Finally, a shift in sample composition, specifically a decline in the frequency of cyberattacks in sensitive industries over time- could also influence our interpretation of the evidence. However, in Section 6.3, we demonstrate that changes in sample composition does not affect our inference.

6.1 Forecast errors

Do analysts accurately integrate the news of a cyberattack into their forecasts? Using annual data on forecasts and actuals, we implement dynamic difference-in-differences regressions to assess whether analysts make larger forecast errors in years when firms experience a cyberattack.

$$Forecast\ Error_{i,t} = \alpha + \beta_1 Cyberattack\ Year_{i,t} + Controls + \gamma_{Firm} + \gamma_{Time \times Industry} + \epsilon_{i,t} \quad (4)$$

The dependent variable is the forecast error made by analysts on EPS, revenues, and EBIT at FY1, FY2, and FY3 horizons. Forecast errors for firm i in year t are computed as $Forecast\ error_{i,t} = \frac{|Forecast_{i,t} - Actual_{i,t}|}{|Actual_{i,t}|} \times 100$. These errors are winsorized at the 1% and 99% levels to mitigate the influence of outliers. Our main independent variable is $Cyberattack\ Year_{i,t}$, a dummy variable that takes the value of 1 if firm i experiences a cyberattack during year t and 0 otherwise. We include a vector of control variables, $controls_{i,t}$, to account for firm and forecast heterogeneities at the yearly level. Specifically, we control for firm characteristics such as leverage, book-to-market ratio, and size, as well as analyst coverage to address forecast heterogeneity (Kong et al., 2021; Ramelli et al., 2021; Charitou et al., 2019; Loh & Stulz, 2018; To et al., 2018; Clement et al., 2011; Barth & Hutton, 2004)¹⁹. Control variables are constructed as described in Section 3. Finally, we include *firm* and *time x industry* fixed effects to control for unobserved firm-specific, time-invariant characteristics and time-varying, industry-specific factors. Standard errors are clustered at the firm level to account for within-firm correlation.

-Insert table 11 here-

Table 11 presents the results. For EPS, sales and EBIT forecasts, the findings indicate no significant differences in forecast errors at any horizon between cyberattack years and other years. This suggests that analysts maintain the same level of accuracy in their predictions regardless of whether a cyberattack occurs. This result imply that analysts have a solid understanding of the implications of cyberattacks on firms. Since analysts appear to assess the impact accurately, our findings further support the conclusion that reputational damage is limited, and that cyberattacks primarily impose a cost burden on affected firms.

¹⁹ Note that some previous forecast heterogeneity controls used in Section 3 are no longer included, as we switched to yearly frequency. This concerns earnings surprise, time until the end of the forecast period and earnings announcement dates.

6.2 Realized firm performance

Next, we evaluate the impact of cyberattacks on firms' actual performance. Using annual data, we examine whether and how revenue and earnings elements change after a cyberattack. We also analyze the impact on specific costs and capitalized expenses. To do so, we implement dynamic difference-in-differences regressions to capture changes in actual performance, as follows:

$$\Delta Actuals_{i,t} = \alpha + \sum_{p=0}^2 \beta_p Cyberattack Year_{i,t+p} + controls_{i,t} + \gamma_{Firm} + \gamma_{Time \times Industry} + \epsilon_{i,t} \quad (4)$$

The dependent variable represents changes in Sales, EBIT, Net income, or EPS. To evaluate actual costs and capitalized expenses, we measure changes in Cost of Goods Sold, Operating expenses, R&D expenses, SG&A expenses, Unusual expenses, Intangibles, and Capex. Changes in actual performance for firm i from year $t-1$ to year t are computed as $\Delta Actual_{i,t} = \frac{Actual_{i,t} - Actual_{i,t-1}}{|Actual_{i,t-1}|} \times 100$. These changes are winsorized at the 1% and 99% levels. Our main independent variables consists on a set of indicator variables, $Cyberattack Year_{i,t+p}$, which equal 1 for years relative to the cyberattack event and 0 otherwise. Specifically, these indicators include $Cyberattack Year_{i,t}$ for the year of the cyberattack, $Cyberattack Year_{i,t+1}$ for one year after, and $Cyberattack Year_{i,t+2}$ for two years after. We also include a vector of control variables, $controls_{i,t}$, to account for firm characteristics at the yearly level. These controls include leverage, book-to-market ratio, and size, constructed as described in Section 3. Finally, we incorporate *firm* and *time x industry* fixed effects to control for unobserved firm-specific, time-invariant characteristics and time-varying, industry-specific factors. Standard errors are clustered at the firm level to account for within-firm correlation.

-Insert table 12 here-

Table 12 presents the results. Regarding revenue and earnings elements, we do not observe any contraction in sales after a cyberattack, which aligns with our findings from analysts' forecast revisions. Similarly, actual EBIT does not show any significant negative evolution following a cyberattack. In contrast, we find adverse effects on net income and actual EPS, with a sharp decline occurring two years after the cyberattack. Turning to actual costs, we observe a significant increase. Specifically, operating costs, R&D expenses, and unusual costs rise both in the year of the cyberattack and two years afterward. As expected, we do not find any negative impact on COGS, since cyberattack-related expenses are unlikely to be associated with production costs. Regarding capitalized expenses, we observe a significant increase in intangibles and Capex one year after the cyberattack, suggesting that firms engage in new investments as part of their recovery process.

Overall, these results are consistent with previous findings from analysts' forecasts. While there is not evidence of a decline in sales, cyberattacks impose a clear cost burden on firms. In addition to incurring higher costs, firms appear to invest in new resources following a cyberattack.

6.3 Sample Composition

Our previous results indicate that cyberattacks in data-sensitive industries lead to expected decline in sales which may signal reputational damage with customers. A potential explanation for the lack of reputational damage across the full sample and in recent years could be a shift in sample composition, with cyberattacks in sensitive industries becoming less frequent over time. To explore this possibility, we construct a distribution table showing the frequency of cyberattacks in sensitive versus non-sensitive industries over time. We then examine whether the proportion of cyberattacks in sensitive industries has declined in recent years.

-Insert table 13 here-

Table 13 shows that the sample composition remains stable over time, with the share of cyberattacks occurring in sensitive industries remaining relatively constant. Based on this observation, we conclude that our results are not driven by changes in sample composition.

7 Conclusion

This paper offers new insights into how cyberattacks impact firms and it challenges the prevailing view that reputational damage is their primary consequence. Using analyst forecast revisions, we show that analysts adjust cost expectations while leaving revenue projections largely unchanged. These findings indicate that the financial burden of recovery is the main channel through which cyberattacks affect firm value. We further show that realized costs significantly increase while revenues do not decline, suggesting that financial analysts accurately assess the consequences of cyberattacks. Moreover, we find that firms' preparedness helps mitigate reputational damage, with firms becoming better prepared in recent years. . We also provide evidence that a firm's reactivity to cyberattacks tends to be associated with no reputational damage and may even have beneficial effects on reputation. We note that our study also faces some limitations. First, we rely on publicly available financial forecasts, which may not capture the granularity of internal adjustments firms make following a cyberattack. Second, while we identify broad trends, firm-specific responses to cyberattacks can vary depending on governance, crisis management strategies, and customer relationships. We leave for future research the analysis of firm-level differences in more detail.

Our findings are relevant to financial analysts, investors, and corporate managers. As cyber threats become more prevalent, understanding their financial impact is important for risk management and valuation. Analysts play a key role in interpreting these risks and our results suggest they effectively incorporate cyber risks into their forecasts. For corporate managers, this study highlights the importance of proactive cybersecurity measures, as firms that are better prepared for cyberattacks tend to face lower financial and reputational consequences.

Beyond firm-level implications, our findings contribute to the broader discussion of cyber risk as a source of deadweight costs. We highlight that cyberattacks require significant resources to mitigate risk and recover from damage, which likely diverts funds from innovation, productivity, and growth. This economic burden likely reduces efficiency by shifting resources away from productive activities. As cyber threats continue to evolve, future research could examine these broader implications as well as the macroeconomic consequences and the value of regulatory responses.

Declaration of generative AI and AI-assisted technologies in the writing process.

During the preparation of this work the author(s) used ChatGPT for proofreading assistance. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article.

References

- Abarbanell, J. S., Lanen, W. N., & Verrecchia, R. E. (1995). Analysts' forecasts as proxies for investor beliefs in empirical research. *Journal of Accounting and Economics*, 20(1), 31-60. doi:https://doi.org/10.1016/0165-4101(94)00392-I
- Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2023). Hacking Corporate Reputations. *Social Science Research Network (SSRN)*. doi:https://dx.doi.org/10.2139/ssrn.3143740
- Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., & Wang, X. (2023). Human Capital Acquisition in Response to Data Breaches. *Social Science Research Network (SSRN)*. doi:https://dx.doi.org/10.2139/ssrn.3806060
- Barth, M. E., & Hutton, A. P. (2004). Analyst Earnings Forecast Revisions and the Pricing of Accruals. *Review of Accounting Studies*, 9, 59-96. doi:https://doi.org/10.1023/B:RAST.0000013629.59222.df
- Bouchaud, J.-P., Krüger, P., Landier, A., & Thesmar, D. (2019). Sticky Expectations and the Profitability Anomaly. *Journal of Finance*, 74(2), 639-674. doi:https://doi.org/10.1111/jofi.12734
- Brogi, M., Arcuri, M. C., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership & Control*, 15(2), 70-83. doi:https://doi.org/10.22495/cocv15i2art6
- Charitou, A., Karamanou, I., & Lambertides, N. (2019). Analysts to the rescue? *Journal of Corporate Finance*, 56, 108-128. doi:https://doi.org/10.1016/j.jcorpfin.2019.01.005
- Clement, M. B., Hales, J., & Xue, Y. (2011). Understanding analysts' use of stock returns and other analysts' revisions when forecasting earnings. *Journal of Accounting and Economics*, 51(3), 279-299. doi:https://doi.org/10.1016/j.jacceco.2010.11.001
- Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, 147(2), 432-448. doi:https://doi.org/10.1016/j.jfineco.2022.12.002
- Derrien, F., Krueger, P., Landier, A., & Yao, T. (2022). ESG News, Future Cash Flows, and Firm Value. *Social Science Research Network (SSRN)*. doi:https://dx.doi.org/10.2139/ssrn.3903274
- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity Risk. *The Review of Financial Studies*, 36(1), 351-407. doi:https://doi.org/10.1093/rfs/hhac024
- Harry, C., & Gallagher, N. (2018). Classifying Cyber Events: A Proposed Taxonomy. *Journal of Information Warfare*, 17(3), 17-31. doi:https://www.jstor.org/stable/26633163
- Havakhor, T., Rahman, M. S., & Zhang, T. (2021). Disclosure of Cybersecurity Investments and the Cost of Capital. *Social Science Research Network (SSRN)*. doi:https://dx.doi.org/10.2139/ssrn.3553470
- Kamiya, S., Jun-Koo, K., Jungmin, K., 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. doi:https://doi.org/10.1016/j.jfineco.2019.05.019
- Kong, D., Lin, Z., Wang, Y., & Xiang, J. (2021). Natural disasters and analysts' earnings forecasts. *Journal of Corporate Finance*, 66. doi:https://doi.org/10.1016/j.jcorpfin.2020.101860
- Loh, R. K., & Stulz, R. M. (2018). Is Sell-Side Research More Valuable in Bad Times? *The Journal of Finance*, 73(3). doi:https://doi.org/10.1111/jofi.12611

- Nijhuis, M. (2022, 3 3). *Company Name Matching DNB - Data Science Hub*. Tratto da Medium: <https://medium.com/dnb-data-science-hub/company-name-matching-6a6330710334>
- Ramelli, S., Ossola, E., & Rancan, M. (2021). Stock price effects of climate activism: Evidence from the first Global Climate Strike. *Journal of Corporate Finance*, 69. doi:<https://doi.org/10.1016/j.jcorpfin.2021.102018>
- Richardson, S. A., Teoh, S. H., & Wysocki, P. D. (2004). The Walk-Down to Beatable Analyst Forecasts: The Role of Equity Issuance and Insider Trading Incentives. *Journal of Accounting Research*, 885-924.
- Sheneman, A. (2017). Cybersecurity Risk and the Cost of Debt. *Social Science Research Network (SSRN)*. doi:<https://dx.doi.org/10.2139/ssrn.3406217>
- To, T. Y., Navone, M., & Wu, E. (2018). Analyst coverage and the quality of corporate investment decisions. *Journal of Corporate Finance*, 51, 164-181. doi:<https://doi.org/10.1016/j.jcorpfin.2018.06.001>
- Trueman, B. (1994). Analyst Forecasts and Herding Behavior. *The Review of Financial Studies*, 7(1), 97-124. doi:<https://doi.org/10.1093/rfs/7.1.97>

Appendix A: Variable definitions

The table gives definitions and information on construction of all variables used in current study.

Variable	Source	Description
Group 1. Analysts' Forecasts Variables		
Coverage	IBES	Number of analysts covering a firm.
Earnings announcement	LSEG Eikon	Indicator variable equal to 1 the year and month an earnings announcement is taking place, 0 otherwise.
EPS surprise	IBES	The difference between the last EPS consensus forecast for a period and the actual EPS value, expressed as a percentage of the absolute value of the last EPS consensus forecast. Values for other months are set to 0.
Error EBIT	IBES	The absolute difference between the consensus forecast and the actual EBIT value at a yearly frequency, expressed as a percentage of the absolute value of the actual EBIT value.
Error EPS	IBES	The absolute difference between the consensus forecast and the actual EPS value at a yearly frequency, expressed as a percentage of the absolute value of the actual EPS value.
Error Revenue	IBES	The absolute difference between the consensus forecast and the actual sales value at a yearly frequency, expressed as a percentage of the absolute value of the actual sales value.
Months to last forecast	IBES	Number of months until the end of the forecast period.
Δ EBIT	IBES	Monthly difference of EBIT consensus forecasts from month t-1 to t, expressed as a percentage of the absolute value of the EBIT consensus forecast in t-1.
Δ EPS	IBES	Monthly difference of EPS consensus forecasts from month t-1 to t, expressed as a percentage of the absolute value of the EPS consensus forecast in t-1.
Δ Revenue	IBES	Monthly difference of sales consensus forecasts from month t-1 to t, expressed as a percentage of the absolute value of the sales consensus forecast in t-1.
Δ Gross Profit	IBES	Monthly difference of gross profit consensus forecasts from month t-1 to t, expressed as a percentage of the absolute value of the gross profit consensus forecast in t-1.
Δ LTG	IBES	Monthly difference of long term EPS growth (3 to 5 years expectations) consensus forecasts from month t-1 to t.
Δ Price target	IBES	Monthly difference of price target consensus forecasts from month t-1 to t, expressed as a percentage of the price target consensus forecast in t-1.
Δ FXRate	IBES	Monthly log difference of FX rate with USD from month t-1 to t expressed in percentage.
Group 2. Firm Characteristics Variables		
Book-to-market ratio	LSEG Eikon	Total equity divided by market capitalization.
Leverage	LSEG Eikon	Total debt divided by total equity.
Size	LSEG Eikon	Log of total assets.
Stock returns	LSEG Eikon	Monthly difference of adjusted close stock prices from month t-1 to t, expressed as a percentage of the adjusted close stock price in t-1.

Δ Sales	LSEG Eikon	Yearly difference of sales from year t-1 to t, expressed as a percentage of the absolute value of sales in t-1.
Δ EBIT	LSEG Eikon	Yearly difference of EBIT from year t-1 to t, expressed as a percentage of the absolute value of EBIT in t-1.
Δ Net Income	LSEG Eikon	Yearly difference of net income from year t-1 to t, expressed as a percentage of the absolute value of net income in t-1.
Δ Actual EPS	LSEG Eikon	Yearly difference of EPS from year t-1 to t, expressed as a percentage of the absolute value of EPS in t-1.
Δ COGS	LSEG Eikon	Yearly difference of cost of goods sold from year t-1 to t, expressed as a percentage of the absolute value of cost of goods sold in t-1.
Δ Operating costs	LSEG Eikon	Yearly difference of operating costs from year t-1 to t, expressed as a percentage of the absolute value of operating costs in t-1.
Δ R&D costs	LSEG Eikon	Yearly difference of R&D costs from year t-1 to t, expressed as a percentage of the absolute value of R&D costs in t-1.
Δ SG&A	LSEG Eikon	Yearly difference of SG&A costs from year t-1 to t, expressed as a percentage of the absolute value of SG&A costs in t-1.
Δ Unusual costs	LSEG Eikon	Yearly difference of unusual costs from year t-1 to t, expressed as a percentage of the absolute value of unusual costs in t-1.
Δ Intangibles	LSEG Eikon	Yearly difference of intangibles from year t-1 to t, expressed as a percentage of the absolute value of intangibles in t-1.
Δ Capex	LSEG Eikon	Yearly difference of CAPEX from year t-1 to t, expressed as a percentage of the absolute value of CAPEX in t-1.

Group 3. Cyberattack Variables

Cyberattack Month + 1	CISSM Cyberattack Database	Indicator variable equal to 1 one month after a firm is experiencing a cyberattack, and 0 otherwise.
Cyberattack Month + 2	CISSM Cyberattack Database	Indicator variable equal to 1 two months after a firm is experiencing a cyberattack, and 0 otherwise.
Cyberattack Month + 3	CISSM Cyberattack Database	Indicator variable equal to 1 three months after a firm is experiencing a cyberattack, and 0 otherwise.
Cyberattack year	CISSM Cyberattack Database	Indicator variable equal to 1 the year a firm is experiencing a cyberattack, and 0 otherwise.
Cyberattack year + 1	CISSM Cyberattack Database	Indicator variable equal to 1 one year after a firm is experiencing a cyberattack, and 0 otherwise.
Cyberattack year + 2	CISSM Cyberattack Database	Indicator variable equal to 1 two years after a firm is experiencing a cyberattack, and 0 otherwise.
Data Privacy Score	MSCI	A 0 to 10 score evaluating a firm's ability to manage its exposure to risks from cyberattacks. A score of 10 corresponds to best practice, and a score of 0 indicates a lack of management.
Data Sensitive Industries	MSCI	Indicator variable equal to 1 if a firm is in one of the three industries (GICS) for which the Privacy and Data Security component of the MSCI ESG S Score has the highest weight, and 0 otherwise. These industries include Communication Services, Financials, and Information Technology.

Table 1: Distribution of cyberattacks

This table displays the distribution of 483 cyberattacks listed in the CISSM database on 483 distinct public companies by industry, type, and year. Industries are classified by GICS sectors. Cyberattack types are classified following the taxonomy of Harry & Gallagher (2018). Exploitive cyberattacks illicitly access or exfiltrate sensitive information such as personal identifiable information, classified information, or financial data. Disruptive cyberattacks impede the target organization's normal operations. Mixed cyberattacks incorporate both disruptive and exploitative elements.

By industry and year											
GICS Sector Name	Cyberattack Year										Total
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	
Communication Services	5	1	2	8	3	1	5	7	3	4	39
Consumer Discretionary	7	8	4	4	6	3	12	14	12	6	76
Consumer Staples	0	1	3	2	1	2	2	5	8	2	26
Energy	0	1	0	1	3	1	4	1	3	1	15
Financials	5	5	8	8	5	5	9	8	10	4	67
Health Care	3	0	1	1	4	4	13	8	7	6	47
Industrials	4	3	4	13	4	10	17	18	13	6	92
Information Technology	1	1	2	4	6	3	21	11	16	14	79
Materials	0	0	1	0	0	5	5	1	3	3	18
Real Estate	0	0	1	0	0	1	2	4	2	2	12
Utilities	0	0	0	0	3	1	2	1	4	1	12
Total	25	20	26	41	35	36	92	78	81	49	483

By type and year											
Cyberattack Type	Cyberattack Year										Total
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	
Disruptive	6	5	4	18	4	12	25	19	20	2	115
Exploitive	18	15	22	22	31	24	33	29	30	14	238
Mixed	1	0	0	1	0	0	34	28	31	31	126
Undetermined	0	0	0	0	0	0	0	2	0	2	4
Total	25	20	26	41	35	36	92	78	81	49	483

Table 2: Propensity score matching

This table presents the difference in means between 483 cyberattacked firms and 483 non-cyberattacked firms for each variable used in the propensity score matching. The propensity score is estimated using a logit regression of *Cyberattack*, a dummy variable equal to 1 if a firm experienced a cyberattack during a year and 0 otherwise, on *leverage*, *stock returns*, and *firm size*. *Leverage* is defined as total debt divided by total equity, *stock returns* are computed as simple returns, and *firm size* is measured as the natural logarithm of total assets. Matched firms are required to be in the same GICS sector as the treated firms and are selected based on the year prior to the cyberattack. T-tests and Wilcoxon z-tests are reported to test for differences in means, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

	(1) Treated Firms	(2) Control Firms	(3) Difference in means		
	Mean	Mean		T-test	Wilcoxon z-test
Leverage	0.986	0.950	-0.036	-0.319	-0.405
Stock returns(%)	11.399	10.531	-0.868	-0.323	-0.831
Firm Size	22.465	22.437	-0.028	-0.201	-0.107
Observations	483	483	966		

Table 3: Summary statistics

This table presents the summary statistics for our main firm-month variables from January 2014 to December 2023. $\Delta FEPS$, $\Delta FRevenue$, $\Delta FGross Profit$, and $\Delta FEBIT$ are pooled forecast revisions from 1-year, 2-year, and 3-year horizons.

	Mean	Min	p10	p50	p90	Max	SD	Observations
$\Delta FEPS(\%)$	-1.08	-58.82	-6.51	0.00	4.28	33.55	9.66	256982
$\Delta FRevenue(\%)$	-0.16	-11.52	-3.01	0.00	2.58	10.13	2.86	254375
$\Delta FGross Profit(\%)$	-0.15	-22.77	-3.70	0.00	2.94	24.88	5.13	188499
$\Delta FEBIT(\%)$	-0.72	-42.95	-5.88	0.00	4.18	29.84	7.85	227155
$\Delta LTG(\%)$	-0.10	-14.51	-1.56	0.00	1.26	13.02	2.92	158143
$\Delta Price targets(\%)$	0.30	-20.75	-4.89	0.00	5.79	21.49	5.58	259238
Stock returns(%)	0.69	-27.61	-10.80	0.40	12.36	34.93	9.94	251064
Firm size	22.88	17.20	20.19	22.92	25.49	27.58	1.99	267317
Leverage	1.02	-6.02	0.02	0.62	2.39	11.79	1.90	267317
Book-to-Market	0.65	-0.27	0.10	0.47	1.37	4.23	0.68	266899
Coverage	14.58	0.00	3.00	14.00	27.00	56.00	9.72	267408
EPS surprise	-0.05	-18.27	0.00	0.00	0.00	13.80	2.97	267408
Months to last forecast	15.18	0.00	2.00	14.00	30.00	36.00	10.09	267261
Earnings announcement	0.06	0.00	0.00	0.00	0.00	1.00	0.25	267408
$\Delta FXRate(\%)$	-0.12	-6.28	-1.87	0.00	1.41	4.95	1.59	264064

Table 4: Analysts' forecast revisions

This table reports regression results examining the dynamic effects of cyberattacks on firms' expected cash flows and firm value. $\Delta FEPS\ FY1$, $\Delta FEPS\ FY2$, and $\Delta FEPS\ FY3$ denote monthly analyst revisions for EPS over 1-year, 2-year, and 3-year horizons, respectively. ΔLTG represents monthly analyst revisions for expected EPS growth over 3 to 5 years, and $\Delta Price\ Target$ reflects monthly revisions in target stock prices issued by analysts. Stock Returns are measured as simple stock returns at monthly frequency. *Cyberattack Month + 1*, *Cyberattack Month + 2*, and *Cyberattack Month + 3* are indicator variables equal to 1 for 1, 2, and 3 months after a cyberattack event, and 0 otherwise. We control for firm size, book-to-market ratio, leverage, analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates with USD. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

	(1) $\Delta FEPS\ FY1$	(2) $\Delta FEPS\ FY2$	(3) $\Delta FEPS\ FY3$	(4) ΔLTG	(5) $\Delta Price\ target$	(6) Stock returns
Cyberattack Month + 1	-0.420 (-0.69)	0.100 (0.19)	-0.095 (-0.19)	-0.081 (-0.51)	-0.055 (-0.20)	-0.423 (-0.93)
Cyberattack Month + 2	-1.227** (-2.05)	-1.467** (-2.48)	-0.848* (-1.83)	0.215 (1.32)	-0.589** (-2.42)	-0.954** (-2.10)
Cyberattack Month + 3	-1.008 (-1.62)	0.158 (0.30)	0.742 (1.43)	-0.024 (-0.15)	0.062 (0.23)	0.167 (0.38)
Constant	12.383** (2.26)	27.665*** (5.00)	28.397*** (5.80)	2.328* (1.69)	23.331*** (9.46)	16.472*** (5.25)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	89,962	89,361	76,686	52,986	87,977	85,173
Adj. R2	0.12	0.11	0.10	0.02	0.21	0.22

Table 5: Analysts' forecast revisions: Sales vs Costs

This table reports regression results disentangling the dynamic effects of cyberattacks on firms' expected cash flows. $\Delta FRevenue FY1$, $\Delta FRevenue FY2$, and $\Delta FRevenue FY3$ denote monthly analyst revisions for revenues over 1-year, 2-year, and 3-year horizons, respectively. $\Delta FGross Profit FY1$, $\Delta FGross Profit FY2$, and $\Delta FGross Profit FY3$ represent monthly analyst revisions for expected gross profit over 1-year, 2-year, and 3-year horizons. $\Delta FEbit FY1$, $\Delta FEbit FY2$, and $\Delta FEbit FY3$ reflect monthly revisions in EBIT issued by analysts over 1-year, 2-year, and 3-year horizons. *Cyberattack Month + 1*, *Cyberattack Month + 2*, and *Cyberattack Month + 3* are indicator variables equal to 1 for 1, 2, and 3 months after a cyberattack event, and 0 otherwise. We control for firm size, book-to-market ratio, leverage, analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates with USD. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Revenues			
	(1) $\Delta FRevenue FY1$	(2) $\Delta FRevenue FY2$	(3) $\Delta FRevenue FY3$
Cyberattack Month + 1	0.190* (1.69)	0.269** (2.10)	0.148 (1.11)
Cyberattack Month + 2	-0.061 (-0.56)	-0.023 (-0.18)	-0.023 (-0.20)
Cyberattack Month + 3	-0.024 (-0.21)	-0.023 (-0.19)	0.136 (1.02)
Constant	8.214*** (8.42)	13.216*** (10.98)	12.780*** (11.77)
CONTROLS	YES	YES	YES
Firm FE	YES	YES	YES
Month x Industry FE	YES	YES	YES
Observations	89,069	88,587	75,762
Adj. R2	0.35	0.31	0.28
Gross Profit			
	(1) $\Delta FGross Profit FY1$	(2) $\Delta FGross Profit FY2$	(3) $\Delta FGross Profit FY3$
Cyberattack Month + 1	-0.210 (-0.79)	-0.017 (-0.07)	-0.057 (-0.21)
Cyberattack Month + 2	-0.287 (-1.08)	0.083 (0.31)	0.118 (0.42)
Cyberattack Month + 3	0.022 (0.08)	0.221 (0.78)	0.440 (1.55)
Constant	10.043*** (5.01)	16.086*** (7.02)	16.245*** (7.21)
CONTROLS	YES	YES	YES
Firm FE	YES	YES	YES
Month x Industry FE	YES	YES	YES
Observations	68,968	67,861	51,240
Adj. R2	0.07	0.07	0.06
EBIT			
	(1) $\Delta FEbit FY1$	(2) $\Delta FEbit FY2$	(3) $\Delta FEbit FY3$
Cyberattack Month + 1	-0.745 (-1.47)	-0.106 (-0.25)	-0.745** (-1.99)
Cyberattack Month + 2	-0.839* (-1.74)	-0.783* (-1.78)	-0.461 (-1.05)
Cyberattack Month + 3	-0.524 (-1.08)	0.153 (0.31)	0.722 (1.65)
Constant	15.851*** (3.69)	27.376*** (6.78)	23.956*** (6.05)
CONTROLS	YES	YES	YES
Firm FE	YES	YES	YES
Month x Industry FE	YES	YES	YES
Observations	79,823	79,328	67,291
Adj. R2	0.10	0.10	0.09

Table 6: Analysts' forecast revisions over time

This table reports regression results examining the dynamic effects of cyberattacks on firms' expected cash flows over time. The regressions are conducted separately for the earlier half of the sample (2014–2018) and the later half of the sample (2019–2023). $\Delta FRevenue\ FY1$, $\Delta FRevenue\ FY2$, and $\Delta FRevenue\ FY3$ denote monthly analyst revisions for revenues over 1-year, 2-year, and 3-year horizons, respectively. $\Delta FEBIT\ FY1$, $\Delta FEBIT\ FY2$, and $\Delta FEBIT\ FY3$ reflect monthly revisions in EBIT issued by analysts over 1-year, 2-year, and 3-year horizons. *Cyberattack Month + 1*, *Cyberattack Month + 2*, and *Cyberattack Month + 3* are indicator variables equal to 1 for 1, 2, and 3 months after a cyberattack event, and 0 otherwise. We control for firm size, book-to-market ratio, leverage, analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates with USD. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Period: 2014-2018						
	(1) $\Delta FRevenue\ FY1$	(2) $\Delta FRevenue\ FY2$	(3) $\Delta FRevenue\ FY3$	(4) $\Delta FEBIT\ FY1$	(5) $\Delta FEBIT\ FY2$	(6) $\Delta FEBIT\ FY3$
Cyberattack Month + 1	0.080 (0.40)	0.261 (1.06)	0.033 (0.12)	-0.190 (-0.24)	0.008 (0.01)	-1.538** (-2.34)
Cyberattack Month + 2	-0.194 (-1.22)	-0.303 (-1.52)	-0.340* (-1.70)	-0.763 (-1.07)	-1.048* (-1.70)	-0.518 (-0.77)
Cyberattack Month + 3	-0.327** (-2.36)	-0.132 (-0.78)	-0.030 (-0.14)	-0.291 (-0.68)	0.569 (1.07)	0.591 (1.08)
Constant	7.886*** (4.20)	14.488*** (6.35)	16.010*** (7.44)	8.495 (1.27)	31.048*** (5.31)	26.707*** (4.95)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	42,166	41,929	35,886	38,124	37,873	32,159
Adj. R2	0.38	0.34	0.31	0.09	0.11	0.10
Period: 2019-2023						
	(1) $\Delta FRevenue\ FY1$	(2) $\Delta FRevenue\ FY2$	(3) $\Delta FRevenue\ FY3$	(4) $\Delta FEBIT\ FY1$	(5) $\Delta FEBIT\ FY2$	(6) $\Delta FEBIT\ FY3$
Cyberattack Month + 1	0.194 (1.45)	0.229 (1.54)	0.186 (1.21)	-1.111* (-1.80)	-0.165 (-0.32)	-0.409 (-0.91)
Cyberattack Month + 2	-0.060 (-0.44)	0.029 (0.19)	0.103 (0.75)	-1.003* (-1.65)	-0.703 (-1.25)	-0.482 (-0.86)
Cyberattack Month + 3	0.037 (0.25)	-0.035 (-0.22)	0.203 (1.19)	-0.758 (-1.16)	-0.044 (-0.07)	0.715 (1.21)
Constant	14.370*** (6.87)	19.495*** (8.08)	19.321*** (8.57)	21.890*** (2.59)	31.624*** (2.92)	32.004*** (2.76)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	46,898	46,653	39,870	41,694	41,450	35,122
Adj. R2	0.33	0.30	0.27	0.14	0.12	0.09

Table 7: Analysts' forecast revisions by industry

This table reports regression results examining the dynamic effects of cyberattacks on firms' expected cash flows over industries. The regressions are conducted separately for industries particularly sensitive to cyberattacks and for non-sensitive industries. Sensitive industries are defined as the three industries with the highest weight in the Privacy & Data Security component of the MSCI ESG Industry Materiality Map. These industries include Communication Services, Financials, and Information Technology. Non-sensitive industries include all other industries. $\Delta FRevenue\ FY1$, $\Delta FRevenue\ FY2$, and $\Delta FRevenue\ FY3$ denote monthly analyst revisions for revenues over 1-year, 2-year, and 3-year horizons, respectively. $\Delta FEbit\ FY1$, $\Delta FEbit\ FY2$, and $\Delta FEbit\ FY3$ reflect monthly revisions in EBIT issued by analysts over 1-year, 2-year, and 3-year horizons. $Cyberattack\ Month + 1$, $Cyberattack\ Month + 2$, and $Cyberattack\ Month + 3$ are indicator variables equal to 1 for 1, 2, and 3 months after a cyberattack event, and 0 otherwise. We control for firm size, book-to-market ratio, leverage, analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates with USD. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Privacy & Data Security Sensitive Industries						
	(1) $\Delta FRevenue$ FY1	(2) $\Delta FRevenue$ FY2	(3) $\Delta FRevenue$ FY3	(4) $\Delta FEbit\ FY1$	(5) $\Delta FEbit\ FY2$	(6) $\Delta FEbit\ FY3$
Cyberattack Month + 1	0.238 (1.38)	0.222 (1.07)	0.267 (1.28)	-0.320 (-0.37)	0.639 (0.93)	-0.426 (-0.79)
Cyberattack Month + 2	0.190 (0.95)	0.123 (0.54)	0.027 (0.14)	-0.507 (-0.67)	-0.186 (-0.27)	0.458 (0.61)
Cyberattack Month + 3	-0.375** (-2.24)	-0.407** (-2.04)	0.155 (0.71)	-1.427** (-2.02)	-0.667 (-0.84)	0.553 (0.86)
Constant	8.190*** (5.86)	12.152*** (6.59)	11.662*** (7.19)	18.090*** (3.39)	25.749*** (5.87)	13.571*** (3.10)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	33,083	32,871	27,820	29,819	29,613	24,777
Adj. R2	0.32	0.28	0.27	0.08	0.08	0.07
Privacy & Data Security Non Sensitive Industries						
	(1) $\Delta FRevenue$ FY1	(2) $\Delta FRevenue$ FY2	(3) $\Delta FRevenue$ FY3	(4) $\Delta FEbit\ FY1$	(5) $\Delta FEbit\ FY2$	(6) $\Delta FEbit\ FY3$
Cyberattack Month + 1	0.151 (1.03)	0.289* (1.77)	0.078 (0.45)	-1.036* (-1.68)	-0.557 (-1.05)	-0.953* (-1.91)
Cyberattack Month + 2	-0.210 (-1.63)	-0.115 (-0.78)	-0.056 (-0.39)	-1.071* (-1.73)	-1.157** (-2.03)	-1.028* (-1.92)
Cyberattack Month + 3	0.178 (1.17)	0.192 (1.24)	0.119 (0.71)	-0.022 (-0.03)	0.604 (0.99)	0.774 (1.33)
Constant	8.234*** (6.08)	13.985*** (8.88)	13.494*** (9.41)	13.867** (2.15)	28.091*** (4.36)	31.173*** (5.54)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	55,986	55,716	47,942	50,004	49,715	42,514
Adj. R2	0.36	0.33	0.29	0.12	0.11	0.10

Table 8: Analysts' forecast revisions by type of cyberattack

This table reports regression results examining the dynamic effects of cyberattacks on firms' expected cash flows over cyberattack types. The regressions are conducted separately for exploitive and disruptive cyberattacks. Exploitive cyberattacks illicitly access or exfiltrate sensitive information such as personal identifiable information, classified information, or financial data. Disruptive cyberattacks impede the target organization's normal operations. $\Delta FRevenue\ FY1$, $\Delta FRevenue\ FY2$, and $\Delta FRevenue\ FY3$ denote monthly analyst revisions for revenues over 1-year, 2-year, and 3-year horizons, respectively. $\Delta FEbit\ FY1$, $\Delta FEbit\ FY2$, and $\Delta FEbit\ FY3$ reflect monthly revisions in EBIT issued by analysts over 1-year, 2-year, and 3-year horizons. *Cyberattack Month + 1*, *Cyberattack Month + 2*, and *Cyberattack Month + 3* are indicator variables equal to 1 for 1, 2, and 3 months after a cyberattack event, and 0 otherwise. We control for firm size, book-to-market ratio, leverage, analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates with USD. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Exploitive						
	(1)	(2)	(3)	(4)	(5)	(6)
	$\Delta FRevenue$ FY1	$\Delta FRevenue$ FY2	$\Delta FRevenue$ FY3	$\Delta FEbit\ FY1$	$\Delta FEbit\ FY2$	$\Delta FEbit\ FY3$
Cyberattack Month + 1	0.265* (1.82)	0.368** (1.97)	0.184 (0.97)	-0.234 (-0.33)	0.413 (0.63)	-0.482 (-0.95)
Cyberattack Month + 2	-0.106 (-0.74)	-0.061 (-0.39)	-0.112 (-0.83)	-1.486** (-2.15)	-0.651 (-1.17)	-0.258 (-0.52)
Cyberattack Month + 3	-0.045 (-0.30)	-0.258 (-1.34)	0.018 (0.09)	-0.632 (-0.99)	-0.462 (-0.68)	0.185 (0.31)
Constant	7.639*** (5.94)	12.311*** (7.42)	12.295*** (8.30)	11.983** (2.57)	23.784*** (4.21)	20.221*** (3.39)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	44,865	44,671	38,970	40,190	39,954	34,635
Adj. R2	0.35	0.31	0.29	0.12	0.10	0.08
Disruptive						
	(1)	(2)	(3)	(4)	(5)	(6)
	$\Delta FRevenue$ FY1	$\Delta FRevenue$ FY2	$\Delta FRevenue$ FY3	$\Delta FEbit\ FY1$	$\Delta FEbit\ FY2$	$\Delta FEbit\ FY3$
Cyberattack Month + 1	0.024 (0.10)	0.220 (0.82)	-0.081 (-0.27)	-0.548 (-0.53)	-1.429* (-1.72)	-1.571** (-2.21)
Cyberattack Month + 2	-0.255 (-1.04)	-0.344 (-1.09)	-0.315 (-1.11)	-0.152 (-0.21)	-2.175** (-2.46)	-0.931 (-1.18)
Cyberattack Month + 3	0.122 (0.54)	0.223 (1.05)	0.582** (2.40)	-0.069 (-0.07)	0.510 (0.54)	1.292* (1.91)
Constant	9.011*** (3.50)	14.972*** (6.09)	14.836*** (6.23)	20.050 (1.40)	30.515*** (2.99)	31.782*** (3.74)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	21,414	21,354	18,243	19,402	19,319	16,539
Adj. R2	0.39	0.36	0.32	0.12	0.14	0.12

Table 9a: Summary Statistics for Privacy & Data Security Management Score

This table presents summary statistics of the annual MSCI Privacy & Data Security Management Score for cyberattacked firms, categorized by early (2014–2018) and late (2019–2023) cyberattack periods and by sensitive and non-sensitive industries. Sensitive industries are defined as the three industries with the highest weight in the Privacy & Data Security component of the MSCI ESG Industry Materiality Map. These industries include Communication Services, Financials, and Information Technology. Non-sensitive industries include all other industries.

Time Periods								
	Mean	Min	p10	p50	p90	Max	SD	Observations
2014	5.21	2.00	3.00	4.95	7.50	8.80	1.63	54
2015	4.91	0.50	2.50	5.05	7.40	8.80	1.98	58
2016	4.70	0.30	2.00	5.00	7.50	8.30	2.03	82
2017	4.11	0.00	0.90	4.20	7.00	8.80	2.20	114
2018	4.48	0.00	1.70	4.30	7.50	9.70	2.09	118
2014-2018	4.57	0.00	1.70	4.60	7.30	9.70	2.06	426
2019	4.44	0.00	1.70	4.20	7.10	10.00	2.09	258
2020	4.68	0.00	2.45	5.00	7.10	10.00	2.01	270
2021	5.13	0.00	2.50	5.00	7.50	10.00	1.81	266
2022	5.56	0.00	3.30	5.80	8.00	10.00	1.85	255
2023	5.78	0.80	3.70	5.80	7.70	10.00	1.57	254
2019-2023	5.11	0.00	2.50	5.00	7.50	10.00	1.94	1303
Total	4.98	0.00	2.50	5.00	7.50	10.00	1.99	1729

Sensitive and Non-Sensitive Industries								
	Mean	Min	p10	p50	p90	Max	SD	Observations
Non-sensitive industries	4.51	0.00	1.70	4.90	6.80	10.00	1.98	885
Sensitive industries	5.47	0.00	3.00	5.50	7.70	10.00	1.87	844

Table 9b: Privacy & Data Security Management Score difference in means

This table presents the differences in means in the annual MSCI Privacy & Data Security Management Score between early period cyberattacked firms (2014-2018) and late period cyberattacked firms (2019-2023), and between sensitive and non-sensitive industries. Sensitive industries are defined as the three industries with the highest weight in the Privacy & Data Security component of the MSCI ESG Industry Materiality Map. These industries include Communication Services, Financials, and Information Technology. Non-sensitive industries include all other industries. T-tests and Wilcoxon z-tests are reported to test for differences in means, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Time periods					
	(1) 2019-2023	(2) 2014-2018	(3) Difference in means		
	Mean	Mean		T-test	Wilcoxon z-test
MSCI Data Security Score <i>Full sample</i>	5.109	4.574	0.535***	4.861	4.633
Observations	1303	426	1729		
MSCI Data Security Score <i>Non sensitive industries</i>	4.724	3.161	1.563***	8.464	7.674
Observations	762	123	885		
MSCI Data Security Score <i>Sensitive industries</i>	5.652	5.148	0.504***	3.776	3.748
Observations	541	303	844		
Sensitive & Non-Sensitive Industries					
	(1) Non-Sensitive	(2) Sensitive	(3) Difference in means		
	Mean	Mean		T-test	Wilcoxon z-test
MSCI Data Security Score	4.507	5.471	-0.964***	-10.398	-9.437
Observations	885	844	1729		

Table 9c: The role of Privacy & Data Security Management

This table reports regression results examining the dynamic effects of cyberattacks on firms' expected revenues, accounting for firms' readiness against cyberattacks. Firm readiness is proxied by the MSCI Privacy & Data Security Management Score. Time periods are divided into early cyberattacks (2014–2018) and later cyberattacks (2019–2023). Industries are categorized as sensitive or non-sensitive. Sensitive industries are defined as the three industries with the highest weight in the Privacy & Data Security component of the MSCI ESG Industry Materiality Map. These industries include Communication Services, Financials, and Information Technology. Non-sensitive industries include all other industries. $\Delta FRevenue\ FY1$, $\Delta FRevenue\ FY2$, and $\Delta FRevenue\ FY3$ denote monthly analyst revisions for revenues over 1-year, 2-year, and 3-year horizons, respectively. $\Delta FEBIT\ FY1$, $\Delta FEBIT\ FY2$, and $\Delta FEBIT\ FY3$ reflect monthly revisions in EBIT issued by analysts over 1-year, 2-year, and 3-year horizons. *Cyberattack Month + 1*, *Cyberattack Month + 2*, and *Cyberattack Month + 3* are indicator variables equal to 1 for 1, 2, and 3 months after a cyberattack event, and 0 otherwise. The MSCI Privacy & Data Security Management Score is interacted with the indicator variables using beginning-of-year scores. We control for firm size, book-to-market ratio, leverage, analysts' coverage, earnings surprise, time until the end of the forecast period, earnings announcement dates and changes in exchange rates with USD. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Whole Sample						
	(1) $\Delta FRevenue\ FY1$	(2) $\Delta FRevenue\ FY2$	(3) $\Delta FRevenue\ FY3$	(4) $\Delta FEBIT\ FY1$	(5) $\Delta FEBIT\ FY2$	(6) $\Delta FEBIT\ FY3$
Cyberattack Month + 1	0.323 (0.86)	-0.071 (-0.17)	-0.274 (-0.70)	-2.717* (-1.92)	-1.297 (-1.06)	-2.127** (-2.49)
Cyberattack Month + 2	-0.740* (-1.87)	-0.305 (-0.79)	-0.181 (-0.65)	-0.903 (-0.62)	0.560 (0.41)	-1.385* (-1.65)
Cyberattack Month + 3	-0.149 (-0.31)	-0.979* (-1.67)	-0.710 (-0.99)	-6.009*** (-2.72)	-2.346 (-1.43)	-1.954 (-1.28)
Month+1 x Data Privacy Score	0.012 (0.16)	0.055 (0.79)	0.089 (1.39)	0.526** (2.15)	0.249 (1.08)	0.316** (2.12)
Month+2 x Data Privacy Score	0.167** (2.50)	0.062 (0.94)	0.031 (0.57)	0.086 (0.30)	-0.076 (-0.28)	0.296* (1.93)
Month+3 x Data Privacy Score	0.033 (0.40)	0.174* (1.75)	0.157 (1.30)	1.064*** (2.84)	0.481* (1.70)	0.499* (1.89)
Constant	8.673*** (4.19)	14.413*** (5.88)	17.187*** (7.21)	8.800 (1.23)	22.893** (2.43)	26.911*** (2.89)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	36,821	36,699	32,290	33,493	33,336	29,200
Adj. R2	0.39	0.36	0.33	0.16	0.14	0.11

Table 9c continued...

Period: 2019-2023						
	(1) ΔFRevenue FY1	(2) ΔFRevenue FY2	(3) ΔFRevenue FY3	(4) ΔFEBIT FY1	(5) ΔFEBIT FY2	(6) ΔFEBIT FY3
Cyberattack Month + 1	0.259 (0.61)	-0.223 (-0.49)	-0.394 (-0.89)	-3.715** (-2.22)	-1.613 (-1.14)	-1.939** (-1.98)
Cyberattack Month + 2	-0.903* (-1.91)	-0.352 (-0.80)	-0.167 (-0.56)	-1.056 (-0.60)	0.553 (0.34)	-1.423 (-1.41)
Cyberattack Month + 3	-0.164 (-0.30)	-1.193* (-1.74)	-0.807 (-0.95)	-7.420*** (-2.92)	-3.352* (-1.75)	-2.867 (-1.57)
Month+1 x Data Privacy Score	0.024 (0.29)	0.085 (1.09)	0.117 (1.61)	0.709** (2.47)	0.302 (1.14)	0.286* (1.69)
Month+2 x Data Privacy Score	0.201** (2.55)	0.066 (0.95)	0.032 (0.58)	0.089 (0.26)	-0.076 (-0.23)	0.297 (1.64)
Month+3 x Data Privacy Score	0.045 (0.49)	0.218* (1.87)	0.189 (1.31)	1.314*** (3.07)	0.665** (2.02)	0.672** (2.14)
Constant	13.423*** (3.31)	20.444*** (4.42)	22.556*** (5.14)	7.509 (0.49)	35.466* (1.70)	34.979** (1.98)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	28,727	28,636	25,306	25,902	25,790	22,684
Adj. R2	0.39	0.36	0.32	0.18	0.16	0.12
Non Sensitive Industries						
	(1) ΔFRevenue FY1	(2) ΔFRevenue FY2	(3) ΔFRevenue FY3	(4) ΔFEBIT FY1	(5) ΔFEBIT FY2	(6) ΔFEBIT FY2
Cyberattack Month + 1	0.604 (1.24)	0.099 (0.20)	-0.336 (-0.79)	-1.587 (-1.32)	-0.389 (-0.24)	-2.190** (-2.26)
Cyberattack Month + 2	-0.867* (-1.74)	0.067 (0.15)	-0.141 (-0.46)	-3.037* (-1.91)	-0.893 (-0.54)	-1.480 (-1.59)
Cyberattack Month + 3	-0.169 (-0.27)	-1.276 (-1.58)	-0.878 (-0.89)	-8.197*** (-2.77)	-3.442* (-1.68)	-2.540 (-1.31)
Month+1 x Data Privacy Score	-0.042 (-0.40)	0.023 (0.23)	0.087 (1.14)	0.387* (1.69)	-0.006 (-0.02)	0.337* (1.95)
Month+2 x Data Privacy Score	0.217** (2.43)	0.025 (0.32)	0.069 (1.10)	0.499* (1.74)	0.309 (1.04)	0.321** (2.02)
Month+3 x Data Privacy Score	0.112 (0.96)	0.294** (2.07)	0.198 (1.12)	1.702*** (3.17)	0.879** (2.45)	0.696* (1.81)
Constant	8.342** (2.18)	15.142*** (3.34)	16.531*** (3.78)	11.236 (1.08)	21.762 (1.16)	36.653** (2.30)
CONTROLS	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES
Month x Industry FE	YES	YES	YES	YES	YES	YES
Observations	18,500	18,455	16,400	16,893	16,825	14,867
Adj. R2	0.40	0.39	0.35	0.20	0.19	0.15

Table 10: Firms' reactivity to cyberattacks

This table reports regression results examining the dynamic effects of cyberattacks on firms' actual sales, given the change in operating expenses on the year of the cyberattack. The change in operating expenses is measured as the difference between operating expenses at the beginning and end of the cyberattack year. Changes in operating expenses are categorized into five quintiles, with quintile 1 representing firms with the smallest changes and quintile 5 representing those with the largest changes. Δ Sales represents the yearly percentage change in actual sales. Cyberattack Year, Cyberattack Year + 1, and Cyberattack Year + 2 are indicator variables equal to 1 for the year of the cyberattack, one year after, and two years after, respectively, and 0 otherwise. We control for firm size, book-to-market ratio, and leverage. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

	Change in Operating Expenses				
	Quintile = 1	Quintile = 2	Quintile = 3	Quintile = 4	Quintile = 5
	Δ Sales	Δ Sales	Δ Sales	Δ Sales	Δ Sales
Cyberattack year	-12.951*** (-5.54)	-4.842* (-1.69)	5.847* (1.75)	6.952*** (3.35)	15.425*** (3.88)
Cyberattack year + 1	3.271 (0.84)	6.862 (1.54)	-3.683 (-1.11)	1.378 (0.44)	0.292 (0.09)
Cyberattack year + 2	3.507 (0.84)	11.061*** (2.93)	-2.948 (-0.88)	-4.352 (-1.48)	-0.693 (-0.24)
Constant	-174.630** (-2.13)	-168.927*** (-2.62)	-16.250 (-0.26)	-98.599 (-0.92)	-25.899 (-0.28)
CONTROLS	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES
Year x Industry FE	YES	YES	YES	YES	YES
Observations	1,714	1,616	1,595	1,642	1,691
Adj. R2	0.12	0.12	0.14	0.20	0.24

Table 11: Analysts' forecast errors

This table reports regression results examining forecast errors issued by analysts on cyberattack years for EPS, revenues, and EBIT. *Error EPS FY1*, *Error EPS FY2*, and *Error EPS FY3* denote yearly forecast errors for EPS over 1-year, 2-year, and 3-year horizons, respectively. *Error Revenue FY1*, *Error Revenue FY2*, and *Error Revenue FY3* reflect yearly forecast errors for revenues over 1-year, 2-year, and 3-year horizons. *Error EBIT FY1*, *Error EBIT FY2*, and *Error EBIT FY3* represent yearly forecast errors for EBIT over 1-year, 2-year, and 3-year horizons. *Cyberattack Year* is an indicator variable equal to 1 for the year of the cyberattack and 0 otherwise. We control for firm size, book-to-market ratio, leverage and analysts' coverage. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

EPS			
	(1) Error EPS FY1	(2) Error EPS FY2	(3) Error EPS FY3
Cyberattack year	0.025 (0.68)	-0.078 (-0.91)	-0.125 (-0.82)
Constant	-0.308 (-0.40)	-5.782*** (-2.77)	-11.457*** (-3.30)
CONTROLS	YES	YES	YES
Firm FE	YES	YES	YES
Year x Industry FE	YES	YES	YES
Observations	7,726	6,832	5,817
Adj. R2	0.20	0.14	0.17
Revenues			
	(1) Error Revenue FY1	(2) Error Revenue FY2	(3) Error Revenue FY3
Cyberattack year	-0.003 (-0.86)	0.006 (0.58)	-0.010 (-0.57)
Constant	0.043 (0.59)	-0.787** (-2.57)	-1.758*** (-2.99)
CONTROLS	YES	YES	YES
Firm FE	YES	YES	YES
Year x Industry FE	YES	YES	YES
Observations	7,733	6,849	5,832
Adj. R2	0.34	0.27	0.33
EBIT			
	(1) Error EBIT FY1	(2) Error EBIT FY2	(3) Error EBIT FY3
Cyberattack year	-0.029 (-1.42)	-0.012 (-0.19)	0.133 (1.08)
Constant	-0.789 (-1.28)	-3.173** (-2.20)	-7.157*** (-3.33)
CONTROLS	YES	YES	YES
Firm FE	YES	YES	YES
Year x Industry FE	YES	YES	YES
Observations	6,764	5,901	4,998
Adj. R2	0.19	0.21	0.26

Table 12: Firms' realized performance

This table reports regression results examining the dynamic effects of cyberattacks on firms' actuals. Revenue and earnings elements include Δ Sales, Δ EBIT, Δ Net Income, and Δ Actual EPS, representing the yearly percentage change in sales, EBIT, net income, and actual EPS, respectively. Costs and capitalized expenses elements include Δ COGS, Δ Operating Costs, Δ R&D Costs, Δ SG&A costs, Δ Unusual Costs, Δ Intangibles, and Δ Capex, representing the yearly percentage change in cost of goods sold, operating costs, research & development costs, selling general & administrative costs, unusual costs, intangibles, and capital expenditures, respectively. Cyberattack Year, Cyberattack Year + 1, and Cyberattack Year + 2 are indicator variables equal to 1 for the year of the cyberattack, one year after, and two years after, respectively, and 0 otherwise. We control for firm size, book-to-market ratio, and leverage. Standard errors are clustered at the firm level. T-statistics are shown in parentheses, with ***, **, and * denoting significance at the 1%, 5%, and 10% levels, respectively.

Revenue and earnings							
	(1) ΔSales	(2) ΔEBIT	(3) ΔNet Income	(4) ΔActual EPS			
Cyberattack year	2.250 (1.63)	-8.543 (-1.18)	-7.519 (-0.49)	-12.168 (-0.85)			
Cyberattack year + 1	1.064 (0.67)	3.919 (0.44)	22.309 (1.27)	20.409 (1.16)			
Cyberattack year + 2	0.564 (0.34)	-11.720 (-1.36)	-50.363*** (-3.45)	-49.258*** (-3.45)			
Constant	-99.208*** (-2.64)	1.965 (0.01)	18.224 (0.08)	62.994 (0.28)			
CONTROLS	YES	YES	YES	YES			
Firm FE	YES	YES	YES	YES			
Year x Industry FE	YES	YES	YES	YES			
Observations	8,311	9,037	9,087	9,083			
Adj. R2	0.15	0.03	0.03	0.03			
Costs and capitalized expenses							
	(1) ΔCOGS	(2) ΔOperating costs	(3) ΔR&D costs	(4) ΔSG&A costs	(5) ΔUnusual costs	(6) ΔIntangibles	(7) ΔCapex
Cyberattack year	1.535 (1.00)	2.574* (1.92)	6.601** (2.42)	0.555 (0.49)	104.947 (0.67)	8.544 (1.11)	2.793 (0.66)
Cyberattack year + 1	1.557 (0.84)	1.122 (0.66)	2.309 (0.84)	2.029 (1.40)	111.017 (0.85)	18.630* (1.96)	8.759** (2.03)
Cyberattack year + 2	-1.117 (-0.63)	4.195** (2.19)	7.578*** (2.66)	1.419 (0.97)	397.735** (2.13)	1.095 (0.15)	-0.831 (-0.21)
Constant	-114.604*** (-2.81)	-111.197** (-2.53)	-80.896* (-1.77)	-127.643*** (-3.84)	289.143 (0.13)	-822.329*** (-4.38)	71.044 (0.68)
CONTROLS	YES	YES	YES	YES	YES	YES	YES
Firm FE	YES	YES	YES	YES	YES	YES	YES
Year x Industry FE	YES	YES	YES	YES	YES	YES	YES
Observations	7,824	8,339	3,560	8,137	6,048	8,150	8,865
Adj. R2	0.15	0.10	0.10	0.11	-0.00	0.02	0.04

Table 13: Sample Composition Over Time

This table displays the sample composition of 483 cyberattacks listed in the CISSM database, involving 483 distinct public companies across sensitive and non-sensitive industries, and years. Industries are classified by GICS sectors. Sensitive industries are defined as the three industries with the highest weight in the Privacy & Data Security component of the MSCI ESG Industry Materiality Map. These industries include Communication Services, Financials, and Information Technology. Non-sensitive industries include all other industries. First rows display frequencies and second rows display column percentages.

Industries	Cyberattack Year										
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Non-Sensitive Industries (%)	14	13	14	21	21	27	57	52	52	27	298
	56.00	65.00	53.85	51.22	60.00	75.00	61.96	66.67	64.20	55.10	61.70
Sensitive Industries (%)	11	7	12	20	14	9	35	26	29	22	185
	44.00	35.00	46.15	48.78	40.00	25.00	38.04	33.33	35.80	44.90	38.30
Total (%)	25	20	26	41	35	36	92	78	81	49	483
	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00