Mutual Funds' Preemptive Response to Major Cyber Attacks

July 30, 2025

Abstract

This paper examines U.S. actively managed equity mutual funds' trading behavior around cyberattack announcements. It documents that active funds preemptively trim high–cyber-risk holdings and tilt into low–cyber-risk stocks, particularly among funds that disclose cyber risk in their prospectuses. It shows that firms with stronger data-privacy safeguards exhibit smaller tilts. It further demonstrates that these anticipatory reallocations generate significant subsequent net inflows driven by institutional investors. These findings extend the literatures on cyber-risk spillovers, pre-announcement trading, and mutual-fund skill, and highlight active managers' informational advantage in responding to emerging cybersecurity threats.

Keywords: Mutual fund; Cyber attack; Preemptive response; Cyber risk; Institutional investor

JEL Classification: G11, G14, G23

1 Introduction

The rapid proliferation of digital technologies and the accompanying expansion of cyber threats have altered the risk landscape facing investing institutions. In November 2018, Marriott International disclosed a breach of its guest-reservation database that exposed approximately 500 million records, culminating in a USD 52 million multistate settlement and comprehensive security overhauls.[1] Investors, traditionally focused on metrics such as earnings volatility, leverage, and liquidity, now face a parallel imperative: to assess firms' resilience to cyber risk and to manage exposures to vulnerabilities that can materialize in severe equity price declines.

Prior research documents significant negative cumulative abnormal returns (CARs) around cyber attack announcements for both breached firms and their peers. For example, Kamiya, Kang, Kim, Milidonis, and Stulz (2021) report a mean three-day CAR of –0.84% for attacked firms and spillover losses for peers, supporting industry-wide contagion effects. Jiang, Khanna, Yang, and Zhou (2024) further show that these spillovers are more severe for firms sharing greater data similarity with the breached entity, underscoring how common vulnerabilities amplify contagion effects. These studies convincingly demonstrate that the effect of cyber attack is beyond the victim firm alone. Parallel to these market impacts, Lin, Sapp, Ulmer, and Parsa (2020) document opportunistic insider trading in the months leading up to breach disclosures. Yet despite this extensive evidence on external abnormal returns and informed insider behavior, it remains unclear whether well-resourced institutional investors likewise anticipate cyber attack announcements and adjust their portfolios in advance.

This paper examines whether U.S. actively managed equity mutual funds systematically reduce exposures to industry-wide high-cyber-risk stocks (those in the top industry tercile of cyber-risk scores) in the months before public breach announcements, revealing an industry-level informational advantage. In the baseline analysis, I show that active funds significantly trim these high-risk holdings prior to disclosure.Drawing on industry-level informational advantages documented by Kacperczyk, Sialm, and Zheng (2005) and Avramov and Wermers (2006), I posit that managers exploit early warning signals—insider trading (Lin et al., 2020) being one potential example—to preempt adverse

[1]See: https://cisolegal.com/marriott-data-breach/

spillovers. By contrast, index funds, constrained by mechanical replication mandates, are not expected to exhibit directional trading before the cyber events, serves as a comparison.

I test the central hypothesis utilizing a sample of eight large-scale cyber attacks affecting publicly traded U.S. firms between 2012 and 2018, identified from the Privacy Rights Clearinghouse database. To qualify as high-impact events, breaches must involve malicious external hacking, result in the compromise of over one million customer records, and occur at corporations outside the government and nonprofit sectors. I construct an event window spanning two months before to two months after public disclosure (denoted τ–2 through $\tau + 2$). The primary dependent variable measures monthly changes in mutual fund holdings on its underlying stocks.

I show that the active mutual funds exhibit statistically significant reductions in their holdings of high-cyber-risk stocks industry-wide in the month before breach announcements. Funds on average decrease the positions in the stock of 48.8% (-0.0020/-0.0041) relative to the overall mean monthly position change in the sample. Translating the estimated -0.0020 percent position change into dollar terms with an average fund size of $406.46 million yields a per-stock monthly adjustment of approximately $\$8,129.23$ ($exp(19.8230) * 0.0020\%$ see Table A3). In contrast, index funds show an insignificant adjustment, confirming that the anticipatory behavior is not driven by mechanical rebalancing.

Since March 31, 2009, the SEC has required mutual funds to deliver a summary prospectus disclosing their principal investment risks. I retrieved these prospectuses from the SEC EDGAR database and applied the textual-analysis method, following Sheng, Xu, and Zheng (2024) to identify funds that explicitly report cybersecurity risk. As Figure 1 shows, funds first disclosed cyber risk in 2014, and the share increases steadily afterwards. Therefore, I hypothesize that funds that disclose cyber risk may trade more aggressively around breach events. Consistent with this prediction, these funds systematically trim their industry-wide high–cyber-risk holdings two months before major cyber-attack announcements and, at the same time, tilt into low–cyber-risk stocks.

Motivated by evidence of within-industry spillovers following cyber attacks (e.g., Kamiya et al., 2021), I hypothesize that active funds will trade more aggressively in securities sharing the breached firm's industry. In line with this, I find funds reduce their industry-wide holdings in the hacked

sector beginning two months before the public announcement and then partially reverse these cuts one month after disclosure. Moreover, within the breached industry, funds disproportionately trim positions in the high-cyber–risk firms while reallocating into lower-cyber–risk firms.

Building on the previous finding that funds shift from high– to low–cyber-risk stocks, I next investigate whether superior data-privacy safeguards attenuate these pre-announcement tilts among similarly high–risk firms. Specifically, I obtain firm-level data privacy policy scores from LSEG Workspace and classify high–cyber-risk stocks by their relative privacy quality. Consistent with the substitution hypothesis, among high–risk firms, those with stronger privacy protections experience significantly smaller pre-announcement reductions in fund holdings. This finding indicates that robust privacy policies can partially substitute for low baseline cyber risk to temper defensive reallocations of active managers.

A potential concern is that these pre-announcement trades merely reflect funds "learning" from early price declines in high–cyber-risk (or low-cyber-risk) stocks rather than any informational edge. In other words, suppose high–risk shares fall before a breach is disclosed, managers could simply be following observable price signals. To test this, I regress the contemporaneous return onto the firm's cyber risk, and find no statistically significant price effects for either group. This lack of anticipatory price movement implies that funds' defensive reallocations cannot be attributed simply to mechanical responses to early price declines, and instead point toward potential informational advantages.

To gauge the economic payoff of anticipatory trading, I regress next-month net fund flows on each fund's pre-announcement tilt into high (low)–cyber-risk stocks. The results show that managers who shift more heavily into low-cyber–risk stocks before a breach announcement receive significantly higher inflows in the following month, consistent with investors rewarding successful industry timing. This "flow reward" underscores that skilled managers not only identify vulnerable firms but also construct robust, low-risk portfolios ahead. Furthermore, since retail investors disproportionately chase recent performance and Morningstar ratings (Ben-David, Li, Rossi, and Song, 2022), a breakdown by investor type reveals that these flow benefits are primarily driven by institutional rather than retail allocations.

This paper extends the cyber attack pre-announcement trading and announcement-timing literatures by showing that well-resourced fund managers exploit the window between a cyber attack's occurrence and its public disclosure. Lin et al. (2020) document that insiders execute opportunistic trades in the three months before breach announcements, and Foerderer and Schuetz (2022) show firms strategically delay disclosure to coincide with high "news pressure," thereby attenuating market reactions. This paper builds on these findings by showing that active mutual funds harness this implicit "timing" gap to gather and process pre–announcement signals, systematically reducing exposures to high–cyber-risk stocks in advance of public announcements.

This paper enriches the cyber attack spillover effect literature by linking breach announcements to mutual-fund trading behavior at the industry level. Florackis, Louca, Michaely, and Weber (2023) document significant negative spillovers from cyber attacks to industry peers, and Jiang et al. (2024) show these effects are magnified for firms with high data-similarity scores, which correlate with elevated cyber risk. This study shows that active funds dynamically adjust their portfolios within affected industries: they systematically trim their position in the highest–cyber-risk firms and reallocate into lower–risk peers in the months leading up to breach announcements. This action effectively reduces their vulnerability to the broader contagion effects of a cyber attack.

This paper also contributes to the extensive mutual-fund performance literature by demonstrating that managerial skill today spans not only traditional fundamental and industry-timing signals but also pre-announcement cyber-risk indicators. Baker, Litov, Wachter, and Wurgler (2010) show that mutual fund trades forecast earnings surprises, indicating that managers can anticipate earnings-related fundamentals. Kim, Hwang, and Kim (2023) document that local mutual funds engage in anticipatory trading by reducing positions in firms before securities class action announcements, evidence of localized informational advantages. Ceccarelli, Evans, Glossner, Homanen, and Luu (2023) find that proactive ESG mutual fund managers' trades predict future changes in ESG ratings, demonstrating skill in the ESG dimension. Furthermore, Pástor, Stambaugh, and Taylor (2015) document marked improvements in fund managerial skill over the past decade. Building on these insights, I show that active managers further incorporate complex pre-announcement cyber-risk indicators—

particularly among funds disclosing cyber risk—to adjust positions earlier and earn significant flow rewards around breach events.

The rest of the paper is organized as follows. Section 2 describes the data, key variable definitions, and summary statistics. Section 3 documents active funds' pre-announcement trimming of high–cyber-risk positions. Section 4 examines how prospectus cyber-risk disclosures affect this behavior. Section 5 explores both industry- and stock-level heterogeneity, Section 6 analyzes the ensuing fund flow rewards, and Section 7 concludes.

2 Data and Summary Statistics

This section first describes the data sources and defines the variables used in this study, and then reports the sample's summary statistics.

2.1 Data Source and Sample Description

This paper draws on multiple data sources. Cyber-attack events are obtained from the Privacy Rights Clearinghouse (PRC) dataset, which reports each breach's entity name, reported date, breach type, number of records affected, organization type, and narrative description. I retain only incidents classified as HACK, indicating breaches due to external hacking or malware attacks, and exclude those involving educational (EDU), government or military (GOV), and nonprofit (NGO) organizations. I further restrict to breaches of personal information, as indicated in the description field. This dataset and filtering procedure are common in the literature (e.g., Dong, Li, Lin, and Yuan (2024); Florackis et al. (2023); Kamiya et al. (2021); Ottonello and Rizzo (2024)). I then manually match breached entities to CRSP identifiers and retain only public firms with valid Fama–French 48 industry codes. To focus on major cyber events, I limit the sample to incidents affecting more than one million records. I identify eight major cyber-attack announcements; details appear in Appendix Table A2. For each announcement, I construct an event window that spans two months before $(\tau - 2)$ through two months after $(\tau + 2)$ the announcement, thus capturing the funds' trading responses and preventing overlap across successive events. The sample, spans from 2012 to 2018, thus comprises these event windows.

I obtain monthly security prices and returns from the Center for Research in Securities Prices (CRSP) database. The firm-level financial ratios are from WRDS Industry Financial Ratio (WIFR) dataset. The stock-level cyber risk score is from Florackis et al. (2023). I obtain the firm-level data privacy policy score from the LSEG workspace dataset (also known as the Refinitiv dataset). This is a continuous measure scaled from 0 to 100 that reflects the relative robustness of a company's publicly disclosed processes to safeguard customer and public data (e.g., account numbers, passwords, personal identification details). The score is industry-adjusted via transparency weights to account for sector-specific disclosure norms.

I obtain mutual fund holdings and fund-level characteristics from CRSP Survivorship Bias Free Mutual Fund Database, which delivers more accurate coverage of mutual-fund information over the sample period (e.g., Zhu, 2020). Consistent with prior studies, I restrict the sample to U.S. domestic equity funds as classified by CRSP objective codes. To mitigate incubation bias (e.g., Evans, 2010), I include only funds that are at least two years old and have at least $5 million in assets under management. Since the event windows span only two months before and after each announcement, I restrict the sample to funds that voluntarily report holdings at a monthly frequency. Although funds are required to report holdings only quarterly, Elton, Gruber, and Blake (2011) show that funds voluntarily reporting monthly holdings exhibit average three–four basis point performance differences relative to matched non-reporters. This performance differences are both economically trivial and statistically insignificant, implying negligible performance-based selection bias. Moreover, there are roughly 60% of U.S. mutual funds voluntarily report holdings at this frequency.[2]

Starting from March 31, 2009, the U.S. Securities and Exchange Commission (SEC) has required mutual funds to deliver a summary prospectus that discloses each fund's principal risk factors, thereby facilitating investors' understanding of the risks they incur. I retrieve these prospectuses from the SEC EDGAR database and apply the textual-analysis procedure of Sheng et al. (2024) to identify explicit disclosures focusing on the cybersecurity risk.[3] Figure 1 plots the percentage of sample funds that disclose cybersecurity risk as a principal risk. This percentage remains at zero through 2014 and then

[2]See:https://www.morningstar.com/funds/when-it-comes-funds-read-fine-print?

[3]Example: `https://www.sec.gov/Archives/edgar/data/1331971/000113322815006714/e427256_497k.htm`

rises steadily, reaching about 10% by the end of 2018.

2.2 Variable Definition and Summary Statistics

I examine how cyber risk affects funds' trading by focusing on the monthly change in fund i's position in stock j. Following Gantchev, Giannetti, and Li (2024), I define the position change as

$$\text{Position Change}_{i,j,t} = \frac{Price_{j,t-1}\left[NumShares_{i,j,t} - NumShares_{i,j,t-1}\right]}{TNA_{i,t-1}}. \tag{1}$$

Let $Price_{j,t-1}$ denote the closing price of stock j in month $t-1$, and $NumShares_{i,j,t}$ the number of shares of j held by fund i in month t. The numerator isolates net purchases (or sales) in dollar terms by valuing share count changes at the lagged price, thus abstracting from valuation effects. This amount is then scaled by fund i's total net assets at month $t-1$. To control for the potential outliers, I winsorize it at 1% on both ends.

The key variable High Cyber Risk Dummy$_{j,t}$ (Low Cyber Risk Dummy$_{j,t}$) is an indicator equal to one if the cyber risk score of stock j at month t falls in the top (bottom) tercile of scores among firms in the same Fama–French 48 industry, and zero otherwise. By converting continuous cyber risk score (cosine similarity measures) into binary high- and low-cyber-risk indicators, I facilitate a clear high-vs.-low comparison and can attribute observed position changes to the sale of high-risk stocks or the purchase of low-risk stocks.

The High Data Privacy Dummy$_{j,t}$ is an indicator equal to one if the stock j's data privacy policy score falls in the top tercile of scores in month t. The Hacked Ind Dummy$_{j,t}$ is an indicator equal to one if the stock j belongs to the same Fama–French 48 industry as a firm that announces a major cyber attack in month τ and $t \in [\tau - 2, \tau + 2]$. The Disclose Cyber Risk Dummy$_{i,t}$ is an indicator variable equal to one if fund i's most recent summary prospectus, as filed on SEC EDGAR within the prior 12 months, discloses cybersecurity risk as a principal risk, and zero otherwise.

My sample comprises 683 actively managed mutual funds and, for comparison, 123 index funds. I include index funds as a passive control group—since they track benchmark indices, I do not anticipate systematic position changes around major cyber-attack announcements.

[Insert Table 1 here]

Table 1 reports holding-level summary statistics for active mutual funds and index funds. The mean Position Change of -0.0041% implies that, on average, active fund trims a single stock position by -0.41 basis points of lagged TNA each month. Translating the estimated 0.41 basis points position change into dollar terms with an average fund size of \$406.46 million yields a per-stock monthly adjustment of approximately $\$16,664.92$ ($exp(19.8230) * 0.0041\%$ see Table A3).

In this study, I include controls for stock characteristics potentially correlated with firm-level cyber risk, namely log market capitalization, tangibility, firm age, return on assets, etc (e.g., Jiang et al., 2024; Florackis et al., 2023). Summary statistics shows that active mutual funds, on average, tilting to large-capitalization stocks and those with stronger recent returns and higher profitability, relative to index funds. In the active mutual fund subsample, approximately 35% of held stocks have high data privacy policy scores, and about 9% of holdings fall in Fama–French 48 industries that experienced a major cyber-attack within the event window.

3 Mutual Fund's Trading on Cyber Risk Stocks

In this section, I analyze mutual funds' position changes around cyber attack announcements by conducting event-window regressions that contrast trading in high-cyber-risk versus low-cyber-risk stocks.

Kamiya et al. (2021) show that cyber attack announcements induce significant negative cumulative abnormal returns not only for the attacked firm but also for its peers, implying the spillover effect of the negative news. Jiang et al. (2024) further show that these spillovers are more pronounced among firms with greater data similarity to the victim firm. This characteristic is positively related to cyber risk. Taken together, the literature indicates that cyberattack spillovers extend beyond the victim firm and are particularly pronounced for firms with higher cyber risk.

Active mutual funds are found to have information advantage in industry level (Kacperczyk et al., 2005). Literature shows that the opportunistic insider trading often precedes cybersecurity breach an-

nouncements (e.g., Lin et al., 2020). The lag between the hacking event and its public announcement may reflect managers' incentives to attenuate investor reactions by timing disclosures (e.g., Foerderer and Schuetz, 2022). These complex pre-announcement signals—including, but not limited to, insider trades and strategic timing of disclosures—are examples of the rich information set that fund managers may draw on to inform their positioning.

Taken together, I form the hypothesis as follows: in the months before a major cyber-attack announcement, mutual funds reduce their holdings of high–cyber-risk stocks industry-wide.

To test this hypothesis, I use the Position Change$_{i,j,t}$ defined in equation 1 as a proxy for the fund i's trading behavior in stock j in month t.

To analyze the fund's position change around the announcement of the major cyber attacks in the sample, I conduct event studies as follows. Let τ_k denote the announcement month of the kth major cyber attack. For each fund–stock pair, I define the relative-time variable Time To Announcement $= t - \tau_k$, and select observations with Time To Announcement $\in \{-2, -1, 1, 2\}$, thereby constructing an event window from two months before to two months after each announcement. In this setup, Time To Announcement $= -2$ pools all observations two months prior to their respective announcements, Time To Announcement $= -1$ pools one month prior, and so on. For each month in the event window, I regress the mutual fund's position change onto the High Cyber Risk Dummy (or Low Cyber Risk Dummy). I also control for firm-level characterisitics including the lagged natural logrithm of the market capitalization, book-to-market ratio, tangibility, leverage, firm age and return on assets. These characteristics are found to correlate with the firm-level cyber risk. (e.g., Florackis et al., 2023; Jiang et al., 2024; Kamiya et al., 2021). I include fund by year fixed effects to capture unobserved, time-varying fund-level strategies, and stock fixed effects to account for unobserved, time-invariant stock characteristics that may affect fund's trading behavior and cyber risk. To be more specific, I conduct the following regression:

$$\text{Position Change}_{i,j,t} = \beta_h \text{ High Cyber Risk Dummy}_{j,t} + X_{j,t} + \theta_{j,t} + \lambda_j + \epsilon_{i,j,t} \tag{2}$$

$$\text{Position Change}_{i,j,t} = \beta_l \text{ Low Cyber Risk Dummy}_{j,t} + X_{j,t} + \theta_{j,t} + \lambda_j + \epsilon_{i,j,t} \quad (3)$$

where $\text{Position Change}_{i,j,t}$ is defined per Equation 1, $\text{High(Low) Cyber Risk Dummy}_{jt}$ is defined above, $X_{j,t}$ is a vector of stock-level control variables, $\theta_{j,t}$ is a fund by year fixed effect, λ_j ia a stock fixed effect, $\epsilon_{i,j,t}$ is the error term.

[Insert Table 2 here]

Panel A of Table 2 shows the regression result for the active mutual fund. In column (2), I find the relationship between the High cyber risk dummy is statistically negative related to the position change. In the economic magnitudes, this suggest that in the one month prior to the announcement of the major cyber attack, if the stock falls in the highest cyber risk tercile within its Fama-French 48 industry, the fund on average decrease the positions in the stock of 48.8% $(-0.0020/-0.0041)$ relative to the overall mean monthly position change in my sample. Translating the estimated -0.2 basis points position change into dollar terms with an average fund size of \$406.46 million yields a per-stock monthly adjustment of approximately $\$8,129.23$ $(exp(19.8230) * 0.0020\%$ see Table A3). This is consistent with my hypothesis that funds preemptively trim high cyber risk holdings. I also find in the previous month, mutual fund increase the position to the stocks with low cyber risk industry-wide, however, the relationship is not statistically significant.

I also include the index funds as a comparison. Index funds track their benchmark indices and thus not expected to adjust positions based on cyber risk. Panel B of Table 2 confirms that index funds exhibit no systematic position-change pattern around major cyber-attack announcements.

In summary, the result suggests that the active mutual funds preemptively trim industry-wide high cyber risk holdings in the months leading up to major cyber-attack announcements, such pattern is unobserved among index funds.

4 What Type of Funds More Actively Response?

In this section, I extend the previous analysis by grouping active funds into those whose most recent SEC summary prospectus explicitly discloses cybersecurity risk and those that do not.

Since March 31, 2009, the SEC has required mutual funds to deliver a summary prospectus disclosing each fund's principal risk factors, thereby enhancing investors' understanding of the risks they assume. I retrieve these prospectuses from the SEC EDGAR website and apply the textual-analysis methodology of Sheng et al. (2024) to identify cybersecurity-related disclosures.

I contruct the Disclose Cyber Risk Dummy$_{i,t}$, an indicator variable equal to one if fund's most recent summary prospectus, as filed on SEC EDGAR within the prior 12 months, discloses cybersecurity risk as a principal risk, and zero otherwise. Figure 1 shows the proportion of sample funds that disclose cybersecurity risk in their summary prospectus.

[Insert Figure 1 here]

I find that until 2014, funds start to report the cyber risk in their prospectus and the proportion continuously increasing until the end of the sample period, reaching to about 10%. This trajectory aligns with the findings of Sheng et al. (2024).

Next, I examine whether funds that disclose cybersecurity risk in their summary prospectus exhibit stronger pre-announcement trading in high-cyber-risk stocks. To this end, I augment the baseline regression in Table 2 by including the Disclose Cyber Risk Dummy$_{i,t}$ and its interaction with the High Cyber Risk Dummy$_{j,t}$. Because disclosure is reported at an annual frequency, I replace the fund by year fixed effects with fund fixed effects to ensure that variation in the disclosure dummy is not absorbed by the fixed-effect structure. Table 3 shows the result.

[Insert Table 3 here]

Column (1) of Table 3 shows that among the high cyber risk stocks within the industry, if the fund disclose the cyber risk in their prosepctus, these funds trim their high cyber risk position two months before the victim firm's announcement. The coefficient is statistically significant at 1% and economically meaningful-corresponding to approximately 134.15% $(-0.0055/-0.0041)$ of the sample's mean monthly position change. This shows that the fund disclose cyber risk adjust their high cyber risk stocks even earlier - two months before the announcement of the major cyber attack. In the one month prior, the coefficient is still negative yet statistically insignificant.

Moreover, Column (5) shows that funds disclosing cyber risk in their prospectus disproportionately increase allocations to low–cyber-risk stocks two months before the announcement of the major cyber attack. This interaction is statistically significant and represents roughly 109.76% of the sample's mean monthly position change.

Overall, Figure 1 illustrates a growing fraction of funds that disclose cyber risk in their summary prospectuses. Table 3 further reveals that, in the two months preceding major cyberattack announcements, these disclosing funds systematically trim high–cyber-risk exposures while increasing allocations to lower-risk positions.

5 Heterogeneous in Mutual Fund's Cyber Risk Related Trading

In this section, I examine whether mutual funds intensify trading in high cyber risk stocks within the same industry as the attacked firm and whether this trading pattern holds uniformly across all high-cyber-risk stocks.

5.1 Industry-level Heterogeneous

In the preceding section, I document that mutual funds preemptively trim high-cyber-risk holdings one month before major cyber-attack announcements, suggesting anticipatory trading. Since literature finds that industry peers suffer significant negative spillovers following the announcement of cyber attack (e.g., Florackis et al., 2023; Jiang et al., 2024). I now investigate whether fund position adjustment is even more pronounced for stocks within the same industry as the attacked firm. I construct Hacked Ind Dummy$_{j,t}$, an indicator equal to one if stock j's Fama–French 48 industry contains the firm that announces a major cyber attack in month τ and $t \in [\tau - 2, \tau + 2]$. As shown in Table 1, approximately 9% of fund–stock observations fall within attacked industries during the event window.

To assess whether funds adjust positions more aggressively in these industries, I augment the baseline specification by adding Hacked Ind Dummy$_{j,t}$ and its interaction with High Cyber Risk Dummy$_{j,t}$. All control variables and fixed effects are unchanged. The estimation results appear in

Table 4.

[Insert Table 4 here]

In column (1) of Table 4, the coefficient on the Hacked Ind Dummy$_{j,t}$ is -0.0047, indicating that two months before a major cyber-attack announcement, funds already reduce holdings in the stocks within the attacked industry. This reduction represents 114.63% of the average monthly position change ($-0.0047/-0.0041$), and is both economically substantial and statistically significant. Interestingly, in column (3), the coefficient is positively significant, suggesting that after the announcement of the major cyber attack, funds tilting back to the industry which they previously liquidate. The result is consistent with evidence that active mutual funds exploit industry-level informational advantages to time industry allocation (e.g., Avramov and Wermers, 2006).

In column (2), the coefficient on the Hacked Ind Dummy is still negative yet insignificant. However, the coefficient for the interaction term between the High Cyber Risk Dummy$_{j,t}$ and Hacked Ind Dummy$_{j,t}$ is -0.0041. This suggests that conditional on high cyber risk, stocks in the attacked industry on average are trimmed an additional 0.41 basis points of lagged TNA. This incremental effect is both statistically significant and economically large—approximately the same as the sample's mean monthly position change.

Furthermore, I find that conditional on the stocks within the hacked industry, the fund tilting their position to the low cyber risk stocks one month before the announcement of the major cyber attack. Column (6) shows that this effect corresponding to approximately 107.32% of the sample's mean monthly position change.

For the firms directly targeted by these breaches, however, I find no evidence of differential trading relative to the non-victim firms. As shown in Table A4, mutual funds do not adjust their positions in victim firms any differently than in non-victims in the months before or after disclosure, suggesting that rather than acting on firm-specific information (which may be legally or operationally constrained), mutual funds rely on broader industry-level signals to adjust their positions ahead of cyberattack disclosures.

In sum, Table 4 shows that mutual funds preemptively trim positions in the attacked industry prior to a major cyber attack announcement and subsequently tilted back. Moreover, within the attacked industry, funds shift allocations away from high-cyber-risk stocks to low-cyber-risk stocks before the announcement.

5.2 Stock-level Heterogeneous

The preceding results imply that funds tilt away from high–cyber-risk stocks toward low–cyber-risk stocks before an announcement. This raises a natural follow-on question: do funds treat all high-risk firms identically, or do they differentiate based on each firm's protective measures? In other words, even among firms classified as high cyber risk, those with stronger safeguards may be viewed more favorably—and, conversely, effective data protection could serve as a partial substitute for low baseline risk.

To test this hypothesis, I obtain the firm-level data privacy policy score from the LSEG database. This is a continuous measure scaled from 0 to 100 that reflects the relative robustness of a company's publicly disclosed processes to safeguard customer and public data (e.g., account numbers, passwords, personal identification details). I generate the High Data Privacy Dummy$_{j,t}$, an indicator equal to one if the stock j's data privacy policy score falls in the top tercile of scores at time t. To the best of my knowledge, I am the first to employ firm-level data privacy policy scores as a proxy for cybersecurity resilience in the cyber risk literature.

I extend the baseline specification in Table 2 by adding High Data Privacy Dummy$_{j,t}$ and its interaction with High Cyber Risk Dummy$_{j,t}$. Because High Data Privacy Dummy$_{j,t}$ exhibit little time-series variation within the same stock, I omit stock fixed effects to avoid absorbing the indicator's cross-sectional variation. Table 5 presents the results.

[Insert Table 5 here]

In Table 5, columns (2) and (6) report a positive and significant coefficient on High Data Privacy Dummy$_{j,t}$ in one month before the announcement, indicating that funds increase holdings in firms with stronger data privacy policies one month before a cyber-attack announcement. This effect

persists into the post-announcement period: columns (3)–(4) and (7)–(8) show significant positive coefficients at $t - \tau = 1$ and $t - \tau = 2$. These results suggest that mutual funds consider firms' data protection capabilities when adjusting portfolios around cyber-risk events.

Robust data-privacy protections aim to mitigate the adverse consequences of an actual breach, therefore, functionally acts as a substitute for low cyber risk. In column (1) of Table 5, the positive and statistically significant coefficient on the interaction between High Cyber Risk Dummy$_{j,t}$ and High Data Privacy Dummy$_{j,t}$ validates the hypothesis: conditional on high baseline cyber risk, stronger data-privacy policies are associated with larger fund position increases. This incremental effect is economically substantial, corresponding to approximately 90.24% of the sample's mean monthly position change.

In sum, Table 5 shows that mutual funds systematically increase allocations to firms with strong data privacy policies in the months before and after the major cyber-attack announcements, and that, conditional on high baseline cyber risk, these firms receive even larger position increases—consistent with robust data privacy safeguards serving as a substitute for low baseline cyber risk.

5.3 Do Funds Change Position Based on Price Signal?

In the previous analysis, I show that active funds adjust positions in high- and low-cyber-risk stocks in the months before major breach announcements. A potential concern is that these trades do not reflect fund's superior information advantage, but merely reflect funds' responses to contemporaneous price pressures—arising from other market participants who anticipate the announcement—instead of managers' own cyber-risk assessments. In this section, I test this alternative explanation.

I examine whether stock prices embed anticipatory information by estimating the monthly return regression. I regress the stock return on to the High Cyber Risk Dummy$_{j,t}$ (or Low Cyber Risk Dummy$_{j,t}$) with the stock-level controls and year and stock fixed effects. A significantly negative (positive) coefficient would imply that the price incorporates investors preemptive opinion for the high (low) cyber-risk stocks before the public disclosure of major cyber attack. Table 6 reports these estimates.

[Insert Table 6 here]

In Table 6, the coefficients on High (Low) Cyber Risk Dummy$_{j,t}$ at pre-and-post announcement are statistically indistinguishable from zero, indicating no evidence of pre-announcement price declines for high-cyber-risk (low-cyber-risk) stocks.

In summary, Table 6 shows that neither high- nor low-cyber-risk stocks exhibit anticipatory price declines, implying that mutual funds' pre-announcement trading cannot be explained solely by learning from price movements.

6 Flow Rewards for the Fund's Trading

The pre-announcement rebalancing of high(low) cyber risk stocks implies that active funds have information advantage and potentially a good industry-timing ability. This skill may be rewarded by investors through subsequent fund flows. In this section, I examine whether funds' preemptive cyber-risk trades generate positive flows in the month following each major cyber-attack announcement.

I follow literature and construct the fund flow in month t as follows:

$$Flow_{i,t} = \frac{TNA_{i,t} - TNA_{i,t-1} \times (1 + r_{i,t})}{TNA_{i,t-1}}, \tag{4}$$

where $TNA_{i,t}$ stands for the total net assets of fund i at the end of month t, and $r_{i,t}$ is the net return of fund i in month t. I winsorize the flow by 1% on both ends.

Since the flow is at fund-level, I aggregate the position change at the holding level and generate the following variables: Sell High Dummy$_{i,t}$ and Buy Low Dummy$_{i,t}$. To be more specific, for each fund i in each month t, I sum up its position changes separately for high- and low-cyber-risk stocks. Sell High Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's total position change in high-cyber-risk holdings ranks in the lowest third of all funds, and zero otherwise. Buy Low Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's total position change in low-cyber-risk holdings ranks in the lowest third of all funds, and zero otherwise. This ensures that when the Sell High Dummy (Buy Low Dummy) equals one, the fund's aggregate position change in high–cyber–risk holdings is

negative (positive).

In the fund flow regressions, I control for variables well-documented in the literature—past flows, past returns, Morningstar ratings, and other fund characteristics—to account for flow persistence and performance-chasing behavior (e.g., Sirri and Tufano, 1998; Del Guercio and Tkac, 2008; Ben-David et al., 2022). In particular, I include controls variables: flow at month t, $t-1$, and $t-2$; total net assets at t and $t-1$, expense ratio, turnover ratio;, Morningstar rating, fund age, raw monthly return, CAPM-adjusted return, and Carhart four-factor alpha, and aggregate position change. The summary statistics can be found in appendix. I include fund fixed effects to absorb unobserved, time-invariant fund characteristics, and year fixed effects to capture economy-wide shocks common to all funds in each year. To be more specific, I conduct the following regression:

$$Flow_{i,t+1} = \beta_s \, Sell\ High\ Dummy_{i,t} + X_{i,t} + \lambda_i + \tau_t + \epsilon_{i,t+1} \tag{5}$$

$$Flow_{i,t+1} = \beta_b \, Buy\ Low\ Dummy_{i,t} + X_{i,t} + \lambda_i + \tau_t + \epsilon_{i,t+1} \tag{6}$$

in which the $Flow_{i,t+1}$ is defined in equation 4, Sell High Dummy$_{i,t}$ and Buy Low Dummy$_{i,t}$ are defined above, $X_{i,t}$ is a vector of fund-level controls including the lagged terms that are available in month t, λ_i is a fund fixed effect, τ_t is a year fixed effect, and $\epsilon_{i,t+1}$ is an error term. Table 7 reports the result.

[Insert Table 7 here]

Column (6) of Table 7 shows that the Buy Low Dummy$_{i,t}$ is statistically significant at 5%, indicating that pre-announcement purchases of low-cyber-risk stocks tend to attract higher net inflows in the following month. Whereas sales of high-cyber-risk stocks, although positive, yet statistically insignificant in predicting subsequent flows. Considering that mutual funds predominantly serve retail investors—who are unlikely to monitor intra-fund trading—it is more plausible that this finding is driven by institutional investors.

Institutional investors, on the other hand, may scrutinize fund trading more closely. However, once controlling for recent fund performance and Morningstar ratings, retail-investor flows might

contain substantial idiosyncratic noise unrelated to cyber-risk–driven trading, thereby masking institutional investors' captial allocation decisions. The previous result may underestimate the flow-based rewards that accrue predominantly to institutional investors. To capture fund-level institutional investors participation, I compute fund-level institutional ownership by taking the TNA under the institutional share-class normalized by the total TNA for all share-classes for the fund. I generate High Inst Own Dummy, an indicator equal to one if fund i at time t's institutional ownership is equal to or greater than 90%, and zero otherwise.

I extend the specification in Table 7 by including the High Inst Own Dummy and its interaction with the Sell High Dummy (or Buy Low Dummy). Table 8 reports the result.

[Insert Table 8 here]

Column (6) shows that condition on funds purchase the low cyber risk stocks, if fund is mostly held by institutional investors, the next period flow is positive statistically significant at 1%. Conditional on pre-announcement purchases of low-cyber-risk stocks, funds with high institutional ownership experience net inflows that are 1 percentage points higher in the following month. This effect represents 27.93% standard deviations of the average monthly flow (0.0100/0.0358), underscoring its economic significance.

A potential concern is that pre-announcement purchases of low-cyber-risk stocks simply reflect superior fund performance rather than anticipatory cyber-risk trading. If this were the case, I would observe positive flow effects both before and after the announcement. However, Column (6) of Table 7 and Table 8 shows that the effect is significant at 5% only at $t - \tau = -1$. This temporal pattern implies that investors specifically reward anticipatory, cyber-risk–driven trades right after they observe the annoucement of the major cyber attack rather than generic performance-chasing.

In sum, pre-announcement purchases of low-cyber-risk stocks are rewarded with higher net inflows in the following month, and this effect is driven primarily by funds with high institutional ownership.

7 Conclusion

This study shows that U.S. active equity mutual funds systematically exploit the interval between a cyberattack's actual occurrence and its public disclosure to mitigate downside risk. I show that active funds trim industry-wide exposures to high–cyber-risk stocks one month before breach announcements—an effect absent in passive index funds—and that those formally disclosing cyber risk in their SEC prospectuses trade even earlier and tilt into lower-risk names. Further, within affected industries, funds differentiate among high-risk firms: those with superior data-privacy safeguards experience smaller pre-announcement cuts, consistent with a substitution effect. Tests of anticipatory price movements and return-predictive regressions find no evidence that these trades simply reflect mechanical reactions to early price declines, and a "flow reward" analysis confirms that successful pre-announcement reallocations generate significantly higher subsequent fund inflows.

Overall, this work reveals that active fund managers possess and deploy an informational edge in the fast-evolving domain of cyber risk, highlighting the importance of incorporating non-traditional risk factors into portfolio management.

References

Avramov, Doron, and Russ Wermers, 2006, Investing in mutual funds when returns are predictable, *Journal of Financial Economics* 81, 339–377.

Baker, Malcolm, Lubomir Litov, Jessica A Wachter, and Jeffrey Wurgler, 2010, Can mutual fund managers pick stocks? evidence from their trades prior to earnings announcements, *Journal of Financial and Quantitative Analysis* 45, 1111–1131.

Ben-David, Itzhak, Jiacui Li, Andrea Rossi, and Yang Song, 2022, What do mutual fund investors really care about?, *The Review of Financial Studies* 35, 1723–1774.

Ceccarelli, Marco, Richard B Evans, Simon Glossner, Mikael Homanen, and Ellie Luu, 2023, Esg skill of mutual fund managers .

Del Guercio, Diane, and Paula A Tkac, 2008, Star power: The effect of monrningstar ratings on mutual fund flow, *Journal of Financial and Quantitative Analysis* 43, 907–936.

Dong, Xi, Edward Xuejun Li, Xintian Lin, and Xin Yuan, 2024, Inside out: Who trade before the start of cyber attacks?, *Available at SSRN* .

Elton, Edwin J, Martin J Gruber, and Christopher R Blake, 2011, Holdings data, security returns, and the selection of superior mutual funds, *Journal of Financial and Quantitative Analysis* 46, 341–367.

Evans, Richard B, 2010, Mutual fund incubation, *The Journal of Finance* 65, 1581–1611.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber, 2023, Cybersecurity risk, *The Review of Financial Studies* 36, 351–407.

Foerderer, Jens, and Sebastian W Schuetz, 2022, Data breach announcements and stock market reactions: a matter of timing?, *Management Science* 68, 7298–7322.

Gantchev, Nickolay, Mariassunta Giannetti, and Rachel Li, 2024, Sustainability or performance? ratings and fund managers' incentives, *Journal of Financial Economics* 155, 103831.

Jiang, Hao, Naveen Khanna, Qian Yang, and Jiayu Zhou, 2024, The cyber risk premium, *Management Science* 70, 8791–8817.

Kacperczyk, Marcin, Clemens Sialm, and Lu Zheng, 2005, On the industry concentration of actively managed equity mutual funds, *The Journal of finance* 60, 1983–2011.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz, 2021, Risk management, firm reputation, and the impact of successful cyberattacks on target firms, *Journal of Financial Economics* 139, 719–749.

Kim, Taeyeon, Hyoseok David Hwang, and Hyun-Dong Kim, 2023, Do local investors know more? evidence from securities class actions, *Journal of Banking & Finance* 156, 107008.

Lin, Zhaoxin, Travis RA Sapp, Jackie Rees Ulmer, and Rahul Parsa, 2020, Insider trading ahead of cyber breach announcements, *Journal of Financial Markets* 50, 100527.

Ottonello, Giorgio, and Antonino Emanuele Rizzo, 2024, Do software companies spread cyber risk?, *Available at SSRN* .

Pástor, L'uboš, Robert F Stambaugh, and Lucian A Taylor, 2015, Scale and skill in active management, *Journal of financial economics* 116, 23–45.

Sheng, Jinfei, Nan Xu, and Lu Zheng, 2024, Do mutual funds walk the talk? evidence from fund risk disclosure, *Evidence from Fund Risk Disclosure (November 27, 2024)* .

Sirri, Erik R, and Peter Tufano, 1998, Costly search and mutual fund flows, *The journal of finance* 53, 1589–1622.

Zhu, Qifei, 2020, The missing new funds, *Management Science* 66, 1193–1204.

Table 1: Summary Statistics

This table reports summary statistics at the holding level for active mutual funds (Panel A) and index funds (Panel B). To mitigate incubation bias, we restrict the sample to funds that are at least two years old and have at least $5 million in assets under management. All variables are defined in the Appendix. For presentation clarity, the Position Change variable is scaled by 100 so it is expressed in percentage terms.

Panel A: Active Mutual Funds

Variable	Count	Mean	SD	5th pct	25th pct	Median	75th pct	95th pct
Position Change$_{i,j,t}$	1,778,034	-0.0041	0.1231	-0.1569	-0.0000	0.0000	0.0000	0.1350
High Cyber Risk Dummy$_{j,t}$	1,632,511	0.3486	0.4765	0.0000	0.0000	0.0000	1.0000	1.0000
Low Cyber Risk Dummy$_{j,t}$	1,632,511	0.2205	0.4146	0.0000	0.0000	0.0000	0.0000	1.0000
Ln Market Cap Lag1m	1,778,025	22.2731	1.7802	19.4699	21.0273	22.1183	23.4424	25.5463
BM	1,493,076	0.4718	0.4021	0.0690	0.2090	0.3830	0.6430	1.1210
Mom6_1	1,764,557	0.0808	0.2404	-0.2441	-0.0443	0.0669	0.1833	0.4296
Ret_Lag1m	1,775,802	0.0102	0.0947	-0.1319	-0.0369	0.0102	0.0560	0.1469
Tangibility	1,497,417	0.4588	0.1776	0.1612	0.3379	0.4694	0.5640	0.7606
Leverage	1,532,270	0.2459	0.2215	0.0000	0.0776	0.2206	0.3586	0.6087
Age	1,539,161	11.0764	4.0565	3.0000	9.0000	12.0000	15.0000	15.0000
ROA	1,537,620	0.1116	0.1615	-0.0670	0.0620	0.1220	0.1770	0.3050
High Data Privacy Dummy$_{j,t}$	1,778,034	0.4067	0.4912	0.0000	0.0000	0.0000	1.0000	1.0000
Disclose Cyber Risk Dummy$_{i,t}$	1,778,034	0.0523	0.2226	0.0000	0.0000	0.0000	0.0000	1.0000
Hacked Ind Dummy$_{j,t}$	1,778,034	0.0904	0.2868	0.0000	0.0000	0.0000	0.0000	1.0000

Panel B: Index Funds

Variable	Count	Mean	SD	5th pct	25th pct	Median	75th pct	95th pct
Position Change$_{i,j,t}$	1,750,847	0.0045	0.0923	-0.0108	0.0000	0.0000	0.0011	0.0308
High Cyber Risk Dummy$_{j,t}$	1,579,198	0.3189	0.4660	0.0000	0.0000	0.0000	1.0000	1.0000
Low Cyber Risk Dummy$_{j,t}$	1,579,198	0.2340	0.4234	0.0000	0.0000	0.0000	0.0000	1.0000
Ln Market Cap Lag1m	1,750,843	21.7384	1.8355	18.8627	20.4807	21.7198	23.0071	24.7981
BM	1,462,907	0.5115	0.4590	0.0790	0.2290	0.4190	0.6860	1.1840
Mom6_1	1,732,268	0.0586	0.2609	-0.3002	-0.0697	0.0471	0.1665	0.4264
Ret_Lag1m	1,748,940	0.0063	0.1084	-0.1525	-0.0443	0.0066	0.0549	0.1559
Tangibility	1,478,269	0.4673	0.1829	0.1619	0.3468	0.4742	0.5702	0.7989
Leverage	1,511,873	0.2475	0.2390	0.0000	0.0650	0.2158	0.3648	0.6375
Age	1,518,308	11.1507	4.2112	2.0000	9.0000	12.0000	15.0000	15.0000
ROA	1,516,339	0.0839	0.2106	-0.2360	0.0370	0.1070	0.1640	0.2900

Table 2: Mutual Fund Trading and Stocks' Cyber Risk

This table estimates the relationship between funds' position changes and stock cyber risk. Panel A reports results for active mutual funds; Panel B reports results for index funds. The sample covers the two months before through the two months after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, positive values months after). Position Change$_{i,j,t}$, defined in equation 1, is multiplied by 100 for clarity so that it is expressed in percentage points. High Cyber Risk Dummy$_{j,t}$ (Low Cyber Risk Dummyj,t) is an indicator equal to one if the cyber-risk score of stock j at time t falls in the top (bottom) tercile of scores among firms in the same Fama–French 48 industry, and zero otherwise. Columns (1)–(4) report results for stocks in the top tercile of cyber-risk scores within their Fama–French 48 industry. Columns (5)-(8) report results for stocks in the bottom tercile of cyber-risk scores within their Fama–French 48 industry. All regressions include fund × year and stock fixed effects. Standard errors, clustered at the fund × year level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Panel A: Active Mutual Funds

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Position Change$_{i,j,t}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
High Cyber Risk Dummy$_{j,t}$	0.0006	−0.0020**	0.0010	0.0001				
	(0.001)	(0.001)	(0.001)	(0.001)				
Low Cyber Risk Dummy$_{j,t}$					−0.0009	0.0011	−0.0005	0.0002
					(0.001)	(0.001)	(0.001)	(0.001)
Observations	312,025	325,021	344,290	349,654	312,025	325,021	344,290	349,654
Adj. R^2	0.1344	0.1105	0.1205	0.1326	0.1344	0.0945	0.1063	0.1326
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund × Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stock FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Panel B: Index Funds

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Position Change$_{i,j,t}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
High Cyber Risk Dummy$_{j,t}$	0.0014	−0.0001	0.0009	−0.0002				
	(0.001)	(0.000)	(0.001)	(0.000)				
Low Cyber Risk Dummy$_{j,t}$					−0.0020*	−0.0001	−0.0007	−0.0002
					(0.001)	(0.000)	(0.001)	(0.000)
Observations	292,209	324,477	331,081	336,830	292,209	324,477	331,081	336,830
Adj. R^2	0.6597	0.6062	0.3688	0.6800	0.6597	0.6011	0.3610	0.6761
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund × Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stock FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

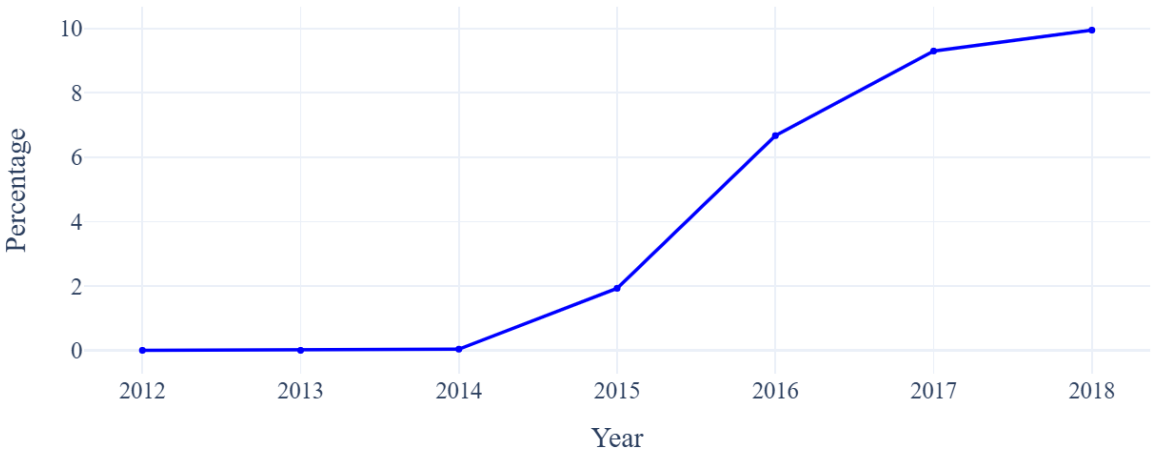

Figure 1: Percentage of Funds Report Cyber Risk in Prospectus

Table 3: Fund-Level Heterogeneity in Fund Rebalancing around Major Cyber Attacks

This table estimates the relationship between funds' position changes and stock cyber risk, comparing funds that disclose cyber risk as a stated concern in their summary prospectus with those without such disclosure. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Position Change$_{i,j,t}$, defined in equation 1, is multiplied by 100 for clarity so that it is expressed in percentage points. High Cyber Risk Dummy$_{j,t}$ (Low Cyber Risk Dummyj,t) is an indicator equal to one if the cyber-risk score of stock j at time t falls in the top (bottom) tercile of scores among firms in the same Fama–French 48 industry, and zero otherwise. Disclose Cyber Risk Dummy$_{i,t}$ is an indicator variable equal to one if fund i's most recent summary prospectus, as filed on SEC EDGAR within the prior 12 months, discloses cybersecurity risk as a principal risk, and zero otherwise. Columns (1)–(4) report results for stocks in the top tercile of cyber-risk scores within their Fama–French 48 industry. Columns (5)-(8) report results for stocks in the bottom tercile of cyber-risk scores within their Fama–French 48 industry. Control variables include Ln Market Cap Lag1m, BM, Mom6_1, Ret_Lag1m, Tangibility, Leverage, Age, and ROA. All regressions include fund and stock fixed effects. Standard errors, clustered at the fund level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Position Change$_{i,j,t}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
High Cyber Risk Dummy$_{j,t}$	0.0009	−0.0016**	0.0012*	−0.0006				
	(0.001)	(0.001)	(0.001)	(0.001)				
High Cyber Risk Dummy$_{j,t}$	−0.0055***	−0.0012	0.0011	−0.0013				
× Disclose Cyber Risk Dummy$_{i,t}$	(0.002)	(0.003)	(0.002)	(0.002)				
Low Cyber Risk Dummy$_{j,t}$					−0.0013	0.0013	−0.0008	−0.0005
					(0.001)	(0.001)	(0.001)	(0.001)
Low Cyber Risk Dummy$_{j,t}$					0.0045*	0.0019	−0.0006	−0.0023
× Disclose Cyber Risk Dummy$_{i,t}$					(0.002)	(0.003)	(0.002)	(0.002)
Disclose Cyber Risk Dummy$_{i,t}$	−0.0025	0.0024	0.0018	−0.0003	−0.0056	−0.015	0.0023	−0.0003
	(0.005)	(0.004)	(0.004)	(0.004)	(0.005)	(0.004)	(0.005)	(0.004)
Observations	312,026	325,013	344,291	349,656	312,026	325,013	344,291	349,656
Adj. R^2	0.0514	0.0337	0.0468	0.0614	0.0514	0.0337	0.0468	0.0508
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stock FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4: Industry-Level Heterogeneity in Fund Rebalancing around Major Cyber Attacks

This table estimates the relationship between funds' position changes and stock cyber risk focusing on the different industries. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Position Change$_{i,j,t}$, defined in equation 1, is multiplied by 100 for clarity so that it is expressed in percentage points. High Cyber Risk Dummy$_{j,t}$ (Low Cyber Risk Dummyj,t) is an indicator equal to one if the cyber-risk score of stock j at time t falls in the top (bottom) tercile of scores among firms in the same Fama–French 48 industry, and zero otherwise. Hacked Ind Dummy$_{j,t}$ is an indicator equal to one if the stock belongs to the same Fama–French 48 industry as a firm that announces a major cyber attack in month τ and $t \in [\tau - 2, \tau + 2]$. Columns (1)–(4) report results for stocks in the top tercile of cyber-risk scores within their Fama–French 48 industry. Columns (5)-(8) report results for stocks in the bottom tercile of cyber-risk scores within their Fama–French 48 industry. Control variables include Ln Market Cap Lag1m, BM, Mom6_1, Ret_Lag1m, Tangibility, Leverage, Age, and ROA. All regressions include fund × year and stock fixed effects. Standard errors, clustered at the fund × year level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Position Change$_{i,j,t}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
High Cyber Risk Dummy$_{j,t}$	0.0007	−0.0016**	0.0012*	0.0003				
	(0.001)	(0.001)	(0.001)	(0.001)				
High Cyber Risk Dummy$_{j,t}$	−0.0009	−0.0041*	−0.0015	−0.0030				
× Hacked Ind Dummy$_{j,t}$	(0.002)	(0.002)	(0.002)	(0.002)				
Low Cyber Risk Dummy$_{j,t}$					−0.0011	0.0008	−0.0002	−0.0001
					(0.001)	(0.001)	(0.001)	(0.001)
Low Cyber Risk Dummy$_{j,t}$					0.0023	0.0044*	−0.0039*	0.0014
× Hacked Ind Dummy$_{j,t}$					(0.003)	(0.002)	(0.002)	(0.002)
Hacked Ind Dummy$_{j,t}$	−0.0047***	−0.0009	0.0045***	0.0008	−0.0055***	−0.0033**	0.0048***	−0.0006
	(0.002)	(0.002)	(0.002)	(0.001)	(0.002)	(0.002)	(0.002)	(0.001)
Observations	312,025	325,021	344,290	349,654	312,025	325,021	344,290	349,654
Adj. R^2	0.1345	0.1105	0.1205	0.1472	0.1345	0.0945	0.1063	0.1325
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund × Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stock FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5: Firm-Level Heterogeneity in Fund Rebalancing around Major Cyber Attacks

This table estimates the relationship between funds' position changes and stock cyber risk focusing on the firms with different level data privacy policy. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Position Change$_{i,j,t}$, defined in equation 1, is multiplied by 100 for clarity so that it is expressed in percentage points. High Cyber Risk Dummy$_{j,t}$ (Low Cyber Risk Dummyj,t) is an indicator equal to one if the cyber-risk score of stock j at time t falls in the top (bottom) tercile of scores among firms in the same Fama–French 48 industry, and zero otherwise. High Data Privacy Dummyj,t is an indicator equal to one if the stock j's data privacy policy score falls in the top tercile of scores at time t. Columns (1)–(4) report results for stocks in the top tercile of cyber-risk scores within their Fama–French 48 industry. Columns (5)-(8) report results for stocks in the bottom tercile of cyber-risk scores within their Fama–French 48 industry. Control variables include Ln Market Cap Lag1m, BM, Mom6_1, Ret_Lag1m, Tangibility, Leverage, Age, and ROA. All regressions include fund × year fixed effects. Standard errors, clustered at the fund × year level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Position Change$_{i,j,t}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
High Cyber Risk Dummy$_{j,t}$	−0.0007	−0.0016**	0.0010	−0.0002				
	(0.001)	(0.001)	(0.001)	(0.001)				
High Cyber Risk Dummy$_{j,t}$	0.0037***	0.0013	−0.0001	−0.0002				
× High Data Privacy Dummy$_{j,t}$	(0.001)	(0.001)	(0.001)	(0.001)				
Low Cyber Risk Dummy$_{j,t}$					−0.0017**	0.0011	−0.0007	0.0006
					(0.001)	(0.001)	(0.001)	(0.001)
Low Cyber Risk Dummy$_{j,t}$					0.0012	−0.0008	0.0005	−0.0003
× High Data Privacy Dummy$_{j,t}$					(0.001)	(0.001)	(0.001)	(0.001)
High Data Privacy Dummy$_{j,t}$	0.0002	0.0015**	0.0022***	0.0014*	−0.0005	0.0030***	0.0017**	0.0017**
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Observations	312,138	325,099	344,372	349,745	312,138	325,099	344,372	349,745
Adj. R^2	0.1163	0.0936	0.1118	0.1304	0.1231	0.1004	0.1118	0.1370
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund × Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6: Stock Return around Major Cyber Attacks

This table estimates the relationship between stock return and the cyber risk around the announcement of major cyber attack. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Position Change$_{i,j,t}$, defined in equation 1, is multiplied by 100 for clarity so that it is expressed in percentage points. High Cyber Risk Dummy$_{j,t}$ (Low Cyber Risk Dummyj, t) is an indicator equal to one if the cyber-risk score of stock j at time t falls in the top (bottom) tercile of scores among firms in the same Fama–French 48 industry, and zero otherwise. Columns (1)–(4) report results for funds sell high cyber risk stocks. Columns (5)-(8) report results for funds buy low cyber risk stocks. Control variables include Ln Market Cap Lag1m, BM, Mom6_1, Ret_Lag1m, Tangibility, Leverage, Age, and ROA. All regressions include fund and year fixed effects. Standard errors, clustered at the fund level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
					Ret$_{j,t}$			
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
High Cyber Risk Dummy$_{j,t}$	0.0032	−0.0029	0.0007	0.0002				
	(0.002)	(0.002)	(0.003)	(0.003)				
Low Cyber Risk Dummy$_{j,t}$					0.0006	0.0027	−0.0015	0.0036
					(0.003)	(0.003)	(0.003)	(0.003)
Observations	18,273	18,296	18,070	18,074	18,273	18,296	18,070	18,074
Adj. R^2	0.0688	0.3571	0.2431	0.2728	0.2396	0.2113	0.0712	0.2729
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stock FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 7: Fund Flows around Major Cyber Attacks

This table estimates the relationship between fund flows and fund's activity in trading cyber risk related stocks. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Sell High Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's aggregate position change in high cyber risk stocks is lower than zero, and zero otherwise. Buy Low Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's aggregate position change in low cyber risk stocks is greater than zero, and zero otherwise. Columns (1)–(4) report results for funds sell high cyber risk stocks. Columns (5)-(8) report results for funds buy low cyber risk stocks. Control variables include Flow$_t$, Flow$_{t-1}$, Flow$_{t-2}$, TNA$_t$, TNA$_{t-1}$, Exp Ratio, Turn Ratio, Fund Rating, Fund Age, Raw Return, CAPM Alpha, FF4 Alpha. All regressions include fund and year fixed effects. Standard errors, clustered at the fund level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Flow$_{i,t+1}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
Sell High Dummy$_{i,t}$	−0.0022	0.0010	0.0008	−0.0001				
	(0.002)	(0.002)	(0.001)	(0.001)				
Buy Low Dummy$_{i,t}$					0.0007	0.0042**	0.0000	0.0026*
					(0.002)	(0.002)	(0.001)	(0.001)
Observations	2,338	2,379	2,509	2,562	2,338	2,379	2,509	2,562
Adj. R^2	0.1937	0.3904	0.3006	0.4120	0.3646	0.3920	0.4436	0.2640
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 8: Fund Flows around Major Cyber Attacks

This table estimates the relationship between fund flows and fund's activity in trading cyber risk related stocks. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Sell High Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's aggregate position change in high cyber risk stocks is lower than zero, and zero otherwise. Buy Low Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's aggregate position change in low cyber risk stocks is greater than zero, and zero otherwise. High Inst Own Dummy$_{i,t}$ is an indicator equal to one if fund i at time t's institutional ownership is equal to or greater than 90%, and zero otherwise. Columns (1)–(4) report results for funds sell high cyber risk stocks. Columns (5)-(8) report results for funds buy low cyber risk stocks. Control variables include Flow$_t$, Flow$_{t-1}$, Flow$_{t-2}$, TNA$_t$, TNA$_{t-1}$, Exp Ratio, Turn Ratio, Fund Rating, Fund Age, Raw Return, CAPM Alpha, FF4 Alpha. All regressions include fund and year fixed effects. Standard errors, clustered at the fund level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	Flow$_{i,t+1}$							
Time to Announcement (months)	−2	−1	1	2	−2	−1	1	2
Sell High Dummy$_{i,t}$	−0.0017	0.0025	−0.0002	−0.0009				
	(0.002)	(0.002)	(0.001)	(0.002)				
Sell High Dummy$_{i,t}$	−0.0028	−0.0075	0.0032	0.0038				
× High Inst Own Dummy$_{i,t}$	(0.006)	(0.005)	(0.004)	(0.004)				
Buy Low Dummy$_{i,t}$					0.0011	0.0025	0.0006	0.0017
					(0.002)	(0.002)	(0.001)	(0.002)
Buy Low Dummy$_{i,t}$					−0.0024	0.0100*	−0.0026	0.0043
× High Inst Own Dummy$_{i,t}$					(0.005)	(0.006)	(0.003)	(0.004)
High Inst Own Dummy$_{i,t}$	0.0010	0.0011	−0.0033	−0.0012	0.0008	−0.0036	−0.0012	−0.0016
	(0.006)	(0.005)	(0.004)	(0.004)	(0.006)	(0.006)	(0.003)	(0.003)
Observations	2,338	2,379	2,509	2,562	2,338	2,379	2,509	2,562
Adj. R^2	0.1931	0.3914	0.3005	0.4123	0.3647	0.2296	0.3002	0.2639
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fund FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Appendix

Table A1: Variable Definitions

Variable Name	**Definition**
Position Change	$\text{Position Change}_{i,j,t} = \dfrac{Price_{j,t-1}\,[NumShares_{i,j,t} - NumShares_{i,j,t-1}]}{TNA_{i,t-1}}$.
High Cyber Risk Dummy$_{j,t}$	Indicator = 1 if stock j's cyber-risk score at t is in the top tercile within its Fama–French 48 industry; 0 otherwise.
Low Cyber Risk Dummy$_{j,t}$	Indicator = 1 if stock j's cyber-risk score at t is in the bottom tercile within its Fama–French 48 industry; 0 otherwise.
Ln Market Cap Lag1m	Natural logarithm of firm j's market capitalization at month-end $t-1$.
BM	Book-to-market ratio of firm j.
Mom6_1	Six-month momentum.
Ret_Lag1m	Monthly return of firm j in month $t-1$.
Tangibility	Firm j's tangibility ratio.
Leverage	Firm j's leverage ratio.
Age	Firm j's age in years.
ROA	Return on assets for firm j.
High Data Privacy Dummy$_{j,t}$	Indicator = 1 if firm j's data-privacy policy score at t is in the top tercile; 0 otherwise.
Disclose Cyber Risk Dummy$_{i,t}$	Indicator = 1 if fund i's most recent summary prospectus (within 12 months of t) discloses cyber risk as a principal risk; 0 otherwise.
Hacked Ind Dummy$_{j,t}$	Indicator = 1 if stock j belongs to the same Fama–French 48 industry as a firm that announces a cyberattack at τ and $t \in [\tau-2, \tau+2]$; 0 otherwise.
Flow	$Flow_{i,t} = \dfrac{TNA_{i,t} - TNA_{i,t-1} \times (1 + r_{i,t})}{TNA_{i,t-1}}$.
Sell High Dummy$_{i,t}$	Indicator = 1 if fund i at time t's total position change in high-cyber-risk holdings ranks in the lowest third of all funds; 0 otherwise.
Buy Low Dummy$_{i,t}$	Indicator = 1 if fund i at time t's total position change in low-cyber-risk holdings ranks in the highest third of all funds; 0 otherwise.
TNA	Fund i's total net assets at month-end t.
Expense Ratio	Share-class expense ratio (value-weighted to fund level).
Turnover Ratio	Share-class portfolio turnover (value-weighted).
Fund Rating	Value-weighted Morningstar rating for fund i.
Raw Ret	Fund i's raw monthly return.
Alpha (CAPM)	CAPM-adjusted return for fund i.
Alpha (4-factors)	Carhart four-factor alpha for fund i.

Table A2: Summary of Major Cyber Attack Incidents

Company	Reported Date	Records	Org. Type	Description
LinkedIn	06/06/2012	6,500,000	BSO	On June 6, 2012, LinkedIn experienced a security breach resulting in the loss of encrypted passwords, potentially compromising around 6.5 million user accounts. They assured that no email addresses were stolen and that financial information remained secure. Affected members were notified to change their passwords.
Target	19/12/2013	40,000,000	BSR	Between November 27 and December 15, 2013, Target Corporation suffered a data breach affecting approximately 40 million customers who used credit or debit cards at its U.S. stores. Authorities and financial institutions were notified, and a third-party forensics firm assisted in the investigation.
Staples Inc.	19/12/2014	1,160,000	BSR	Staples confirmed a data breach on December 19, 2014, impacting 115 stores between July 20 and September 16, 2014. Approximately 1.16 million payment cards were compromised by malware on point-of-sale systems. Staples provided free credit monitoring services to affected customers.
Yahoo Inc.	14/12/2016	1,000,000,000	BSO	In August 2013, an unauthorized third party stole data from over one billion Yahoo user accounts. The breach included names, email addresses, telephone numbers, dates of birth, hashed passwords, and security questions. It was revealed to Yahoo by law enforcement in November 2016 and publicly disclosed on December 14, 2016.
Equifax	07/09/2017	145,500,000	BSF	Equifax experienced a data breach through a website application vulnerability, with unauthorized access occurring from mid-May through July 29, 2017, impacting approximately 145.5 million U.S. consumers. Personal information including names, Social Security numbers, birth dates, and addresses were accessed, along with driver's license numbers and credit card numbers for some. The breach was announced on September 7, 2017, and it was reported to law enforcement.
Equifax	01/03/2018	2,400,000	BSF	Equifax experienced a cybersecurity incident in which names and partial driver's license information of approximately 2.4 million U.S. consumers were stolen. This breach update was announced on March 1, 2018, though the original incident occurred at an earlier, unspecified date.
Under Armour	29/03/2018	150,000,000	BSO	In late February 2018, Under Armour Inc. dba MyFitnessPal experienced a data breach in which an unauthorized user accessed approximately 150 million user accounts, acquiring usernames, email addresses, and hashed passwords. Under Armour engaged law enforcement and a data security firm, notified users to change passwords, and updated its website.
Marriott Int.	30/11/2018	500,000,000	BSO	An unauthorized party gained access to Marriott International Inc.'s Starwood guest reservation database from 2014 until September 10, 2018. Personal information for up to 500 million guests was involved, including names, contact details, passport numbers, and encrypted payment card numbers. Encryption keys may also have been compromised.

Table A3: Summary Statistics for Fund Flows and Controls

This table reports summary statistics of fund flow, performance and other characteristics. Sell High Dummy$_{i,t}$ is an indicator equal to one if fund i in month t's aggregate position change in high cyber risk stocks is lower than zero, and zero otherwise. Buy Low Dummy$_{i,t}$ is an indicator equal to one if fund i in month t's aggregate position change in low cyber risk stocks is greater than zero, and zero otherwise. High Inst Own Dummy$_{i,t}$ is an indicator equal to one if fund i in month t's institutional ownership is equal to or greater than 90%, and zero otherwise. Position Change is the fund's aggregate position change for all holding stocks in month t. TNA is the natural logrithm of the fund's total net asset. Fund Rating is the fund's Morningstar fund rating. I obtain the share-class level rating and calculate the fund-level rating weight by the fund's TNA. Fund Age is the fund's oldest share-class in years since its inception date. For each month, I regress each fund's monthly return on the market excess return (Carhart four-factors) using a 24-month window and take the intercept as the Alpha (CAPM) (Alpha (4-factors)).

Variable	Count	Mean	SD	5th pct	25th pct	Median	75th pct	95th pct
Flow$_{t+1}$	11,409	-0.0050	0.0358	-0.0508	-0.0147	-0.0059	0.0027	0.0436
Sell High Dummy$_{i,t}$	11,446	0.3489	0.4766	0.0000	0.0000	0.0000	1.0000	1.0000
Buy Low Dummy$_{i,t}$	11,446	0.3454	0.4755	0.0000	0.0000	0.0000	1.0000	1.0000
High Inst Own Dummy$_{i,t}$	11,446	0.2077	0.4057	0.0000	0.0000	0.0000	0.0000	1.0000
Flow$_{t}$	11,423	-0.0041	0.0354	-0.0484	-0.0145	-0.0057	0.0034	0.0455
Flow$_{t-1}$	11,396	-0.0054	0.0375	-0.0537	-0.0158	-0.0065	0.0027	0.0469
Flow$_{t-2}$	11,364	-0.0050	0.0377	-0.0519	-0.0151	-0.0063	0.0026	0.0441
TNA	11,446	19.8196	1.7206	16.9553	18.5196	19.9175	21.1223	22.4983
TNA$_{t-1}$	11,423	19.8230	1.7190	16.9640	18.5286	19.9185	21.1297	22.4984
Expense Ratio	11,438	0.0106	0.0030	0.0061	0.0090	0.0105	0.0124	0.0152
Turnover Ratio	11,396	0.6699	0.5596	0.1400	0.3100	0.5318	0.8600	1.6200
Fund Rating	10,258	2.9250	1.0062	1.0088	2.0371	3.0000	3.7988	4.6653
Fund Age	11,446	18.6748	12.4032	3.7479	10.5671	16.3479	23.9288	44.1507
Raw Ret	11,446	0.0076	0.0482	-0.0892	-0.0167	0.0144	0.0364	0.0786
Alpha (CAPM)	11,446	-0.0010	0.0036	-0.0069	-0.0031	-0.0009	0.0011	0.0046
Alpha (4-factors)	11,446	-0.0003	0.0030	-0.0049	-0.0020	-0.0004	0.0013	0.0043

Table A4: Fund Rebalancing for the Victim Firms

This table estimates the relationship between funds' position changes and whether the firm is the victim firm during each event window. The sample covers the two months before through the two month after the announcement of a major cyber attack. Time to Announcement measures months relative to the announcement (negative values indicate months before, position values months after). Position Change$_{i,j,t}$ is defined in 1. Victim Dummy$_{j,t}$ is an indicator equal to one if the firm j is the attacked victim during the event window, and zero otherwise. Control variables include Ln Market Cap Lag1m, BM, Mom6_1, Ret_Lag1m, Tangibility, Leverage, Age, and ROA. All regressions include fund × year and stock fixed effects. Standard errors, clustered at the fund × year level, are in parentheses. * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

	(1)	(2)	(3)	(4)
	Position Change			
Time to Announcement (months)	−2	−1	1	2
Victim Dummy$_{j,t}$	−0.0148	−0.0109	−0.0115	−0.0047
	(0.014)	(0.011)	(0.010)	(0.010)
Observations	338,407	352,545	373,934	381,348
Adj. R^2	0.1191	0.0922	0.1194	0.1307
Controls	Yes	Yes	Yes	Yes
Fund × Year FE	Yes	Yes	Yes	Yes
Stock FE	Yes	Yes	Yes	Yes