Impact of cybersecurity incidents on stock prices

Richard Ostertág, Martin Stanek*

Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava, Slovakia

Abstract

We analyze the short-term impact of cybersecurity incidents on the stock prices of affected companies. The dataset used in our analysis consists of mandatory filings required by the Securities and Exchange Commission. In addition to observing a measurable impact of these filings, we propose and test the relative price movement with respect to a sector benchmark. We also experiment with automatic severity assessment of cybersecurity incidents using a LLM.

Keywords

Cybersecurity, Incident, Stock price

1. Introduction

Cybersecurity incidents, such as data breaches, ransomware attacks, denial-of-service attacks, and other events, impact companies and can hinder their business operations. The immediate response and follow-up activities after an incident often incur extra expenses and resources. Estimating this impact is challenging, both internally and externally. Companies usually focus on damage control, and disclose only the details they are legally required to share.

A common approach to assess the economic impact of cybersecurity incidents is to analyze their effect on stock price performance. In the U.S. equity markets, publicly traded companies are mandated to disclose any cybersecurity incident that is determined to be material within four business days. The Securities and Exchange Commission (SEC) adopted this requirement as Item 1.05 of Form 8-K in 2023 [6]. Additionally, the Commission provided further clarification on what should be reported and how to determine the materiality of a cybersecurity incident in May 2024[1].

For the purpose of the Form 8-K, the definition of the term *cybersecurity incident* is provided by 17 CFR § 229.106[2].

> *Cybersecurity incident* means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

The impact of cybersecurity incidents on stock prices can be of interest to various groups, each with different motivations and interpretation of the results, although they must consider other relevant information in their decisions:

- Shareholders (investors) are interested in understanding the impact of cybersecurity incidents on the market capitalization of a company and their investments.
- Managers and cybersecurity professionals aim to reflect the expected impact in their cybersecurity plans and actions.
- Traders consider the possibility of a trading opportunity in light of the information provided.

ITAT'25: Information Technologies – Applications and Theory, September 26–30, 2025, Telgárt, Slovakia

*Corresponding author.

richard.ostertag@fmph.uniba.sk (R. Ostertág); martin.stanek@fmph.uniba.sk (M. Stanek)

0000-0002-6560-1515 (R. Ostertág)

[1] https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-05212024

[2] https://www.ecfr.gov/current/title-17/section-229.106

Related work

The impact of cybersecurity incidents on stock prices was analyzed in various publications. The effect of data breaches on share price is analyzed in [1]. The data includes breaches spanning from 2007 to 2023, and includes 118 companies. Even though the analysis confirmed an expected negative impact, it is unclear how data breaches are selected. Moreover, the stock price is compared to the NASDAQ composite index. We think this is problematic, since in the last 15 years the NASDAQ generally outperformed the market as a whole. Therefore, given a random company and a random date, one can reasonably expect that NASDAQ outperforms, which might slightly distort the results.

A systematic review of 37 papers was published in 2016 [7]. The authors conclude that the majority of studies report statistical significance of the impact of security events on stock prices, but there are no quantitative results in the review. Moreover, the papers are relatively old, with majority being published before 2011. Given the constant changes in the attack landscape, countermeasures, preparedness, and other aspects of cybersecurity, the findings of these studies might not be entirely applicable to the current situation.

A recent study [3] uses data breach notification laws to assess the impact of these events on stock price, analyzing a sample of 3,615 U.S. public firms over the period 1997–2019. The main result is that the adoption of data breach notification laws leads to higher future stock price crash risk, confirming the findings of previous works like [5]. Extrapolating to the mandatory reporting of material cybersecurity incidents, we might expect similar outcomes in the future.

The more popular presentations, such as [2], focus mostly on well-known cases with large-scale media attention. Consequently, the dataset is biased, and the conclusions and perceived impact can be skewed.

Our contribution

We emphasize the importance of a clearly defined dataset, where inclusion criteria prevent possible biases. In our case, the dataset is implied by a regulatory framework, and it is obtained via the SEC's online service. It contains all Form 8-K filings with Item 1.05. A detailed description of data acquisition, cleaning, and post-processing is discussed in Section 2.

There are two basic approaches to evaluate stock price movements, and we employ both. The first approach examines the change in price itself. The second approach involves comparing price changes with a benchmark, assessing how the stock underperforms or overperforms relative to the benchmark. Rather than using broad market benchmarks like S&P 500 or more narrowly focused but potentially unrelated indices like NASDAQ, we opt for sector benchmarks. We evaluate the relative performance of the stock in relation to its corresponding sector's ETF. This evaluation is detailed in Section 3. We caution readers to carefully interpret any results, given the dataset is still relatively small, with only 48 fillings. This paper is an expanded version of [8] where only 37 fillings were available for analysis.[3]

An additional variable that contributes to the impact of cybersecurity incidents is their severity. The Item 1.05 in Form 8-K filings includes a brief description of the impact. We performed a simple zero-shot analysis of these texts and employed a large language model to classify the incidents into three categories: High, Medium, and Low. The results of this experiment are detailed in Section 4.

2. The dataset

The dataset containing relevant filings was constructed following these steps:

1. Data search and download: The SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system is used for automated search of 8-K form fillings containing the strings "Material Cybersecurity Incident" or "Material Cybersecurity Incidents" or "Item 1.05". When a company amends

[3]We also extend analysis window to 20 days after filing and use better LLM for classification.

the original filing, this usually happens when the information in Item 1.05 becomes available or can be determined, we process and analyze this amended 8-K form as a separate record.
2. Data cleaning: We manually inspect all results to remove entries that are not real Item 1.05 filings – mostly entries where this item was only mentioned in other context. We also fix duplicate entries, entries without a ticker, and other errors.
3. Enhancing data: We add additional attributes for each record in the dataset[4] – sector, benchmark ticker, performance of the stock itself and its relative performance with respect to the benchmark, as well as the relevant text part of the filing describing the cybersecurity incident.

To compare relative price movements, we use 11 sectors defined by the Global Industry Classification Standard [4]. For benchmark, we opted for ETFs provided by State Street Global Advisors that aim to replicate the performance of individual S&P 500 sectors, see Table 1.

Table 1
Sectors and the corresponding benchmark tickers.

Sector	benchmark ticker
Consumer Cyclical/Discretionary	XLY
Consumer Defensive/Staples	XLP
Energy	XLE
Financial Services	XLF
Health Care	XLV
Industrials	XLI
Technology	XLK
Materials	XLB
Real Estate	XLRE
Communication Services	XLC
Utilities	XLU

We analyze the stock price 5 days prior and 20 days after the filing day. We base our calculation on Close price only, i.e., intraday fluctuations are not evaluated. All further mentions of price denote the Close price. Similarly, we do not take into account a time when the filing was done, whether it was before, during or after trading hours.

In order to prepare the historical stock price data for further analysis and aggregation, we fill gaps with missing price (which are typically days where markets are closed), with the nearest previously-known price. For example, Sunday and Saturday prices are set to the previous Friday's price.

Performance of the stock. Let p_i be the price of a stock at the filing day plus/minus i days, for $i \in \{-5, \dots, 20\}$. We calculate the relative performance of the stock in our interval as a series $r_{-5}, \dots, r_{20}$, where $r_i = (p_i - p_0)/p_0$, for $i \in \{-5, \dots, 20\}$. The relative performance at the filing day is trivially $r_0 = 0$.

Relative performance of the stock with respect to the benchmark. Let b_i be the price of the benchmark for the stock's sector at the filing day plus/minus i days, for $i \in \{-5, \dots, 20\}$. We calculate the relative performance of the stock with respect to the benchmark as a series $\Delta_{-5}, \dots, \Delta_{20}$, where $\Delta_i = (b_i - b_0)/b_0 - r_i$, for $i \in \{-5, \dots, 20\}$. It is easy to see that $\Delta_0 = 0$.

3. Results – analyzing the impact

The dataset contains $n = 48$ relevant filings from July 2024 to June 2025. Records span across 10 sectors, some with multiple incidents, while one sector (Utilities) is without a single filing. On average, the

[4]We use Python's yfinance library to access Yahoo Finance data.

stock price declined -3.09%, -4.40%, and -2.73% in 5, 10, and 20 days after the filing, respectively. Table 2 shows these statistics for each sector observed in our dataset.

Table 2
Impact of cybersecurity incidents in different sectors (5, 10 and 20 days after the filing).

		Stock price			Benchmark delta		
Sector	count	r_5	r_{10}	r_{20}	Δ_5	Δ_{10}	Δ_{20}
Full dataset	48	-3.09%	-4.40%	-2.73%	-3.12%	-4.93%	-4.20%
Technology	10	-3.09%	-6.25%	-7.02%	-3.63%	-7.65%	-11.59%
Financial Services	9	-2.48%	-1.00%	4.40%	-2.33%	-1.48%	3.61%
Consumer Cyclical	9	-0.26%	0.62%	1.36%	-0.45%	-0.47%	0.37%
Health Care	6	-0.50%	-1.05%	0.53%	0.01%	-0.90%	-0.54%
Industrials	4	-21.36%	-28.93%	-29.07%	-20.38%	-28.33%	-29.14%
Consumer Defensive	3	1.24%	0.76%	2.88%	0.53%	0.09%	2.42%
Communication Services	3	-1.88%	-5.02%	-4.00%	-1.19%	-3.70%	-2.07%
Real Estate	2	1.19%	1.50%	-0.76%	-0.57%	-1.42%	-2.28%
Basic Materials	1	-1.09%	-7.35%	4.46%	-3.40%	-7.82%	1.60%
Energy	1	-3.67%	-6.10%	0.91%	-0.30%	-2.26%	-0.04%

The average movement of a stock starting five days prior to the filing and ending twenty days after the filing is shown in Figure 1.

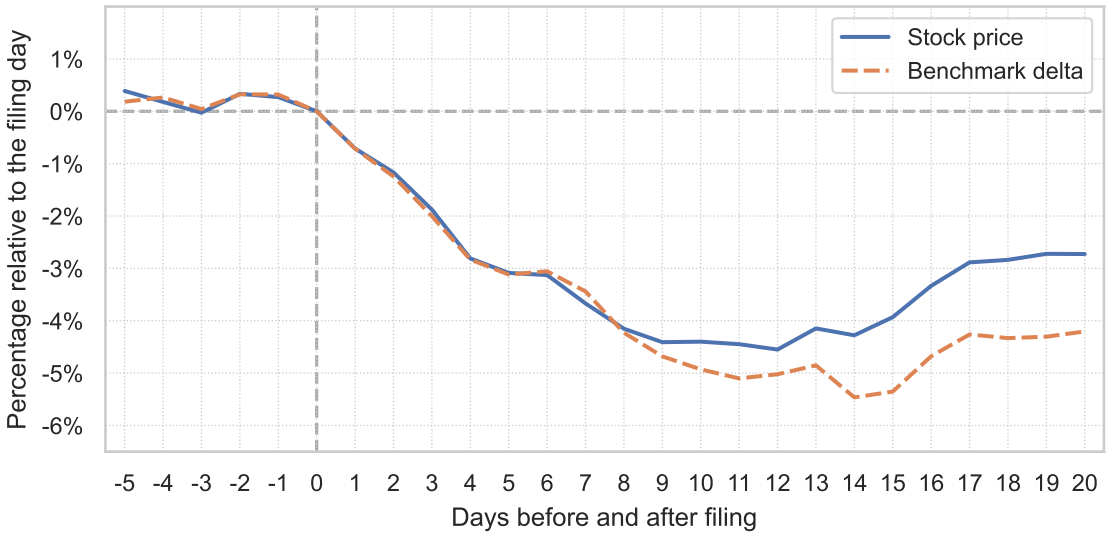

Figure 1: Average stock performance.

3.1. Observations

Let us summarize key observations from our dataset. However, the limited number of 48 fillings analyzed must be considered when interpreting any results and conclusions. The values can be skewed by a few outliers, such as Meta Materials Inc. and its nearly 62% stock price decline on the eight day after the filling[5], or iLearningEngines Inc. with unrelated business problems and its fluctuating stock price around the filing date. In both cases companies filed for bankruptcy and were delisted by Nasdaq shortly after the cybersecurity incidents.

[5]Not directly linked to the cybersecurity incident.

1. Days prior the filings show, as expected, a flattish average price. In some cases, the knowledge of a cybersecurity incident can precede the filing (there is a limit of four business days), which can explain slight negative return prior the filing in some cases (did not manifest in average).
2. After the filing day we observe a measurable impact of the news. This impact lasts the entire interval, with slight recovery after 14 days.
3. Some sectors are more sensitive to cybersecurity incidents. If we limit ourselves to the sectors with at least 5 cybersecurity incidents, Technology and Financial services seems more sensitive than the others. We assume that the reasons are a connection of cybersecurity and the core business of a company in the case of technology companies, and the heavily regulated sector with possible immediate financial impact in the case of financial services. On the other hand, Financial services show the fastest recovery of the stock price. All these conclusions are limited and more data points are needed. The impact of outliers is clearly seen in Industrials sector.
4. It seems that comparing with a benchmark shows a steeper effect of a cybersecurity incident than looking at stock price itself. However, this effect shows only after a week, in the first week there is no measurable difference in these metrics. In other words, a short-term strategy (longer than a week) going long on the benchmark while shorting the stock might be more profitable than shorting the stock alone (and less risky, see the next observation).
5. The standard deviation is relatively high, however even this measurement favors the approach of comparing price movements to the benchmark. Table 3 shows these values for the entire dataset.

Table 3
Average price movement and the standard deviation.

	Stock price			Benchmark delta		
Full dataset (48)	r_5	r_{10}	r_{20}	Δ_5	Δ_{10}	Δ_{20}
mean	-3.09%	-4.40%	-2.73%	-3.12%	-4.93%	-4.20%
standard deviation	8.94%	15.38%	18.20%	8.34%	14.41%	17.85%

4. A simple severity analysis

Cybersecurity incidents can vary in their impact on an organization's operations and financial stability. Market reactions can be disproportionately more significant in response to severe incidents compared to minor ones. The descriptions provided in Item 1.05 can be analyzed to evaluate the severity of such incidents. This problem is similar to the sentiment analysis problem in natural language processing, which has been extensively studied. In recent years, large language models have been applied to this domain [10]. We conduct a simple zero-shot classification using a small Gemma3 4B model [9] using the following prompt:

> *You are a cybersecurity analyst. Carefully review the following text describing a cybersecurity incident. Assess and rate the severity of the incident's impact on the organization's operations and financials. Respond with only one word: 'Low', 'Moderate', or 'High', based on the overall severity. Do not provide explanations or additional text.*

Overall, 3 filings were classified as 'High', 35 as 'Moderate', and 10 as 'Low'. We split the dataset and evaluate the impact on market prices for each class separately. The results are inconclusive. We do not observe any meaningful price action for 'High' filings, although this can be attributed to low count. On the other hand, 'Moderate' severity filings shows deeper price decline and slower recovery in comparison to 'Low' filings, see Table 4 and Figure 2 for additional details.

To enhance our assessment's accuracy, we consider using a few-shot learning approach, leveraging manually classified examples to train the model. Additionally, we can adjust our classification scale

Table 4
Impact of cybersecurity incidents 5, 10 and 20 days after the filing.

		Stock price			Benchmark delta		
Severity	count	r_5	r_{10}	r_{20}	Δ_5	Δ_{10}	Δ_{20}
High	3	2.35%	2.20%	-3.70%	3.01%	4.88%	0.62%
Moderate	35	-3.64%	-5.62%	-4.73%	-3.72%	-6.37%	-6.60%
Low	10	-2.80%	-2.12%	4.59%	-2.84%	-2.84%	2.72%

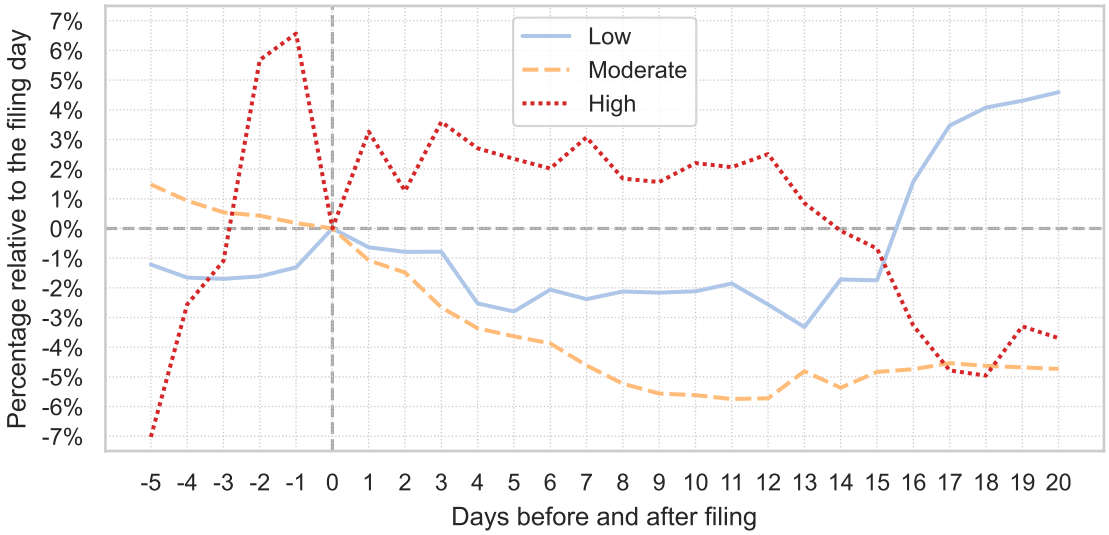

Figure 2: Average stock performance based on the severity.

to focus on market impact, using high/medium/low price decline indicators as a reference, before asking LLM to classify new Item 1.05 texts. However, we postpone these and other techniques until we accumulate a more substantial dataset of cybersecurity incidents.

5. Conclusion

We performed a basic analysis on the impact of cybersecurity incidents on stock prices. The dataset covers Form 8-K filings containing Item 1.05 up to the end of June 2025. While overall results confirm a negative performance of the stock after the incident, more records are needed for a more detailed analysis. Since there will definitely be other cybersecurity incidents in the future, we plan to extend our analysis accordingly.

Declaration on Generative AI

The authors have used Generative AI tools for experiments in Section 4. The model Gemma3 4B was used for incident classification as described in the section.

References

[1] Paul Bischoff. *How data breaches affect stock market share prices*, 2024. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis

[2] Alejandro Hernández. *A Walk Through Historical Correlations Between Vulnerabilities & Stock Prices*, Black Hat Asia 2021.
https://www.blackhat.com/asia-21/briefings/schedule/speakers.html#alejandro-hernndez-40918
[3] Hung Cao, Hieu V. Phan, Sabatino Silveri. *Data breach disclosures and stock price crash risk: Evidence from data breach notification laws*, International Review of Financial Analysis, Volume 93, 103164, ISSN 1057-5219, 2024. https://doi.org/10.1016/j.irfa.2024.103164.
[4] MSCI: *The Global Industry Classification Standard (GICS®)*,
https://www.msci.com/our-solutions/indexes/gics (Accessed 2025-07-11)
[5] Ivan Obaydin, Limin Xu, Ralf Zurbruegg. *The unintended cost of data breach notification laws: Evidence from managerial bad news hoarding*, Journal of Business Finance & Accounting, 1–28, 2024. https://doi.org/10.1111/jbfa.12794
[6] The Securities and Exchange Commission. *Form 8-K*
https://www.sec.gov/files/form8-k.pdf (Accessed 2025-07-11)
[7] Georgios Spanos and Lefteris Angelis. *The impact of information security events to the stock market: A systematic literature review*, Computers & Security, Volume 58, 2016, pp. 216-229.
https://doi.org/10.1016/j.cose.2015.12.006
[8] Martin Stanek. *Impact of Cybersecurity Incidents on Stock Prices*, SSRN, 2024.
http://dx.doi.org/10.2139/ssrn.5001228
[9] Gemma Team. *Gemma 3 Technical report*, Google DeepMind, 2025.
https://arxiv.org/abs/2503.19786
[10] Wenxuan Zhang et al. *Sentiment Analysis in the Era of Large Language Models: A Reality Check*, Findings of the Association for Computational Linguistics: NAACL 2024, Association for Computational Linguistics, pp. 3881-3906.
https://aclanthology.org/2024.findings-naacl.246

A. Fillings used in the analysis

Company Document (prefix with https://www.sec.gov/Archives/edgar/data/)	Filing date
AT&T INC. (T, TBB, TBC, T-PA, T-PC) (CIK 0000732717)	
0000732717/000073271724000046/t-20240506.htm	12.07.2024
B. Riley Financial, Inc. (RILY, RILYG, RILYK, ...) (CIK 0001464790)	
0001464790/000121390024031252/ea0203500-8k_briley.htm	08.04.2024
BASSETT FURNITURE INDUSTRIES INC (BSET) (CIK 0000010329)	
0000010329/000143774924022743/bset20240715_8k.htm	15.07.2024
0000010329/000143774924024679/bset20240805_8ka.htm	06.08.2024
BRANDYWINE REALTY TRUST (BDN) (CIK 0000790816)	
0000790816/000119312524133132/d824906d8k.htm	07.05.2024
0000790816/000119312524147625/d774339d8ka.htm	28.05.2024
CONDUENT Inc (CNDT) (CIK 0001677703)	
0001677703/000167770325000067/cndt-20250409.htm	14.04.2025
Cencora, Inc. (COR) (CIK 0001140859)	
0001140859/000110465924028288/tm247267d1_8k.htm	27.02.2024
0001140859/000110465924084351/tm2420501d1_8ka.htm	31.07.2024
Coinbase Global, Inc. (COIN) (CIK 0001679788)	
0001679788/000167978825000094/coin-20250514.htm	15.05.2025
Crimson Wine Group, Ltd (CWGL) (CIK 0001562151)	
0001562151/000156215124000032/cwgl-20240725.htm	25.07.2024
DROPBOX, INC. (DBX) (CIK 0001467623)	
0001467623/000146762324000024/dbx-20240429.htm	01.05.2024
ENGLOBAL CORP (ENG) (CIK 0000933738)	
0000933738/000165495424015098/eng_8k.htm	02.12.2024
First American Financial Corp (FAF) (CIK 0001472787)	
0001472787/000095017023073848/faf-20231220.htm	29.12.2023

0001472787/000095017024004247/faf-20231220.htm	12.01.2024
Frontier Communications Parent, Inc. (FYBR) (CIK 0000020520)	
0000020520/000119312524100764/d784189d8k.htm	18.04.2024
GLOBE LIFE INC. (GL, GL-PD) (CIK 0000320335)	
0000320335/000032033524000029/gl-20240614.htm	14.06.2024
HALLIBURTON CO (HAL) (CIK 0000045012)	
0000045012/000004501224000052/hal-20240830.htm	03.09.2024
Hewlett Packard Enterprise Co (HPE) (CIK 0001645590)	
0001645590/000164559024000009/hpe-20240119.htm	24.01.2024
KEY TRONIC CORP (KTCC) (CIK 0000719733)	
0000719733/000071973324000015/ktcc-20240506.htm	10.05.2024
0000719733/000071973324000035/ktcc-20240506.htm	14.06.2024
0000719733/000071973324000047/ktcc-20240506.htm	06.08.2024
Karat Packaging Inc. (KRT) (CIK 0001758021)	
0001758021/000121390024089965/ea0218366-8k_karat.htm	23.10.2024
Krispy Kreme, Inc. (DNUT) (CIK 0001857154)	
0001857154/000185715424000123/dnut-20241211.htm	11.12.2024
LEE ENTERPRISES, Inc (LEE) (CIK 0000058361)	
0000058361/000162828025005855/lee-20250212.htm	18.02.2025
MARINEMAX INC (HZO) (CIK 0001057060)	
0001057060/000095017024030041/hzo-20240310.htm	12.03.2024
0001057060/000095017024038881/hzo-20240310.htm	01.04.2024
META MATERIALS INC. (MMATQ) (CIK 0001431959)	
0001431959/000095017024089345/mmat-20240725.htm	01.08.2024
MICROSOFT CORP (MSFT) (CIK 0000789019)	
0000789019/000119312524011295/d708866d8k.htm	19.01.2024
0000789019/000119312524062997/d808756d8ka.htm	08.03.2024
NATIONAL PRESTO INDUSTRIES INC (NPK) (CIK 0000080172)	
0000080172/000143774925006475/npk20250306_8k.htm	06.03.2025
NUCOR CORP (NUE) (CIK 0000073309)	
0000073309/000119312525119311/d795264d8k.htm	14.05.2025
ORASURE TECHNOLOGIES INC (OSUR) (CIK 0001116463)	
0001116463/000119312524094797/d825009d8k.htm	12.04.2024
PRUDENTIAL FINANCIAL INC (PFH, PRH, PRS, ...) (CIK 0001137774)	
0001137774/000119312524033753/d770643d8k.htm	13.02.2024
0001137774/000119312524040749/d766318d8ka.htm	21.02.2024
RADIANT LOGISTICS, INC (RLGT) (CIK 0001171155)	
0001171155/000095017024033954/rlgt-20240319.htm	20.03.2024
SONIC AUTOMOTIVE INC (SAH) (CIK 0001043509)	
0001043509/000104350924000060/sah-20240705.htm	05.07.2024
0001043509/000104350924000063/sah-20240705.htm	05.08.2024
Sensata Technologies Holding plc (ST) (CIK 0001477294)	
0001477294/000147729425000047/st-20250406.htm	09.04.2025
SouthState Corp (SSB) (CIK 0000764038)	
0000764038/000095010324002017/dp206600_8k.htm	09.02.2024
0000764038/000155837024004390/ssb-20240206x8ka.htm	29.03.2024
UNITED NATURAL FOODS INC (UNFI) (CIK 0001020859)	
0001020859/000102085925000036/unfi-20250621.htm	26.06.2025
UNITEDHEALTH GROUP INC (UNH) (CIK 0000731766)	
0000731766/000073176624000045/unh-20240221.htm	22.02.2024
0000731766/000073176624000085/unh-20240221.htm	08.03.2024
0000731766/000073176624000150/unh-20240221.htm	24.04.2024
V F CORP (VFC) (CIK 0000103379)	
0000103379/000095012323011228/d659095d8k.htm	18.12.2023
0000103379/000119312524010243/d641969d8ka.htm	18.01.2024
Zoomcar Holdings, Inc. (ZCAR, ZCARW) (CIK 0001854275)	
0001854275/000121390025054319/ea0245724-8k_zoomcar.htm	13.06.2025