Regulating the Reveal: SEC Item 1.05 and Corporate Cybersecurity Incident Disclosure

John Pierman

Brock University

August 2026

Abstract

I study how SEC Form 8-K Item 1.05 has shaped corporate cybersecurity reporting. The rule requires public companies to disclose a material cybersecurity incident within four business days after they determine that the incident is material to investors. I assemble a consistent 2018–2025 sample of cybersecurity-related 8-K filings from EDGAR and examine filing intensity, observed incident/discovery-to-filing delay, disclosure content, and filing-date stock returns. Cyber 8-K intensity rises at the large-filer effective date but returns to its pre-rule level after full implementation. The associated difference-in-differences estimates are positive but imprecise. Observed delays cluster near short horizons but retain a substantial right tail. Pre-rule filing-date returns are negative, whereas short-window post-rule returns are smaller and statistically indistinguishable from zero. Post-rule filings are shorter on average but do not score as less specific on a transparent text-based measure. Taken together, the evidence documents a transitory change in the observed reporting channel, but does not detect a corresponding shift in investors' filing-date response. The results are early and descriptive on timing and market consequences because the statutory materiality-determination date is rarely public.

Keywords: cybersecurity disclosure, mandatory disclosure, Form 8-K, disclosure timing, securities regulation.
JEL codes: D82, G14, G18, K22, M48.

1 Introduction

The timing of disclosure determines when investors can incorporate material information into prices. This is especially consequential after a cybersecurity incident: a firm may know that an intrusion occurred while still investigating its scope, operational implications, and financial cost. The resulting gap between private and public information is a central concern of disclosure economics [Dye, 1985, Verrecchia, 2001, Guttman et al., 2014]. Yet, until recently, U.S. securities law offered no cyber-specific current-report item with a fixed deadline.

The Securities and Exchange Commission's 2023 rule changed that setting. Form 8-K Item 1.05 requires a registrant to disclose a *material* cybersecurity incident, meaning an incident that a reasonable investor would consider important, within four business days after the registrant determines materiality [Securities and Exchange Commission, 2023b]. The rule therefore standardizes the public channel, but not the underlying point at which a firm concludes that the regulatory clock has started. This distinction is more than semantic: an incident-to-filing interval contains discovery, investigation, legal review, materiality determination, and filing preparation. Only the last portion is governed directly by Item 1.05.

I ask whether Item 1.05 changed what firms disclose or mainly changed how they disclose it. The question separates two forces. A compliance response would appear as a persistent increase in cyber current reports, a compression of observed disclosure delays, and less surprise at the filing date because investors expect the standardized report. A strategic-minimalism response would instead preserve discretion by concentrating disclosure in a formal channel while allowing scope, timing, and detail to remain managerially determined. These mechanisms are not mutually exclusive, and the data do not permit a clean structural separation. They provide a useful organizing framework for interpreting the evidence across outcomes.

I construct a filing-level sample from SEC EDGAR full-text search between 2018 and 2025. The same incident-oriented queries are applied before and after the rule so that the sample does not mechanically expand merely because Item 1.05 headers appear after 2023. A

transparent text screen retains 215 cybersecurity 8-K filings issued by 154 firms. I use the phased implementation dates, December 18, 2023 for earlier-covered registrants and June 15, 2024 for smaller reporting companies, to organize the analysis.

The empirical exercise has four parts. First, I compare daily cyber and non-cyber 8-K counts in a difference-in-differences design, with count models as the preferred specification. Second, I describe public incident/discovery-to-filing intervals, while treating them explicitly as a proxy rather than a statutory compliance measure. Third, I use a filing-date event study to assess whether the information arriving through the 8-K channel changes after implementation. Finally, I examine filing text to distinguish a shorter document from a systematically less informative one.

Three findings are most important. Cyber filing intensity roughly doubles during the initial large-filer phase, from 0.069 to 0.144 filings per day, but falls to 0.067 per day after coverage expands. Poisson and transformed-count estimates are directionally positive in some specifications but not conventionally precise. In the high-confidence timing subsample, the post-rule median observed delay is six calendar days, while the mean is 13.9 days and the right tail remains long. Finally, pre-rule filings have a statistically negative short-window cumulative abnormal return (CAR), whereas the post-rule estimate is smaller and imprecise. The pre/post difference is not statistically significant. Post-rule filings are shorter, but their average text-based specificity score is higher, not lower. Thus the content evidence does not support a simple claim that smaller filing-date reactions are caused by vaguer reports.

This study contributes to work on mandated disclosure and the Form 8-K as a rapid information channel [Lerman and Livnat, 2010, McMullin et al., 2019], and to event-study evidence on cybersecurity incidents [Campbell et al., 2003, Cavusoglu et al., 2004, Kamiya et al., 2021]. Its contribution is deliberately narrow. The paper documents a transitory change in firms' observed reporting behavior: cyber 8-K intensity rises when the rule first binds larger filers and reverts after full implementation. In contrast, the market evidence does not show a statistically detectable shift in investors' filing-date response. The analysis

cannot estimate statutory compliance rates because materiality-determination dates are rarely observed.

The remainder of the article first describes the institutional setting and data, then presents the empirical design and results. The final section discusses interpretation and limitations. Detailed sample-composition checks and dynamic estimates appear in the appendix.

2 Institutional Setting and Data

2.1 Item 1.05 and the interpretation problem

Before Item 1.05, firms could disclose a cyber incident in periodic reports, press releases, or voluntary current reports. SEC guidance had emphasized that existing securities law could require cyber disclosure, but it did not establish a dedicated incident item or a cyber-specific current-report deadline [Securities and Exchange Commission, 2018]. The 2023 final rule requires disclosure of the incident's nature, scope, timing, and material impact in Item 1.05. It applied first to larger registrants on December 18, 2023, and later to smaller reporting companies on June 15, 2024 [Securities and Exchange Commission, 2023a].

The clock begins when a registrant determines that an incident is material, not when an attack occurs or is discovered. This feature limits what public data can establish. A long interval between a mentioned incident date and the 8-K filing date may reflect a prolonged investigation or a late determination. It is not, by itself, evidence of a missed four-business-day deadline. Conversely, a short interval is not proof that the determination was prompt. I therefore reserve "statutory-clock delay" for the small set of filings that explicitly disclose a materiality-determination date.

2.2 Sample construction and scope

The sample begins with EDGAR full-text search for incident-oriented terms, including cybersecurity incident, data breach, ransomware, unauthorized access, and forensic investigation.

I apply the identical query set over the entire 2018–2025 window. Candidate filings are then scored using positive signals for victim, incident, investigation, notification, and attack language, and negative signals for routine vendor, risk-factor, or corporate-action language. The procedure retains 215 filings from 154 firms and rejects 1,099 candidates that do not meet the incident-disclosure standard. The retained sample is a reproducible set of filings with clear incident language, not a census of all cyber incidents or all material incidents.

The analysis uses four related samples. Daily filing-intensity models aggregate EDGAR filing counts over 2,922 calendar days. The event study includes 199 retained filings with an identified ticker and enough return history for model estimation. The principal timing sample includes 91 filings with a high-confidence incident or discovery date. The supplemental determination-date sample has only 20 explicit dates. These selection margins are central to interpretation, rather than a technical footnote: firms that offer a date or describe an incident in sufficient detail may systematically differ from firms that do not.

Table 1 gives the basic filing pattern. The first phase is visibly elevated, but the full-coverage period is nearly indistinguishable from the pre-rule period. This descriptive reversion motivates the paper's emphasis on a transient channel response rather than a durable policy effect.

Table 1: Cybersecurity 8-K filing intensity by implementation period

Period	Calendar days	Cyber filings	Mean per day	Share of all 8-Ks
Pre-implementation	2,177	151	0.069	0.036%
Large-filer phase-in	180	26	0.144	0.072%
Full coverage	565	38	0.067	0.037%

Notes: The unit of observation is the calendar day. "Pre-implementation" ends on December 17, 2023. The large-filer phase runs from December 18, 2023 through June 14, 2024, and full coverage begins June 15, 2024. Cyber filings are the retained incident-related 8-Ks identified by the common EDGAR search and screening procedure. The final column is 100 times the period total of cyber filings divided by all 8-K filings in that period.

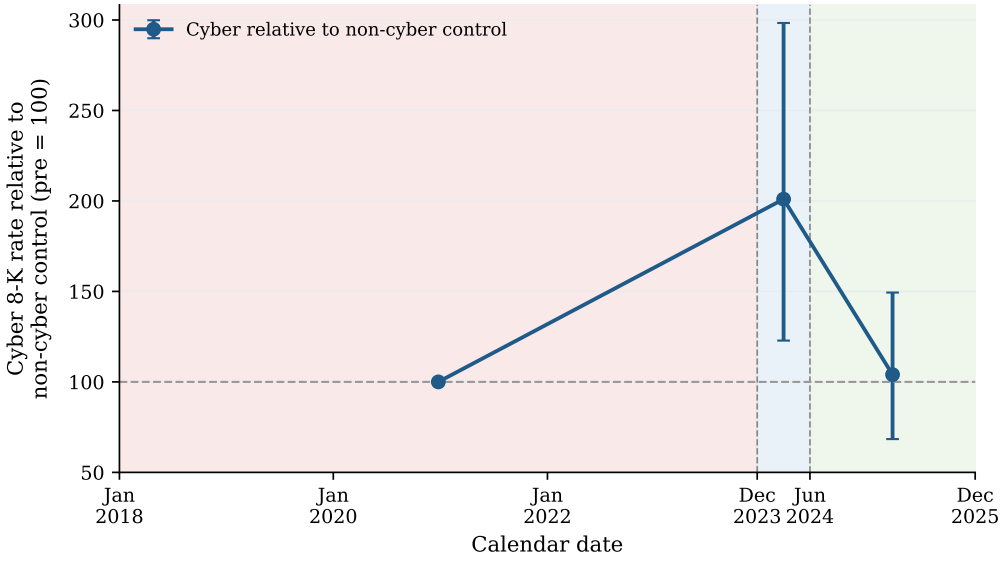


Figure 1: Three-period filing-rate comparison net of the non-cyber 8-K control trend. The plotted value equals 100 times the period-specific ratio of retained incident-related cybersecurity 8-Ks to other 8-Ks, divided by the corresponding pre-implementation ratio. Values above 100 therefore indicate that cyber filing intensity rose more than the control series. The red, blue, and green bands denote the pre-implementation, large-filer phase-in, and full-coverage periods, respectively. Whiskers are 95 percent percentile-bootstrap intervals that resample calendar days within each period. The figure is descriptive. Regression-adjusted estimates are reported in Table 2.

3 Empirical Design

3.1 Filing intensity

The main design compares daily cyber and non-cyber 8-K counts around the first effective date. Let Y_{gt} denote the number of Form 8-K filings in group $g \in \{\text{cyber}, \text{non-cyber}\}$ on calendar day t. I estimate

$$Y_{gt} = \exp\left[\alpha_g + \lambda_t + \delta(\text{Cyber}_g \times \text{Post}_t)\right] + u_{gt},$$

by Poisson pseudo-maximum likelihood. The interaction coefficient is the differential change in cyber filings after December 18, 2023. Group fixed effects absorb time-invariant differences in baseline filing levels. Alternative specifications add week, day, or month effects. I also estimate transformed ordinary least squares models with $\log(1 + Y_{gt})$ and a three-period specification that separates the phase-in and full-coverage periods. Because the treated series is sparse and the rule announcement preceded implementation, these designs should be read as evidence consistent with a response under parallel-trends assumptions, not as an isolated policy experiment.

3.2 Timing, returns, and filing text

For timing, I calculate the calendar-day difference between an extracted incident or discovery date and the EDGAR filing date. This outcome is called the *observed incident/discovery-to-filing delay* throughout. I report distributional facts rather than a causal delay regression because date extraction is selective and because the statutory trigger is typically unobserved.

For market reactions, I estimate a standard market model for each issuer using a 252-trading-day estimation window that ends ten trading days before the event window. Cumulative abnormal returns aggregate residual returns around the filing date. The primary window is $[t-2, t+2]$ trading days, and neighboring windows are diagnostic. A post-rule difference

in CARs can reflect anticipation, information content, incident severity, or changing sample composition, so it is not a direct estimate of the rule's welfare effect.

The text analysis is similarly descriptive. For each accessible filing, I count words, incident details (such as record counts, attack type, third-party systems, remediation, data type, system detail, and timing detail), vague terms, and boilerplate terms. The specificity score equals the number of concrete details minus 0.25 times vague-term hits minus 0.5 times boilerplate hits. This transparent score cannot determine whether every omitted fact is material, but it provides a direct check on the claim that post-rule reports became mechanically thinner.

4 Results

4.1 Filing intensity: an initial response, not a durable shift

The descriptive pattern in Table 1 is sharp: filings per day rise by 109 percent in the initial phase and then return to their pre-implementation rate after full coverage. This is consistent with an early response among the population first facing the new item, but it is not sufficient to attribute the increase to the rule.

Table 2 reports the preferred count model. The point estimate implies a 29 percent differential increase in the cyber incidence rate at the first cutoff, but its standard error is large and the estimate is not conventionally significant. The phased transformed-count estimates in Appendix Table 6 likewise provide no precise first-phase effect once time effects are included. Dynamic estimates have no individually significant pre-period coefficient, and the joint pre-trend test has a p-value of 0.20. Their confidence intervals remain wide. In short, the data are compatible with a short-run increase. They do not establish a persistent change in the cyber 8-K filing rate.

Table 2: Difference-in-differences estimates: Poisson PPML robustness (single cutoff)

	(1) Group FE	(2) + Week FE	(3) + Day FE	(4) + Month FE
$Treat \times Post$	0.258	0.258	0.258	0.256
	(0.169)	(0.168)	(0.163)	(0.169)
$\exp(\hat{\delta}) - 1$ (%)	29.4%	29.4%	29.4%	29.2%
Group FE	Yes	Yes	Yes	Yes
Time FE	None	Week	Day	Month
Observations	5,844	5,844	5,844	5,844
Calendar days	2,922	2,922	2,922	2,922

Notes: Unit of observation is the group-day for the 2018–2025 analysis window, with one cyber and one non-cyber filing-count observation per calendar day. The outcome is the raw integer count of Form 8-K filings in each group on day t. The table reports single-cutoff Poisson pseudo-maximum-likelihood estimates with $Post_t = \mathbb{1}\{t \geq T_0\}$ and $T_0 =$ December 18, 2023. All columns include group fixed effects; columns (2)–(4) add week, day, and month fixed effects, respectively. Standard errors are heteroskedasticity-robust (HC1). $\exp(\hat{\delta}) - 1$ rows report the implied percentage change in the incidence rate. $^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.10$.

4.2 Observed disclosure delays

Table 3 reports the timing distribution for 91 filings with a high-confidence incident or discovery date. The post-rule median is six calendar days, which is near the rough six-calendar-day analogue of four business days, while the mean rises from 11.4 pre-rule days to 13.9 post-rule days. The pattern is driven by a persistent right tail: only 55 percent of post-rule filings fall within six calendar days. This evidence is consistent with some concentration near short delays, but it does not show that firms met or missed the statutory deadline.

The supplemental statutory-clock sample underscores the problem. Only 20 of 215 retained filings state an explicit materiality-determination date. In that selected set, the median determination-to-filing interval is four business days, but the small sample cannot represent the broader population. Appendix Table 9 shows substantial composition differences: date-disclosing filings are more concentrated in the full-coverage period, are smaller on average, and are more concentrated in retail. Public disclosure of a materiality-determination date is

therefore itself an economically relevant selection decision.

Table 3: Observed incident/discovery-to-filing delay

Period	N	Mean days	Median days	Share at or below 6 days
Pre-implementation	51	11.4	5.0	66.7%
Large-filer phase-in	18	9.8	6.0	61.1%
Full coverage	22	17.3	6.5	50.0%
Post-implementation, combined	40	13.9	6.0	55.0%

Notes: The unit of observation is the retained cybersecurity 8-K filing with an extracted incident or discovery date. Delay is the calendar-day difference between that public date and the EDGAR filing date. The six-day threshold is a descriptive approximation to four business days. It is not a legal compliance test because the Item 1.05 clock begins at materiality determination, which is usually not disclosed. Period definitions are given in Table 1.

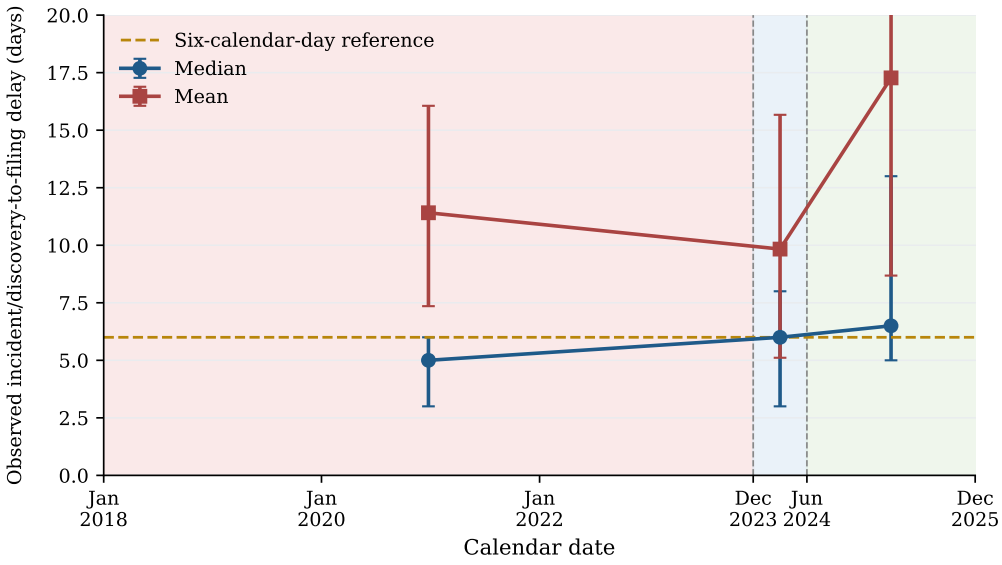


Figure 2: Observed incident/discovery-to-filing delay by implementation period. Markers report the mean and median calendar-day interval between the public incident or discovery date and the EDGAR filing date in the 91-filing high-confidence timing subsample. The red, blue, and green bands denote the pre-implementation, large-filer phase-in, and full-coverage periods, respectively. Whiskers are 95 percent percentile-bootstrap intervals that resample filings within period. The dashed line is a six-calendar-day descriptive approximation to four business days. It is not a statutory compliance benchmark because the Item 1.05 clock begins at materiality determination, which is generally unobserved.

4.3 Information at the filing date and the content of reports

Table 4 shows that cyber 8-K filings were associated with negative stock-price reactions before Item 1.05. The mean $[t-2, t+2]$ CAR is -2.34 percent for 138 pre-rule observations. The corresponding post-rule CAR is -1.20 percent for 61 observations and is not statistically distinguishable from zero. The post-minus-pre difference, however, is also not statistically distinguishable from zero. Figure 3 reports the complementary event-time DiD in cumulative returns. Its first series compares the phase-in differential between cyber and non-cyber 8-Ks with the corresponding pre-implementation differential. Its second series measures the incremental difference from phase-in to full coverage. The estimates are imprecise at most event times. Thus the CAR evidence does not identify a statistically detectable causal change in filing-date price discovery. This lack of precision is not evidence that the causal effect is zero, because the confidence intervals also admit economically meaningful changes. At longer post-rule windows, returns are negative again. These facts are consistent with less information arriving at the immediate filing date, but they cannot distinguish anticipation from differences in the incidents that enter the sample.

The filing-text evidence narrows one interpretation. Table 5 shows that post-rule filings are markedly shorter on average, but their mean specificity score is higher than before the rule because they contain fewer vague and boilerplate terms while retaining a similar number of concrete details. In a 101-filing matched-return regression, a one-unit increase in the score predicts a 0.46 percentage-point larger absolute $[t-2, t+2]$ CAR ($p = 0.042$), conditional on the post indicator and log word count. This association is not causal, but it runs against the simplest strategic-minimalism account in which post-rule filings became uniformly vaguer and therefore less informative. A more cautious interpretation is that Item 1.05 may have standardized a shorter disclosure format while leaving the information content of individual reports heterogeneous.

Table 4: Event study: cumulative abnormal returns around cybersecurity 8-K filings

	Event window				
	$[t-1, t+1]$	$[t-2, t+2]$	$[t-3, t+3]$	$[t-4, t+4]$	$[t-5, t+5]$
Full sample					
Mean CAR	-0.0146^{***}	-0.0199^{***}	-0.0218^{***}	-0.0248^{***}	-0.0241^{***}
	(0.0037)	(0.0051)	(0.0059)	(0.0067)	(0.0072)
N	199	199	199	199	199
Pre-regulation					
Mean CAR	-0.0170^{***}	-0.0234^{***}	-0.0231^{***}	-0.0267^{***}	-0.0230^{***}
	(0.0047)	(0.0065)	(0.0076)	(0.0083)	(0.0083)
N	138	138	138	138	138
Post-regulation					
Mean CAR	-0.0091	-0.0120	-0.0189^{**}	-0.0203^{*}	-0.0267^{*}
	(0.0057)	(0.0077)	(0.0087)	(0.0115)	(0.0140)
N	61	61	61	61	61
Post − Pre					
Difference	0.0079	0.0114	0.0042	0.0064	-0.0038
	(0.0074)	(0.0101)	(0.0115)	(0.0142)	(0.0163)
Post(1) − Post(0)					
Difference	0.0029	0.0061	-0.0031	0.0046	-0.0084
	(0.0108)	(0.0140)	(0.0166)	(0.0213)	(0.0265)

Notes: Unit of observation is the cybersecurity 8-K filing with an identified ticker and sufficient return history. CARs are cumulative abnormal returns over the indicated trading-day event windows, computed using a market model estimated over 252 trading days ending 10 days before the event window opens and requiring at least 30 non-missing return observations. The market benchmark is the SPDR S&P 500 ETF (SPY). The full event-study sample contains 199 filings from 2018–2025. Pre-regulation filings occur before December 18, 2023 ($N = 138$); Post(0) filings occur from December 18, 2023 through June 14, 2024 ($N = 25$); Post(1) filings occur from June 15, 2024 onward ($N = 36$). Post-regulation combines Post(0) and Post(1) ($N = 61$). Standard errors are in parentheses. Post−Pre and Post(1)−Post(0) rows report mean differences with standard errors computed as $\sqrt{SE_A^2 + SE_B^2}$. $^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.10$.
BMP-adjusted t-statistics (Table 8) confirm the significance pattern.

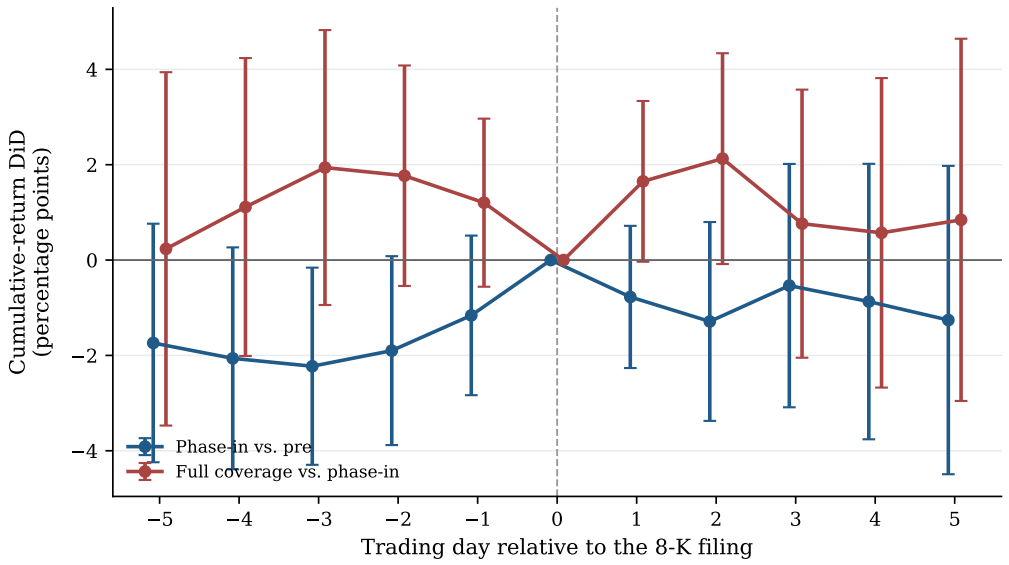


Figure 3: Event-time difference-in-differences estimates for market returns. At each trading day from −5 to +5 relative to the 8-K filing, the blue series is the cyber-minus-non-cyber cumulative-return differential during phase-in minus its pre-implementation counterpart. The red series is the incremental difference in that differential from phase-in to full coverage. Whiskers are 95 percent confidence intervals calculated from independent-sample standard errors. Day 0 is normalized to zero because cumulative returns are measured relative to the filing date. The figure is complementary to the market-model CAR estimates in Table 4 and does not identify a causal effect of Item 1.05 on market prices.

Table 5: Descriptive text evidence by regulatory period

Period	Filings	Mean words	Median words	Specificity score	Concrete details
Pre-implementation	156	1,523	852	-1.82	4.21
Large-filer phase-in	20	866	807	-0.38	4.55
Full coverage	23	938	922	-0.13	4.70

Notes: The unit of observation is the retained cybersecurity 8-K filing with successfully retrieved text ($N = 199$). Concrete details include mention of records exposed, attack type, third-party systems, remediation, data type, affected systems, or timing. The specificity score equals concrete-detail count minus 0.25 times vague-term hits minus 0.5 times boilerplate-term hits. A higher score indicates more concrete detail relative to vague or boilerplate language. This table is descriptive and does not make a legal materiality assessment. Period definitions are given in Table 1.

5 Discussion and Conclusion

The evidence provides a disciplined answer to the paper's organizing question. Item 1.05 appears to have changed the reporting channel more clearly than it changed disclosure behavior in a durable way. The visible increase in cyber 8-Ks at the large-filer effective date is followed by reversion after full coverage, and the estimated intensity effects are too imprecise to support a strong causal claim. Observed delays show both short-horizon concentration and a persistent long tail, but public data cannot separate investigation time from post-determination filing time. Filing-date returns become less negative at short horizons, yet neither the pre/post CAR comparison nor the phase-specific market-return comparisons identifies a statistically detectable causal change. The null results should not be interpreted as proof that no causal effect exists. They remain consistent with effects that the available sample cannot estimate precisely, and the text evidence does not indicate a uniform decline in specificity.

One plausible interpretation is that the rule's initial salience was not reinforced by deadline-specific enforcement. Item 1.05 creates a mandatory four-business-day reporting duty after a materiality determination, but the study does not observe a publicly announced monetary penalty imposed specifically for a late Item 1.05 filing during the sample period. This is distinct from the Commission's cybersecurity-disclosure actions against Unisys, Avaya, Check

Point, and Mimecast, which imposed monetary penalties for misleading disclosures under other securities-law provisions [Securities and Exchange Commission, 2024]. The contrast does not show that the Commission lacks enforcement authority, and it cannot rule out nonpublic supervisory activity. It does, however, leave the deadline's expected penalty less visible to firms and investors than the existence of the formal reporting duty. The initial increase and subsequent reversion are consistent with, but do not establish, an adjustment in which firms and investors gradually re-anchor toward the pre-rule disclosure environment when no deadline-specific penalty is publicly observed. In that interpretation, the observed muting of filing-date CARs reflects a possible change in the timing or packaging of information, not evidence that the rule causally eliminated price discovery.

These results matter for regulatory design. A deadline triggered by an externally unobserved determination can standardize the venue for disclosure while preserving considerable discretion over the process that precedes the deadline. Requiring a registrant to report its materiality-determination date would improve enforcement transparency and make direct compliance measurement possible. More visibly linking confirmed deadline violations to enforcement outcomes could also strengthen the rule's deterrent content, though this paper does not estimate that counterfactual. At the same time, the small number of filings and the sample's reliance on disclosed incident language warrant restraint. The study should be read as early evidence on a new rule, not as a final estimate of its long-run effects.

Several limits remain. The search-and-screening procedure can miss incidents that use unanticipated language or appear late in long filings. The timing subsample is selected on the availability of an incident or discovery date. The event study is susceptible to confounding news and compositional change. Finally, the phase-in is observed at the calendar level rather than through a complete firm-level filer-status panel. Further work should use a larger post-rule sample, manually validate retained and rejected filings, and broaden disclosure of determination dates. These extensions would yield a stronger test of firm compliance and information production.

A Supplementary Evidence

Table 6: Difference-in-differences estimates: cybersecurity filing intensity (phased cutoff)

	(1) Group FE	(2) + Week FE	(3) + Day FE	(4) + Month FE
δ_0 (Post(0) - Pre)	-0.032	0.015	-0.032	-0.000
	(0.203)	(0.082)	(0.127)	(0.078)
$\delta_0 + \delta_1$ (Post(1) - Pre)	0.095	0.080	0.095	0.082*
	(0.123)	(0.061)	(0.085)	(0.048)
Group FE	Yes	Yes	Yes	Yes
Time FE	None	Week	Day	Month
Observations	5,844	5,844	5,844	5,844
Calendar days	2,922	2,922	2,922	2,922

Notes: Unit of observation is the group-day for the 2018–2025 analysis window, with one cyber and one non-cyber filing-count observation per calendar day. The dependent variable is $\log(1 + \text{count})$, where count is the number of Form 8-K filings in group g on day t. $Post_t^{(0)} = \mathbb{1}\{t \geq T_0\}$ and $Post_t^{(1)} = \mathbb{1}\{t \geq T_1\}$ where T_0 = December 18, 2023 and T_1 = June 15, 2024. The first row reports δ_0, the phase-in effect relative to the pre-regulation period. The second row reports $\delta_0 + \delta_1$, the net full-coverage effect relative to the pre-regulation period. All specifications include group fixed effects. Column (1) includes no time fixed effects; columns (2)–(4) add week, day, and month fixed effects, respectively. Standard errors are heteroskedasticity-robust (HC1) for column (1) and week-clustered for columns (2)–(4). $^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.10$.

Table 7: Dynamic treatment effects: monthly event-time coefficients around T_0

Event bin (months rel. T_0)	Estimate	SE	p-value
$k = -6$	-0.1586	(0.2339)	0.4978
$k = -5$	-0.0222	(0.2894)	0.9388
$k = -4$	-0.2967	(0.2478)	0.2312
$k = -3$	-0.0009	(0.2643)	0.9972
$k = -2$	+0.0591	(0.2760)	0.8305
$k = -1$ (reference)	0	—	—
$k = +0$	+0.0389	(0.2868)	0.8921
$k = +1$	+0.0696	(0.2948)	0.8134
$k = +2$	-0.1521	(0.2754)	0.5808
$k = +3$	-0.1844	(0.2368)	0.4361
$k = +4$	-0.2342	(0.2557)	0.3598
$k = +5$	-0.3526	(0.3180)	0.2676
$k = +6$	-0.0755	(0.2390)	0.7522

Notes: Unit of observation is the group-day in a monthly event-time window around T_0 = December 18, 2023. The dependent variable is $\log(1 + \text{count})$, where count is the number of Form 8-K filings in the cyber or non-cyber group on day t. Event bins are monthly intervals relative to T_0; $k = -1$ is omitted as the reference period. Interaction terms are $\mathbb{1}\{\text{event_bin} = k\} \times Treat_g$. The specification includes group and week fixed effects with week-clustered standard errors. The joint F-test for pre-trend coefficients, $k \in \{-6, \ldots, -2\}$, yields $p = 0.2035$. $^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.10$.

Table 8: Event study: BMP-adjusted standardized abnormal return tests

	Event window				
	$[t-1, t+1]$	$[t-2, t+2]$	$[t-3, t+3]$	$[t-4, t+4]$	$[t-5, t+5]$
Full sample					
Mean CAR	-0.0146^{***}	-0.0199^{***}	-0.0218^{***}	-0.0248^{***}	-0.0241^{***}
Simple t	-3.95^{***}	-3.92^{***}	-3.71^{***}	-3.68^{***}	-3.37^{***}
BMP t	-3.36^{***}	-2.65^{**}	-2.71^{**}	-2.02^{*}	-1.83^{*}
N	199	199	199	199	199
Pre-regulation					
Mean CAR	-0.0170^{***}	-0.0234^{***}	-0.0231^{***}	-0.0267^{***}	-0.0230^{***}
Simple t	-3.61^{***}	-3.61^{***}	-3.05^{***}	-3.22^{***}	-2.76^{***}
BMP t	-3.26^{***}	-2.94^{***}	-2.68^{**}	-2.45^{**}	-2.20^{**}
N	138	138	138	138	138
Post-regulation					
Mean CAR	-0.0091	-0.0120	-0.0189^{**}	-0.0203^{*}	-0.0267^{*}
Simple t	-1.61	-1.56	-2.18^{**}	-1.77^{*}	-1.91^{*}
BMP t	-1.45	-0.83	-0.95	-0.31	-0.26
N	61	61	61	61	61
Post − Pre					
Difference	0.0079	0.0114	0.0042	0.0064	-0.0038
Simple t	1.07	1.13	0.37	0.45	-0.23
BMP t	0.01	0.43	0.55	0.84	-0.81
Post(1) − Post(0)					
Difference	0.0029	0.0061	-0.0031	0.0046	-0.0084
Simple t	0.27	0.44	-0.19	0.22	-0.32
BMP t	1.14	0.02	-0.28	1.33	-1.17

Notes: Unit of observation is the cybersecurity 8-K filing in the 2018–2025 event-study sample. CARs are cumulative abnormal returns over the indicated trading-day event windows from the market model. Each firm's CAR is divided by the product of its estimation-window standard deviation of daily abnormal returns and the square-root adjustment for window length and estimation sample size, following Boehmer, Musumeci, and Poulsen (1991). This firm-specific standardization makes the BMP test robust to event-induced variance that can mis-size the simple cross-sectional t-test. Pre-regulation filings occur before December 18, 2023 ($N = 138$); Post(0) filings occur from December 18, 2023 through June 14, 2024 ($N = 25$); Post(1) filings occur from June 15, 2024 onward ($N = 36$). $^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.10$.

Table 9: Balance check: filings with materiality determination dates versus other validated cyber 8-Ks

Variable	Has determination date	Other validated filings	Difference
Market capitalization (log USD)	19.748	22.155	-2.407
Market capitalization (USD billions)	1.113	73.911	-72.798
Regulatory period: Pre-regulation	40.0%	70.2%	-30.2%
Regulatory period: Post T1 full coverage	45.0%	17.7%	27.3%
Regulatory period: Post T0 phase-in	15.0%	12.1%	2.9%
Filer size category: Unknown	25.0%	41.9%	-16.9%
Filer size category: Large accelerated filer	25.0%	39.5%	-14.5%
Filer size category: Accelerated filer; Smaller reporting company	10.0%	6.5%	3.5%
Filer size category: Non-accelerated filer; Smaller reporting company	20.0%	5.6%	14.4%
Filer size category: Accelerated filer	10.0%	6.0%	4.0%
Sector: Unknown	25.0%	41.9%	-16.9%
Sector: Manufacturing	30.0%	20.0%	10.0%
Sector: Services	0.0%	14.4%	-14.4%
Sector: Finance, Insurance, Real Estate	20.0%	11.2%	8.8%
Sector: Retail Trade	20.0%	4.7%	15.3%
Sector: Transportation & Utilities	5.0%	5.1%	-0.1%

Notes: Unit of observation is the SEC 8-K filing. The first group contains $N = 20$ filings and the second group contains $N = 215$ filings. Shares are column percentages within each group. Market capitalization is measured from the existing firm-characteristics snapshot and is missing for some smaller or delisted firms. Regulatory periods are defined by the Item 1.05 effective dates: pre-regulation before December 18, 2023, post-T_0 phase-in from December 18, 2023 through June 14, 2024, and post-T_1 full coverage from June 15, 2024 onward. The appendix table reports the main firm-characteristic categories for readability; the underlying balance output also includes detailed SIC industry rows. Differences are computed as the first group minus the second group.

Table 10: Balance check: retained validated filings versus rejected EFTS candidates

Variable	Retained filings	Rejected candidates	Difference
Market capitalization (log USD)	22.155	21.809	0.346
Market capitalization (USD billions)	73.911	34.895	39.016
Regulatory period: Pre-regulation	70.2%	61.2%	9.0%
Regulatory period: Post T1 full coverage	17.7%	28.5%	-10.8%
Regulatory period: Post T0 phase-in	12.1%	10.3%	1.8%
Filer size category: Unknown	41.9%	74.9%	-33.0%
Filer size category: Large accelerated filer	39.5%	17.0%	22.5%
Filer size category: Accelerated filer; Smaller reporting company	6.5%	3.0%	3.5%
Filer size category: Accelerated filer	6.0%	1.9%	4.1%
Filer size category: Non-accelerated filer; Smaller reporting company	5.6%	1.9%	3.7%
Sector: Unknown	41.9%	74.9%	-33.0%
Sector: Manufacturing	20.0%	7.8%	12.2%
Sector: Services	14.4%	6.2%	8.2%
Sector: Finance, Insurance, Real Estate	11.2%	4.0%	7.2%
Sector: Transportation & Utilities	5.1%	5.0%	0.1%
Sector: Wholesale Trade	2.3%	1.6%	0.7%

Notes: Unit of observation is the SEC 8-K filing. The first group contains $N = 215$ filings and the second group contains $N = 1,099$ filings. Shares are column percentages within each group. Market capitalization is measured from the existing firm-characteristics snapshot and is missing for some smaller or delisted firms. Regulatory periods are defined by the Item 1.05 effective dates: pre-regulation before December 18, 2023, post-T_0 phase-in from December 18, 2023 through June 14, 2024, and post-T_1 full coverage from June 15, 2024 onward. The appendix table reports the main firm-characteristic categories for readability; the underlying balance output also includes detailed SIC industry rows. Differences are computed as the first group minus the second group.

References

Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448, 2003.

Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, 9 (1):69–104, 2004.

Ronald A. Dye. Disclosure of nonproprietary information. *Journal of Accounting Research*, 23(1):123–145, 1985. doi: 10.2307/2490910.

Ilan Guttman, Ilan Kremer, and Andrzej Skrzypacz. Not only what but also when: A theory of dynamic voluntary disclosure. *American Economic Review*, 104(8):2400–2420, 2014. doi: 10.1257/aer.104.8.2400.

Shinichi Kamiya, Jun-Koo Kang, Jiyoon Kim, Andreas Milidonis, and René M. Stulz. What is the impact of successful cyberattacks on target firms? *Journal of Financial Economics*, 139(3):719–749, 2021. doi: 10.1016/j.jfineco.2020.08.015.

Alina Lerman and Joshua Livnat. The new Form 8-K disclosures. *Review of Accounting Studies*, 15(4):752–778, 2010. doi: 10.1007/s11142-009-9114-7.

Jeff L. McMullin, Brian P. Miller, and Brady J. Twedt. Increased mandated disclosure frequency and price formation: Evidence from the 8-K expansion regulation. *Review of Accounting Studies*, 24(1):1–33, 2019. doi: 10.1007/s11142-018-9462-2.

Securities and Exchange Commission. Commission statement and guidance on public company cybersecurity disclosures. https://www.sec.gov/files/rules/interp/2018/33-10459.pdf, 2018. Release No. 33-10459; Accessed: February 2026.

Securities and Exchange Commission. SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure. https://www.sec.gov/news/press-release/2023-139, 2023a. Release No. 33-11216, July 26, 2023. Accessed: February 2026.

Securities and Exchange Commission. Cybersecurity risk management, strategy, governance, and incident disclosure. https://www.sec.gov/files/rules/final/2023/33-11216.pdf, 2023b. 17 CFR Parts 229, 232, 240, 249, and 270. Accessed: February 2026.

Securities and Exchange Commission. SEC charges four companies with misleading cyber disclosures. https://www.sec.gov/newsroom/press-releases/2024-174, 2024. Press Release No. 2024-174, October 22, 2024; Accessed: March 2026.

Robert E. Verrecchia. Essays on disclosure. *Journal of Accounting and Economics*, 32(1-3): 97–180, 2001. doi: 10.1016/S0165-4101(01)00025-8.