Is Ransomware an Economically Distinct Attack Type? An Event Study of Market Reactions

Ambarish Gurjar*, Dalyapraz Manatova†, Benjamin Staples†, Spencer Chambers†, L. Jean Camp*
* College of Computing and Informatics, UNC Charlotte, Charlotte, USA
† Luddy School of Informatics, Computing, and Engineering, Indiana University, Bloomington, USA

***Abstract*—Ransomware attacks have emerged as a significant threat, but has this new mode of attack transformed the economic calculus of cybersecurity? Before the emergence of ransomware, vulnerabilities could be characterized largely as having high negative network externalities while also creating risks for vulnerable parties. However, with ransomware's rise, attackers can more directly extract payments from victims. Such a shift may change negative externalities into directly tangible and quantifiable costs for affected firms.**

To investigate whether ransomware victims internalize these costs, we compute Cumulative Abnormal Returns (CARs) around ransomware disclosure dates. Specifically, we leverage an event-study methodology to estimate CARs across multiple event windows for publicly traded firms affected by ransomware and compare these effects against prior findings in the cybersecurity finance literature. Our results show that firms in the critical manufacturing sector experience negative returns, whereas firms in the information technology and communications sector exhibit comparatively mild effects and a faster recovery trajectory, often showing positive cumulative abnormal returns in longer windows.

Our findings illuminate an important difference in how the market reacts to ransomware incidents in different sectors. However, our findings could also imply that standard market valuations may understate the full economic impact of such incidents, failing to incentivize adequate investment in risk remediation.

***Index Terms*—Ransomware; Event Study; Cumulative Abnormal Returns; Cybersecurity Risk; Empirical Risk Measurement.**

I. Introduction

The rising prevalence of ransomware attacks presents a compelling case for reevaluating traditional cybersecurity economic models. The misalignment of incentives between different stakeholders has long been a chronic source of underinvestment in most cybersecurity preventive measures [1]. Lack of information is another reason that losses caused by stolen data or reputational damage can be difficult for executives to quantify, making it challenging to communicate the value of cybersecurity investments.

In economics, an externality refers to an indirect loss or benefit caused by a certain activity [2]. In the context of information security, a traditional cybersecurity attack can represent a negative externality, as a vulnerability that stems from underinvestment in cybersecurity can be exploited to harm unrelated parties, such as users of the service provided by the company [3]. Moreover, these costs are not internalized by the organization but are instead borne by other affected parties [4], [5].

979-8-3315-8969-1/25/$31.00 ©2025 IEEE

However, ransomware attacks are distinct from other forms of cyberattacks in the sense that they have a measurable and direct impact on the firm's operational costs. While other attacks may primarily harm third parties, ransomware imposes a direct and internalized cost either in the form of a payment made to the attackers or as a payout from ransomware insurance. As such, it is often perceived as a direct, tangible financial loss [6]. To investigate how ransomware attacks are different compared to other security incidents in terms of financial losses, we approach the question by measuring the market response after a ransomware incident and comparing the results to the previous studies related to other types of attacks (e.g., denial-of-service (DoS), data breaches, etc.) [7]–[10] .

The assumption that ransomware is different is built on the fact that by encrypting critical assets and holding data hostage, a bad actor can demand a payment that imposes an immediately quantifiable cost that arises from the operational disruption, which solely needs to be absorbed by the affected firm. Therefore, this means that the attack imposes a direct effect on the firm's cash flows, which are an important component in determining the valuation of a firm [11]. If these losses are truly internalized by the victimized firm, the financial markets, under the efficient-markets hypothesis [12], would respond less favorably to ransomware revelations than to ordinary breaches.

Often, financial losses include only the direct consequences, i.e., the direct cost due to fraud. But there are also response costs such as certification of systems, data checking, longer-term victim outreach, reputation, and trust loss. Such costs often dominate the direct loss, as seen in the comparison of two casinos that suffered from a ransomware attack: Caesar paid $15 million in ransom, while MGM spent nearly $10 million on recovering without a ransom payment, while reporting a loss of 100 million due to business interruption [13]. Presumably, Caesar also bore the cost of removing malware, hardening their systems, and evaluating the integrity of the once-encrypted data. However, Caesar reported only the money paid to the criminals as the cost of the incident. Therefore, to capture other incident-related costs, under the efficient-markets hypothesis, the total impact of an incident—including both direct and indirect costs which can be more consistently captured through changes in a firm's market capitalization.

In this study, we use the event study methodology, which rightly quantifies this phenomenon, capturing the effect of the incident.

Previous event-study research has consistently found that cybersecurity incidents reduce firm value, though the magnitude and persistence of losses vary across studies. Early analyses often assumed that affected firms were representative of the market as a whole, without differentiating by industry or attack type [7]–[9], [14]. When later studies separated firms into categories such as online, brick-and-mortar, and hybrid businesses, results showed that online companies experienced the greatest capitalization losses [15]. However, these analyses predated the surge in ransomware activity and therefore captured cyber incidents primarily involving data breaches or denial-of-service disruptions, not uniquely internalized financial effects of ransomware.

To address this gap, we conduct a ransomware-specific event study that measures cumulative abnormal returns (CARs) across various windows. Previous empirical evidence on data-breach announcements indicates an average cumulative abnormal returns (CARs) of –0.5 % to –2 % over a ten-day window (-5 to +5 days), with statistical significance [10], [14], [16]. However, these effects vary by industry, i.e., financial services firms may incur the most significant losses, while the food and beverage sector and direct-to-consumer services display more subdued responses. Therefore, we examine the market reaction across diverse business sectors to improve our understanding of the effects, including the effect with different windows.

This study seeks to address the research gaps in quantifying financial losses resulting from ransomware attacks by answering the following three questions:

- **RQ1:** Do market responses to ransomware attacks exhibit the same general pattern as other security incidents?
- **RQ2:** If short-term losses occur, is the time to recovery from lost capitalization similar to that observed in prior event-study research?
- **RQ3:** Does industry segment materially influence the equity impact of ransomware, or are these effects sector-agnostic?

Our findings suggest that, in contrast to traditional negative-shock-inducing events such as major data breaches, ransomware does not impose sustained market penalties on affected firms. Moreover, the effect varies by the business sector, penalizing companies in the critical manufacturing sector more, whereas companies in the technology sector exhibit mild positive abnormal returns.

II. Related Work and Motivation

In this work, we have focused on cumulative abnormal returns (CAR) as an approach to quantify the loss of capitalization after the incident event. This approach is a standard method for this type of analysis. Cumulative abnormal return measures the difference between the expected changes in stock value for a given stock, measured immediately around an event. In the Methods section, we offer a mathematical definition of CAR; however, in this section, we examine prior research that employed this event-study methodology to assess the impact of various security incidents.

A. Event Studies of Cybersecurity and Privacy Incidents

Event-study methods have been widely used to quantify how cybersecurity incidents affect firm value. Early work by Cavusoglu et al. [9] analyzed 66 breach announcements and documented statistically significant—though economically modest—negative cumulative abnormal returns of –0.5% to –2%. Acquisti et al. [10] extended this analysis to 333 breaches and confirmed negative CARs over a –5/+5 day window. Bharadwaj et al. [16] examined more than 200 IT failures and found average CARs around –2%.

Other studies focused on the implications of disclosures. Campbell et al. [14] showed that markets penalize firms when illegal data breaches become known. Ko and Dorantes [17], on the other hand, compared constant-mean and multifactor approaches and found no significant drops after the breach announcements.

Collectively, most papers report negative abnormal returns following cybersecurity incidents, although the effect's magnitude and significance vary across samples and incidents. Table I summarizes these findings and the attack types considered in prior work. Note that ransomware has not been as widely studied via the event-study methodology as other attacks, and our study contributes to the existing body of work by focusing on ransomware incidents.

B. Event-Window Design in Prior Research

One methodological divergence in event-study methodology concerns the choice of event window. Short symmetric windows such as (–1, +1) [17], [21] and (–2, +2) [15], [22] are common in research on security incidents, while other studies adopt asymmetric windows, e.g., (–1, +2) [23] or even single-day windows centered on disclosure [9], [10]. Some researchers systematically compared multiple window lengths to test the stability of the results [19], [20]. For our research, we employed a rigorous approach, using seven different event windows, all of which are present in previous studies of security breach event studies.

C. Company Categorization

Prior studies often grouped firms using criteria tailored to specific attack vectors. Early analyses treated affected firms as representative of the overall market, without distinguishing by industry or attack type [9], [10], [16]. Later work introduced more refined categories, such as online, brick-and-mortar, and hybrid firms, which subsequently found that online companies experienced the largest market-value losses [15]. However, these classifications were utilized in the early 2000s and do not accurately represent the current business landscape of firms; nearly every firm now possesses an online presence and could be categorized at least as hybrid. Moreover, categorization of firms that reflect attack types does not always translate to ransomware. For example, with a DOS attack, a firm with a large web presence may experience a stronger negative CAR

TABLE I
SUMMARY OF PRIOR EVENT STUDY FINDINGS ON SECURITY BREACH DISCLOSURES

Type of Attack	Citation	Study Period	Sample	Data Source	Findings (Market Impact)
Data Breach	[9]	1998–2000	66	InfoSec News & Infosec Magazine	∼**–2.1%** CAR over 2-day window (day 0 to +1) for breached firms (significant drop in market value).
Privacy Breach	[10]	1999–2006	79	News databases & compilations	**Negative, short-lived effect:** ∼–0.6% abnormal return on breach announcement day (significant but brief; ∼–1.4% over 5 days in total).
IT System Failure	[16]	1990–2000	213	News reports (multiple sources)	∼**–2%** average CAR over 2-day window for IT failures (statistically significant 2-day drop in stock price).
InfoSec Breach	[14]	1995–2000	43	Press reports (newspapers)	**Mixed:** overall ∼–1.9% CAR (3-day window) not significant, but breaches involving confidential data had larger ∼–5.4% CAR (highly significant).
InfoSec Breach	[17]	1997–2001	19	Prior literature cases	**No significant stock drop** detected on breach announcements; short-term CAR essentially zero.
Virus/Worm Attack	[8]	≈1988–2003	186	News reports & CRSP data	**No effect:** average abnormal returns slightly positive; virus announcements did not result in significant negative CAR.
Multiple Breach Types	[15]	pre-2007	185	Public announcements & news	**Depends on attack type:** data corruption events caused significant negative CAR; simple disclosures or script attacks showed minimal impact.
Denial-of-Service	[7]	≈1998–2002	23	Public announcements	**Negative (sector-specific):** e-commerce firms suffered drops; non-Internet firms saw no significant change.
Data Breach (Churn)	[18]	2011	49	Interviews (cost survey)	**Customer churn:** ∼4.2% abnormal churn rate post-breach (5.6% in finance vs 1.9% in retail).
First-time Cyberattack	[19]	2005–2014	65	Public disclosures (global)	**Significant drop:** Share prices fell on disclosure; short-term CAR significantly negative.
Cyberattacks (general)	[20]	2005–2016	75	Public disclosures (global)	**Significant negative CAR** for successful cyberattacks; long-term sales growth declined up to 3 years.
Ransomware	This Study	2016–2024	44	Temple University's CIRA and CRSP data	**Mixed by sector:** DTC firms saw negative CAR; ITC firms showed no drop (some rebounded); CM firms in between.

if its business depends on that web traffic [7]. Ransomware, however, does not necessarily have such a direct connection to publicly facing resources. For example, an organization could be attacked only on its corporate server. In this scenario, customers might only find out about the attack through a public announcement or through a company insider affected by the attack.

D. Motivation

Despite the prevalence and financial severity of ransomware, it remains underrepresented in event-study research relative to other attack vectors. Prior studies have examined a variety of breaches (e.g., denial-of-service, data exfiltration, service outages), but coverage is uneven across attack types. Hovav and Andoh-Baidoo [15] found that attacks carried out by skilled, professional actors, such as those employing autonomous agents, produce the largest negative CARs. This is particularly relevant for ransomware, which is typically executed by vertically integrated, operationally sophisticated criminal service-providing groups [24]. These observations raise the question of whether ransomware conforms to established patterns in the event-study literature or departs from them in economically meaningful ways. One possibility is that ransomware behaves much like denial-of-service or data-breach incidents. If so, cumulative abnormal returns should yield results consistent with other studies: a minor, potentially significant, short-term decline, followed by recovery.

However, ransomware may also represent a fundamentally different economic mechanism. Unlike other attacks, ransomware enables attackers to impose immediate, direct financial losses through extortion payments. This can shift patching and security investments from decisions dominated by externalities into choices with direct, internalized costs for the victim firm. This possibility is grounded in foundational work in the economics of security that identified the incentive alignment challenges for patching vulnerabilities. Camp & Wolfram noted that unpatched vulnerabilities are network externalities analogous to pollution on the network [4]. Gordon and Loeb determined that, from the firm's perspective, the optimal time to implement a patch is post-intrusion, and that approximately thirty-seven percent of the anticipated loss should be allocated for this purpose [25]. Anderson similarly emphasized the persistent misalignment of incentives in which

there were strong network effects on the negative externalities and limited ability to capture the value of patching [1].

Ransomware has the potential to alter this calculus. Because attackers can extract payments directly, the financial consequences become immediate and quantifiable for individual firms rather than diffuse across the network. If this is the case, market responses to ransomware may differ meaningfully from those documented for other attack classes, providing theoretical motivation for examining both the magnitude of short-term losses (RQ1) and the speed of recovery (RQ2).

The above-mentioned gaps motivate us to examine ransomware separately. Unlike earlier work that categorizes incidents by attacker type or method, our analysis focuses exclusively on ransomware events and therefore does not further subdivide attacks into additional classifications. However, we still consider that affected firms might differ in the market valuation behavior and therefore exhibit different response patterns to the incidents (RQ3). Therefore, we assess whether certain business sectors experience systematically different market reactions. We discuss further how we categorized firms into industry sectors in the Methodology section.

III. Methodology

Our analysis is guided by three research questions:

- **RQ1:** Do market responses to ransomware attacks exhibit the same general pattern as other security incidents?
- **RQ2:** If short-term losses occur, is the time to recovery from lost capitalization similar to that observed in prior event-study research?
- **RQ3:** Does industry segment materially influence the equity impact of ransomware, or are these effects sector-agnostic?

To address RQ1 and RQ2, we compute cumulative abnormal returns (CARs) across multiple event windows centered around each ransomware disclosure and then compare our results with findings summarized in Table I. We use the standard formulation of CAR, described in Section III-B, and Patell's test for statistical significance of the results. For RQ3, we group incidents by the victim firm's industry sector and examine cross-sector differences in CARs.

A. Data Source

In the literature discussed in Section II, a wide range of incidents have been studied, resulting in numerous attack events. In this work, however, we focused on ransomware incidents exclusively. We used the Temple University Critical Infrastructure Ransomware Attacks (CIRA) dataset as the primary source for identifying ransomware incidents relevant to this study [26]. The dataset contains 2,119 documented ransomware attacks recorded between November 2013 and March 2025. Affected organizations are concentrated in government facilities (23%), healthcare (19%), and education (15%). We initially screened 55 entries from this dataset corresponding to publicly traded companies. After cross-referencing these entries with stock exchange records and validating event timelines, 43 companies met our inclusion criteria of having active stock market listings during their attack periods and possessing sufficient price-movement data for analysis. For example, Twitter was delisted after acquisition, while Uber experienced two ransomware attacks in 2014 and 2016; however, Uber's IPO was not launched until 2019, rendering these incidents ineligible for our market-reaction analysis. All companies in this list were hit by ransomware only once, except the Coca-Cola Company (KO), which got hit by ransomware twice. Thus, we refer to those incidents as KO1 and KO2 (see Figure 1).

For each company event, we obtained daily stock price and returns data from the Center for Research in Security Prices (CRSP) database. We focused on the primary stock listing for each firm (for U.S. companies, this was typically the NYSE or NASDAQ listing). We also retrieved market index data to represent the overall market movement; specifically, we used the CRSP value-weighted market return (which approximates the performance of the broad U.S. market) as our benchmark for normal market movements. All returns were adjusted for splits and dividends.

B. Cumulative Abnormal Return Calculations

Using estimation window data, we estimated a market model for each stock. We perform a standard OLS linear regression of the given stock's return on the value-weighted market return

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t}, \tag{1}$$

where

- $R_{i,t}$ is the return of stock,
- $R_{m,t}$ is the return of the market index on day t,
- α_i is the intercept, and
- β_i is the slope

All of these are estimated for each stock using only the estimation window period. This model represents the expected behavior of stock i given market movements under normal circumstances. $\varepsilon_{i,t}$ represents the residuals (or error term), which capture the portion of the stock's return not explained by general market movements.

We computed the Abnormal Return (AR) for each day in the event window as follows:

$$AR_{i,t} = R_{i,t} - (\hat{\alpha}_i + \hat{\beta}_i R_{m,t}), \tag{2}$$

where $\hat{\alpha}_i$ and $\hat{\beta}_i$ are the estimated coefficients from the market model regression. The Cumulative Abnormal Return (CAR) for the time window, e.g.,$[-1, +5]$ is:

$$CAR_{i,[-1,+5]} = AR_{i,-1} + AR_{i,0} + AR_{i,1} + ... + AR_{i,5}$$

Note that rather than relying on a single "event window", we computed CARs over seven different windows: $-1 \rightarrow +1$, $0 \rightarrow +1$, $-1 \rightarrow +2$, $-2 \rightarrow +2$, $-3 \rightarrow +3$, $-4 \rightarrow +4$, and $-5 \rightarrow +5$ trading days. This multi-horizon approach guards against the arbitrary selection of window length and allows

us to trace the temporal profile of any abnormal-return effect. This also facilitates a more effective comparison with prior research.

After computing CARs for all events, we aggregated these to assess the average impact and distribution across events. Following the null hypothesis of no market effect, defined by MacKinlay [27] as $H_0 : \mathbb{E}[CAR] = 0$, a significantly negative average CAR would indicate that ransomware attacks erode shareholder value in the immediate term, while a near-zero or mixed CAR distribution might suggest idiosyncratic or negligible market impact. The aggregate CAR is calculated as follows:

$$\overline{CAR} = \frac{1}{N} \sum_{i=1}^{N} CAR_i \tag{3}$$

To investigate further the statistical significance of computer CAR, we utilize Patell's standardized cross-sectional test [**?**], which evaluates the aggregate strength of the CAR signal across all N events while accounting for each stock's individual volatility. Simply averaging raw CARs can overweight firms with noisier return series; by converting each event's CAR to a z-score,

$$z_i = \frac{\mathrm{CAR}_i}{\hat{\sigma}_i \sqrt{L}},$$

and then forming

$$Z = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} z_i,$$

we obtain a statistic that is approaching standard normal distribution under the null $E[\mathrm{CAR}] = 0$. Patell's test thus tells us whether there is a consistent abnormal-return effect once we normalize for estimation-window risk across the entire sample.

C. Business Sector Categorization

Most prior event-study analyses do not distinguish victim firms by industry. An early study introduced broad categories classifying victims of intrusions into online vs. brick-and-mortar firms, which was appropriate for the time of the study (the early 2000s) [9]. The results showed that online firms were significantly different from brick-and-mortar. However, technology has advanced since then, and every company arguably has an online presence in its supply chain now. If certain industries (e.g., technology) are overrepresented among ransomware victims, aggregate CAR estimates may mask heterogeneous sector-specific responses. This motivates a more granular categorization to assess whether industry membership shapes equity reactions to ransomware incidents. Given the sample size and distribution of publicly traded victims, we classify firms into three analytically meaningful groups:

- *Information Technology & Communications (ITC)*
  Examples: Cisco, MongoDB, Dish Network, AT&T
- *Critical Manufacturing/Infrastructure (CM)*
  Examples: Toyota, Boeing, Kia, Garmin
- *Direct-to-Consumer Services (DTC)*
  Examples: Walmart, Krispy Kreme

These groups have emerged from the informed understanding of the authors of industry-based stock pricing groups, previous literature that categorized incidents in business sectors, and an adequate sample for comparative analysis across meaningful groups that were chosen to reflect differences in operational exposure and customer interface relevant for cybersecurity risk. Table II lists all stock tickers by sector.

TABLE II
LIST OF IDENTIFIED PUBLICLY TRADED COMPANIES FROM THE CIRA RANSOMWARE DATASET (UPDATED SECTOR CLASSIFICATION).

ITC	**CM**	**DTC**
AVDX	XRX	CLX
CAN	BA	COR
CDW	GOLF	DNUT
CSCO	GRMN	FDX
EXTR	HAL	UNH
MDB	KTCC	CZR
NVDA	SSD	DISH
OMCL	TM	PNRA
RNG	WDC	XRX
SONY	WHR	WMT
CTSH		KO
BLKB		KHC
CNDT		PBI
EQIX		INGR
T		BNED
LUMN		
RXT		
SCSC		
Count: 18	Count: 10	Count: 15
Total companies: 43		

To examine whether ransomware affects sectors differently, we conduct a one-way comparison of mean CARs across the three groups: Critical Manufacturing, Direct-to-Consumer Services, and Info Tech&Comm. The null hypothesis formally tests:

$$H_0 : \mu_{\mathrm{CM}} = \mu_{\mathrm{DTC}} = \mu_{\mathrm{ITC}},$$

i.e. whether the mean abnormal return is the same in each sector. A significant F-statistic indicates that sector membership explains a nontrivial fraction of the variance in CAR and justifies further pairwise comparisons.

Due to the violation of the equal variances assumption inherent in standard one-way ANOVA within our dataset, we employ Welch's ANOVA, which is resilient to unequal variances and sample sizes [28]. When Welch's ANOVA identifies significant differences, we apply the Games–Howell post-hoc test [29], which, unlike Tukey's HSD, does not assume homogeneity of variance or equal group sizes. This facilitates valid inferences regarding which pairs of sectors exhibit differences in mean CAR.

Together, Welch's ANOVA and the Games–Howell procedure provide a statistically appropriate framework for testing sector-level heterogeneity in market reactions to ransomware attacks. This allows us to move beyond "Did ransomware move stocks on average?" to the more nuanced conclusions: "Is there a cross-market effect once we normalize for risk?" and "Which sectors drive any observed differences in valuation reactions?".

IV. Results

A. Overall Cumulative Abnormal Returns (RQ1)

To address RQ1, we begin with the immediate event windows around the ransomware disclosure date. Figure 1 shows that the distribution of one-day abnormal returns is centered near zero, and Table III confirms this pattern. In the Day -1 to $+1$ window, the overall CAR is only -0.16%, with Patell's test not indicating significance (Patell $p = 0.3476$). The next window (Day 0 to $+1$) likewise shows a negligible overall CAR (-0.09%), and Patell's test again fails to reject the null (Patell $p = 0.6290$).

These results indicate that immediate market reactions to ransomware disclosures are weak and statistically insignificant, contrasting with the sharp Day-0 impacts reported for some other cybersecurity events such as major data breaches [18]–[20]. Thus, in response to RQ1, we find that the short-term market reaction to ransomware disclosures is mildly negative but statistically insignificant, indicating that the market does not perceive these incidents as value-destroying shocks in the immediate window. This response is far more muted than the canonical short-run losses documented for major data breaches, and this conclusion holds when ransomware is viewed in the aggregate.

It is worth noting, though, that the effect varies across different sectors, as shown in Table III with Welch's ANOVA showing that sectoral differences are significant. This reflects cross-sector heterogeneity but not an aggregate market shock. We investigate this further in the Section IV-C.

B. Overall Recovery Dynamics (RQ2)

To address RQ2, we continue examining the overall cumulative abnormal returns (CARs), but now move beyond the two immediate disclosure windows (Day 0 to 1 and Day -1 to +1) into the multi-day event windows that capture short-run dynamics around the ransomware announcement.

Across Day 0 to 1 and Day -1 to 1, the average CARs remain slightly negative and statistically insignificant, which is consistent with RQ1, indicating no immediate capitalization shock attributable to ransomware. However, once we expand the window beyond the first two days, the pattern shifts meaningfully. Beginning with Day -1 to 2, the overall CAR becomes positive and statistically meaningful, with this trend strengthening over broader $\pm$2-day and $\pm$3-day windows. For example, the Day -2 to 2 and Day -3 to 3 windows both exhibit positive and statistically significant CARs (Patell $p < 0.05$), and this positive direction persists through Day -4 to 4 and Day -5 to 5 as well.

Importantly, we are still not accounting for sector differences at this stage; this is the aggregated effect across all firms. Even at this aggregate level, the data show no evidence of persistent losses, and instead reveal a clear pattern of short-run recovery and, in many windows, a net positive valuation effect.

This pattern is markedly different from classic negative-shock cyber events documented in the literature. Especially data breaches and reputation-damaging intrusions that typically produce sharp CAR declines followed by slower reversion (e.g., [9], [10], [17], [19], [20], [23]). For instance, Cavusoglu et al. [9] and Acquisti et al. [10] found immediate and significant drops in firm value following breach disclosures; Kamiya et al. [20] similarly show reputational damage driving strong negative shock effects.

In contrast, our ransomware sample demonstrates that any small declines are short-lived and reverse quickly, typically within two to five trading days, and in many cases fully recover to positive CARs. This aligns more with previous event studies involving elements that disrupted some operational aspects of a company, like denial-of-service attacks, which had a brief impact [7], [8].

In summary, answering RQ2, the evidence strongly suggests that even when ransomware incidents create mild short-run pressure on valuation, the market rapidly recovers, and broader windows reveal no systematic negative effect. If ransomware were functioning as a classic negative externality, we would expect sustained or compounding losses [1], [4]; instead, the aggregated CAR profile reveals rapid normalization and, in most windows, a mild positive correction rather than long-lived depreciation.

C. Cross-sectoral Differences (RQ3)

A central contribution of this study lies in uncovering substantial cross-sector heterogeneity in how markets respond to ransomware disclosures. As shown in the right panel of Figure 1 and Table III, the cumulative abnormal return (CAR) trajectories diverge meaningfully across the three business segments examined.

Firms in the Critical Manufacturing (CM) sector exhibit consistently negative CARs across all event windows. By contrast, Direct-to-Consumer (DTC) firms display modest and mixed reactions. Their CARs generally oscillate around zero with no sustained directional trend, indicating that ransomware events in this segment do not, on average, materially alter investor expectations of future cash flows. The Information Technology & Communications (ITC) sector presents the most striking departure from prior literature. ITC firms experience consistently positive and increasingly large abnormal returns in the days following disclosure

The sector-level Games–Howell comparisons (Table IV) reinforce this finding. ITC firms significantly outperform CM firms in the $\pm$2-day, $\pm$3-day, and $\pm$5-day windows, and similarly exceed DTC firms in multiple mid-range windows (e.g., Day -3 to +3, Day -4 to +4). Differences between CM and DTC firms remain largely insignificant, confirming that much of the cross-sector variation is driven specifically by the strong positive performance of ITC firms.

V. Discussion

In this work, we examined the daily public stock price of a set of companies that have been subject to ransomware, applying standard CAR analysis over a range of time windows to assess whether ransomware produces a market effect distinct

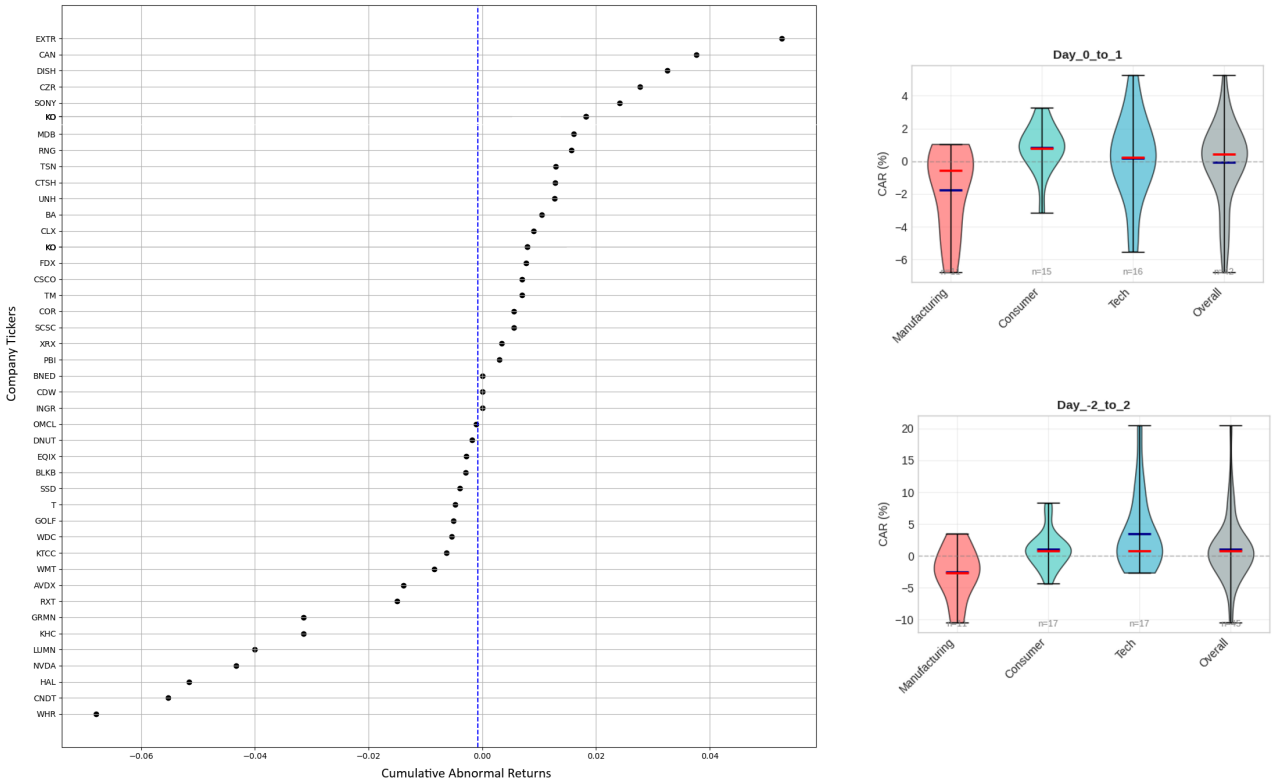

Fig. 1. Cumulative abnormal returns (CAR) surrounding ransomware disclosure events. **Left panel:** CARs for all publicly traded victim firms ($N = 44$), sorted from lowest to highest, with the blue dotted line indicating the cross-firm mean. Values represent Day 0 to Day +1 cumulative abnormal returns. **Right panels:** Sector-wise decomposition of CARs using violin plots for two event windows: Day 0 to +1 (top) and Day –2 to +2 (bottom). Red bars denote sector means and blue bars denote medians. The distributional patterns show that firms in the *Critical Manufacturing* sector exhibit consistently negative CARs in both windows, whereas firms in the *Information Technology & Communications* sector recover rapidly and display positive CARs even within short windows. Direct-to-consumer firms remain close to zero with greater dispersion.

TABLE III
MEAN CUMULATIVE ABNORMAL RETURNS (BY BUSINESS SECTOR AND OVERALL), PATELL'S TEST OF SIGNIFICANCE, AND WELCH ANOVA ACROSS VARIOUS EVENT-WINDOW DEFINITIONS.

Window	Overall CAR	CM CAR	DTC CAR	ITC CAR	Welch F	Welch p
Day 0 to 1	$^{\dagger\dagger}-0.09\%$	$^{**}-1.73\%$	$^{**}0.81\%$	0.20%	4.0685	0.0315
Day -1 to 1	$^{\dagger\dagger}-0.16\%$	$^{**}-1.98\%$	$^{***}1.10\%$	-0.26%	3.7848	0.0385
Day -1 to 2	$^{\dagger\dagger**}0.41\%$	$^{*}-2.11\%$	$^{***}1.46\%$	0.98%	3.5375	0.0447
Day -2 to 2	$^{\dagger\dagger**}1.07\%$	$^{*}-2.59\%$	$^{**}1.04\%$	$^{**}3.46\%$	5.2799	0.0129
Day -3 to 3	$^{\dagger**}1.36\%$	$^{*}-2.37\%$	$^{**}0.99\%$	$^{***}4.15\%$	3.3405	0.0551
Day -4 to 4	$^{**}1.96\%$	-1.60%	$^{**}0.71\%$	$^{***}5.51\%$	1.9353	0.1679
Day -5 to 5	$^{\dagger*}1.88\%$	-1.43%	-0.96%	$^{***}6.86\%$	2.4821	0.1048

Note on Abbreviations:
CM = Critical Manufacturing, DTC = Direct-to-Consumer Services, ITC = Information Technology & Communications.
Statistical significance (using Patell's test) of CAR's trend is denoted as follows: $^{*}p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.
Statistical significance of sectoral differences in CARs: $^{\dagger}p < 0.10$, $^{\dagger\dagger}p < 0.05$.

TABLE IV
GAMES–HOWELL PAIRWISE COMPARISONS OF MEAN CAR (%) BY SECTOR FOR EACH EVENT-WINDOW. "REJECT" INDICATES A SIGNIFICANT DIFFERENCE AT $\alpha = 0.05$.

Window	Group 1	Group 2	Mean Diff (%)	p-value	Reject
Day -1 to 1	Critical Manufacturing	Direct-to-Consumer	-3.0765	0.0145	Yes
	Critical Manufacturing	Info Tech & Comm	-1.7161	0.2606	No
	Direct-to-Consumer	Info Tech & Comm	1.3604	0.2852	No
Day 0 to 1	Critical Manufacturing	Direct-to-Consumer	-2.5447	0.0112	Yes
	Critical Manufacturing	Info Tech & Comm	-1.9365	0.0749	No
	Direct-to-Consumer	Info Tech & Comm	0.6083	0.4416	No
Day -1 to 2	Critical Manufacturing	Direct-to-Consumer	-3.5703	0.0156	Yes
	Critical Manufacturing	Info Tech & Comm	-3.0887	0.0797	No
	Direct-to-Consumer	Info Tech & Comm	0.4815	0.7478	No
Day -2 to 2	Critical Manufacturing	Direct-to-Consumer	-3.6268	0.0222	Yes
	Critical Manufacturing	Info Tech & Comm	-6.0481	0.0038	Yes
	Direct-to-Consumer	Info Tech & Comm	-2.4214	0.1461	No
Day -3 to 3	Critical Manufacturing	Direct-to-Consumer	-3.3559	0.0679	No
	Critical Manufacturing	Info Tech & Comm	-6.5169	0.0179	Yes
	Direct-to-Consumer	Info Tech & Comm	-3.1611	0.1621	No
Day -4 to 4	Critical Manufacturing	Direct-to-Consumer	-2.3092	0.3315	No
	Critical Manufacturing	Info Tech & Comm	-7.1127	0.0566	No
	Direct-to-Consumer	Info Tech & Comm	-4.8035	0.1398	No
Day -5 to 5	Critical Manufacturing	Direct-to-Consumer	-0.4689	0.8522	No
	Critical Manufacturing	Info Tech & Comm	-8.2891	0.0452	Yes
	Direct-to-Consumer	Info Tech & Comm	-7.8201	0.0425	Yes

from other cybersecurity incidents. As ransomware simultaneously compromises confidentiality, integrity, and availability, one might expect more severe negative returns than those observed for breaches or denial-of-service attacks. However, our findings do not support this assumption; thus, we cannot conclude that companies that are subject to ransomware experience consistently significant negative impact on their capitalization as a result, and therefore we do not observe that ransomware is creating more negative effects than other security breach events.

In fact, we observe a more nuanced pattern once the results are categorized by industry sector, i.e., significant differences in short-term windows. Critical Manufacturing (CM) firms exhibit consistent negative CAR immediately after the incident, whereas Information Technology & Communications (ITC) firms show a slight insignificant decline followed by consistent recovery after the second day (see *Day* -2 *to* 2 in Table III). Welch's ANOVA confirms that sectoral differences are statistically significant in short windows, indicating that markets react heterogeneously to ransomware disclosures. The results of the pairwise comparison of sectors (see Table IV) further confirm that the critical manufacturing sector is consistently more adversely affected than direct-to-consumer, while the technology sector has generally outperformed in longer windows (see Table IV), although with no significance in Welch's ANOVA (see Table III).

We cannot ascertain that these positive effects are attributable to ransomware incidents, as it is reasonable to assert that the technology sector has experienced significant growth over the past decades in contrast to critical manufacturing industries, which may account for the subdued impact of the ransomware events. Additionally, as we see in longer windows, sector differences converge and the ANOVA is no longer significant, suggesting that market reactions are transient.

Several mechanisms could explain the positive CARs for ITC firms, though isolating their individual contributions remains for future studies. First, ITC firms possess superior technological resilience and incident response capabilities, leading to reduced penalties or even positive valuations following cyber events [20]. Second, competitive spillovers may benefit firms perceived as more secure when attacks expose industry-wide vulnerabilities [20]. Third, ransomware events may catalyze overdue infrastructure upgrades, effectively forcing technical debt reduction that creates long-term value [30], [31]. Fourth, cyber insurance adoption that are more prevalent among ITC firms [32]–[34] buffers financial impacts [35], [36]. Fifth, timely disclosure may signal regulatory compliance strength, particularly under GDPR frameworks where prompt notification can mitigate penalties [37], [38]. These factors could explain why ITC firms show positive abnormal returns while CM and DTC firms, facing operational disruptions and supply chain impacts, exhibit negligible or negative effects.

Recent research by the Dutch Police demonstrated that companies possessing ransomware insurance tend to pay higher ransoms, rather than lower ones [39]. The lack of negative CAR and the premium provided by insurance to attackers leaves open the question that ransomware and insurance against it are subject to incentive alignment failures. First, as

argued above, ransomware is an externality where the price is not paid by the party that makes the decision to invest in preventing ransomware. Second, and supported by these more recent findings, cyber insurance creates a moral hazard in the case of ransomware. Both these possibilities deserve additional scrutiny.

From a policy perspective, our results imply that current market valuations, including those shaped by insurance markets, fail to impose consistent negative valuation pressure on ransomware victims, offering insufficient incentives for preventive cybersecurity investment. At the same time, transient mispricings create exploitable opportunities for sophisticated investors, indicating some level of market sophistication in processing cyber risk.

These patterns must also be understood in light of widespread underreporting. Our conceptual model assumes that firms lacking segmentation, backups, or encrypted data at rest are more likely to pay ransoms. Yet most payments are never disclosed. A blockchain analysis by NYU identified nearly $900 million of ransomware payments flowing through cryptocurrency channels [40], far exceeding the subset of attacks reported publicly. This means that a lot of companies end up paying the ransom without ever reporting the attack.

VI. Limitations and Future Work

Previous analysis has found company size and market power to be strong indicators of the market response of software firms where vulnerabilities are made public. Our analysis does not account for either of these factors; companies are treated uniformly, and market response is measured relatively. This can be considered a significant limitation of our work, as it is likely that these factors could potentially contribute to the stability or instability of company valuation following an attack. Similarly, this research does not differentiate attacks based on severity and estimated losses. In this scope, a minor attack that results in minimal losses or data leakage would be on even footing with a massive attack that results in significant financial loss and customer trust. Such information is often not shared publicly, but is very likely to have an additional impact on market valuation.

Our work does not consider an event-by-event basis, meaning we do not consider how the ransomware attack was handled by the victim. These possibilities include payment to the attacker in order to prevent data leakage, or total non-cooperation and refusal to negotiate, resulting in full damage. The victim's reaction could feasibly play a large role in determining market valuation; if the attack was handled efficiently, the market would likely not react the same as if the attack escalated or deepened in severity. Again, this type of data is not likely to exist reliably, so our work can't capture this meaningfully.

Finally, while Welch's ANOVA helps mitigate unequal variances across relatively small sectoral samples, our analysis remains constrained by the limited number of publicly traded ransomware cases available in the CIRA dataset, suggesting that future research would benefit substantially from a richer and more longitudinal dataset.

The present study evaluates whether ransomware disclosures generate systematic shocks by estimating abnormal returns relative to a broad market benchmark. While this approach follows the canonical structure of event-study methodology, future work could enhance the granularity of inference in several ways. First, instead of using market-model abnormal returns, one could compute peer-adjusted abnormal returns by regressing each event firm's return against a carefully constructed matched competitor or synthetic control portfolio. Such a design is common in industrial-organization and market-microstructure research [41]–[43]. And would allow us to isolate within-sector competitive dynamics and may clarify why technology firms exhibit disproportionately positive reactions. Benchmarking against peers that are themselves high-performing could attenuate confounding upward trends and reveal whether the ITC-sector premium reflects genuine investor confidence, competitive advantage, or systematic drift shared across the industry. Second, the current analysis focuses on first-order effects (i.e., level returns), whereas higher-order market responses may provide a more complete picture. Ransomware incidents may alter the volatility, skewness, or kurtosis of return distributions.

VII. Conclusions

This study provides a comprehensive assessment of how ransomware attacks influence stock valuations by integrating a traditional event-study analysis. Standard CAR analysis reveals ransomware disclosures do not generate the large, persistent losses often assumed in public incident disclosures. The results show that the immediate market reaction is weak and varies by industry sector. Moreover, any short-term declines reverse quickly, with multi-day windows showing rapid normalization and mild positive CARs in the Direct-to-Consumer and Information Technology & Communications sectors. The major finding from our results indicates that market reactions differ by industry, with Critical Manufacturing consistently exhibiting negative cumulative abnormal returns, whereas ITC demonstrates significant positive abnormal returns across multiple time windows. These results indicate a significant understanding of the impact of ransomware on firm valuation, suggesting that it is sector-dependent rather than uniformly negative.

Acknowledgment

The authors would like to thank Jay Sippelstein for his valuable contributions and support during this research. The authors also gratefully acknowledge Dr. Aunshul Rege and Temple University for providing access to the Critical Infrastructure Ransomware Attacks (CIRA) dataset, which was essential for this study. Furthermore, the authors express gratitude to the reviewers whose feedback substantially enhanced the paper. AI-assisted coding tools (Claude, ChatGPT, and/or GitHub Copilot) were used to generate initial code implementations for data analysis and statistical testing. The

authors verified all code correctness and take full responsibility for the final implementation.

REFERENCES

[1] R. J. Anderson, "Why information security is hard-an economic perspective," in *17th Annual Computer Security Applications Conference (ACSAC 2001), 11-14 December 2001, New Orleans, Louisiana, USA*, pp. 358–365, IEEE Computer Society, 2001.

[2] A. Marshall, *Principles of Economics*. London: Macmillan, 1890.

[3] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[4] L. J. Camp and C. Wolfram, "Pricing security: Vulnerabilities as externalities," 2004.

[5] H. R. Varian, "System reliability and free riding," in *Economics of Information Security*, pp. 1–15, Springer, 2004.

[6] E. V. Cobos and S. Cakir, "A review of the economic costs of cyber incidents," *World Bank Group, Working Paper*, 2024.

[7] A. Hovav and J. D'Arcy, "The impact of denial-of-service attack announcements on the market value of firms," 2003.

[8] D. J. Hovav A., "The impact of virus attack announcements on the market value of firms," 2004.

[9] R. S. Cavusoglu H., Mishra B., "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," 2004.

[10] T. R. Acquisti A., Friedman A., "Is there a cost to privacy breaches? an event study," in *Twenty Seventh International Conference on Information Systems, Milwaukee 2006 and Workshop on the Economics of Information Security 2006*, 2006.

[11] A. Damodaran, *Investment Valuation: Tools and Techniques for Determining the Value of Any Asset*. John Wiley & Sons, 2002.

[12] J. Y. Campbell, A. W. Lo, and A. MacKinlay, *The Econometrics of Financial Markets*. Princeton University Press, 1997.

[13] "A Tale of Two Cyberattacks: MGM and Caesars — mcgriff.com." https://www.mcgriff.com/resources/articles/client-advisory-a-tale-of-two-cyberattacks-mgm-and-caesars/. [Accessed 14-07-2025].

[14] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," *Journal of Computer Security*, vol. 11, no. 3, pp. 431–448, 2003.

[15] A. Hovav and F. K. Andoh-Baidoo, "Classification of security breaches and their impact on the market value of firms," 2007.

[16] K. M. Bharadwaj A., Mähring M., "Effects of information technology failures on the market value of firms," 2009.

[17] D. C. Ko Myung, "The impact of information security breaches on financial performance of the breached firms: An empirical investigation," *Journal of Information Technology Management*, 2006.

[18] P. Institute, "2011 cost of data breach study: United states," tech. rep., Ponemon Institute, 2012.

[19] O. K. Tosun, "Cyber-attacks and stock market activity," *International Review of Financial Analysis*, vol. 76, p. 101795, 2021.

[20] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *Journal of Financial Economics*, vol. 139, no. 3, pp. 719–749, 2021.

[21] S. W. Rahul Telang, "Impact of software vulnerability announcements on the market value of software vendors - an empirical investigation," 2005.

[22] M. K. Anandhi Bharadwaj, "Effects of information technology failures on the market value of firms," 2009.

[23] F. K. Andoh-Baidoo and K.-M. Osei-Bryson, "Exploring the characteristics of internet security breaches that impact the market value of breached firms," 2007.

[24] C. Dalyapraz Manatova and L Jean Camp, "The organizational anatomy of cybercrime: A multilayer framework for modeling resilience," 2025.

[25] L. Gordon and M. Loeb, "The economics of information security investment. acm transactions on information and system security," 2002.

[26] R. Rege, A. Bleiman, "A free and community-driven critical infrastructure ransomware dataset," in *Proceedings from the IEEE Cyber Science Conference*, 2022.

[27] A. C. MacKinlay, "Event studies in economics and finance," *Journal of economic literature*, vol. 35, no. 1, pp. 13–39, 1997.

[28] B. L. Welch, "On the comparison of several mean values: an alternative approach," *Biometrika*, vol. 38, no. 3/4, pp. 330–336, 1951.

[29] P. A. Games and J. F. Howell, "A pairwise multiple comparison procedure for means with unequal variances," *Journal of Educational Statistics*, vol. 1, no. 1, pp. 113–125, 1976.

[30] T. Smith, A. F. Tadesse, and N. Vincent, "The impact of github copilot on technical debt: Evidence from github projects," *arXiv preprint arXiv:2212.05030*, 2022.

[31] H. Chen, L. Cheng, and H. Zhu, "Buy-side analysts and cyber risk disclosure," *Journal of Business Finance & Accounting*, vol. 48, no. 9-10, pp. 1795–1826, 2021.

[32] R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Workshop on the Economics of Information Security (WEIS)*, 2010.

[33] D. Woods and T. Moore, "Does insurance have a future in governing cybersecurity?," *IEEE Security & Privacy*, vol. 17, no. 4, pp. 21–27, 2019.

[34] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *Journal of Cybersecurity*, vol. 5, no. 1, 2019.

[35] M. Eling and W. Schnell, "What do we know about cyber risk and cyber risk insurance?," *Journal of Risk Finance*, vol. 17, no. 5, pp. 474–491, 2020.

[36] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Computer Science Review*, vol. 24, pp. 35–61, 2017.

[37] B. E. Howell and P. H. Potgieter, "A tale of two cybercrimes: Financial and privacy-related breaches and enterprise valuation," *Digital Policy, Regulation and Governance*, vol. 23, no. 4, pp. 365–383, 2021.

[38] H. Li, W. G. No, and T. Wang, "Sec's cybersecurity disclosure guidance and reported cyber incidents," *Contemporary Accounting Research*, vol. 39, no. 2, pp. 1280–1313, 2022.

[39] T. Meurs, E. Cartwright, A. Cartwright, M. Junger, R. Hoheisel, E. Tews, and A. Abhishta, "Ransomware economics: A two-step approach to model ransom paid," pp. 1–13, 2023.

[40] J. Cable, I. W. Gray, and D. McCoy, "Showing the receipts: Understanding the modern ransomware ecosystem," in *2024 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 149–161, 2024.

[41] A. Alti and J. Sulaeman, "Competing for capital," *Journal of Financial Economics*, vol. 103, no. 3, pp. 587–611, 2012.

[42] B. M. Barber and J. D. Lyon, "Detecting long-run abnormal stock returns: The empirical power and specification of test statistics," *Journal of Financial Economics*, vol. 43, no. 3, pp. 341–372, 1997.

[43] E. Gatev, W. N. Goetzmann, and K. G. Rouwenhorst, "Pairs trading: Performance of a relative-value arbitrage rule," *Review of Financial Studies*, vol. 19, no. 3, pp. 797–827, 2006.