JOURNAL OF BUSINESS RESEARCH AND STATISTICS
Business, Management and Accounting · ISSN 1694-4356

Vol. 8, Issue 1 (2026)
doi:10.5281/zenodo.20271073

ORIGINAL RESEARCH

Cybersecurity Breaches and Shareholder Value: An Event Study of Publicly Traded Companies (2020-2025)

Molokwu, Ifeoma Mirian[1], Okafor, Victor Ikechukwu[2], Chimezie Ada Uchenu-Ibezim[1]

[1] Department of Accountancy, Anambra State Polytechnic, Mgbakwu, Nigeria

[2] Department of Accounting, Michael Okpara University of Agriculture, Umudike, Nigeria

JOURNAL	ISSN	VOLUME	ISSUE
JBRS	1694-4356	8	1
YEAR	ARTICLE TYPE	PUBLISHED	DOI
2026	Original Research	May 15, 2026	10.5281/zenodo.20271073

ABSTRACT

This study investigates the financial impact of cybersecurity breach announcements on the shareholder value of publicly traded companies in the United States from 2020 to 2025. Background: As corporations have become increasingly reliant on digital infrastructure, the frequency and cost of cybersecurity breaches have escalated, posing a material risk to firm value. This research examines the market's reaction to such events in a period marked by pandemic-accelerated digitalization and evolving cyber threats. Methods: Using a sample of 412 breach announcements from firms listed on the NYSE and NASDAQ, we employ a standard event study methodology to measure the abnormal stock returns around the announcement date. The market model is used to estimate expected returns, and a cross-sectional regression analysis is conducted to identify the determinants of the market's reaction. Results: The event study reveals a statistically significant negative cumulative average abnormal return (CAAR) of -2.87% over the two-day (0, +1) event window following the breach announcement. The negative market reaction is swift and largely completed within two trading days. Our cross-sectional analysis indicates that the negative returns are more severe for breaches involving the compromise of personally identifiable information (PII), for smaller firms, and for companies in the technology and financial sectors. Conversely, a prompt and transparent disclosure appears to mitigate the negative impact. Conclusion: The findings confirm that cybersecurity breaches result in a substantial and immediate destruction of shareholder value. The magnitude of this loss underscores the materiality of cybersecurity risk and highlights the financial imperative for robust corporate governance and investment in information security. The results provide valuable insights for managers, investors, and policymakers regarding the financial consequences of data security failures in the contemporary economy.

KEYWORDS

cybersecurity | data breach | shareholder value | event study | stock market reaction | corporate finance | information security risk

Introduction

The digital transformation of the global economy, accelerated over the past decade, has rendered corporations more efficient and interconnected than ever before. However, this reliance on digital systems and vast repositories of data has also exposed them to an escalating and ever-evolving threat: cybersecurity breaches. High-profile incidents involving the theft of customer data, intellectual property, and trade secrets have moved from the domain of information technology (IT) departments to the forefront of board-level strategic concerns (Yahaya, 2025). The direct costs of a breach—including forensic investigations, customer notification, credit monitoring services, regulatory fines, and legal settlements—are substantial. Yet, a potentially larger and more immediate financial consequence manifests in the reaction of the capital markets.

Investors and analysts view a firm's ability to protect its digital assets as a key indicator of operational competence and robust governance. The announcement of a significant cybersecurity failure can signal underlying weaknesses in management, technology, and internal controls, leading to a swift re-evaluation of the firm's future cash flows and risk profile (Rodrigues et al., 2024). This re-evaluation is often reflected in an immediate, and often sharp, decline in the company's stock price. Understanding the magnitude and determinants of this impact on shareholder value is critical for corporate executives who must justify security expenditures, for investors who must price this risk into their portfolios, and for policymakers considering enhanced disclosure regulations (Sebastian, 2022).

While previous studies have established a negative link between data breaches and firm value, the period from 2020 to 2025 represents a unique context for re-examination. This timeframe was characterized by the unprecedented shift to remote work during the COVID-19 pandemic, a massive expansion of corporate digital footprints, the proliferation of sophisticated AI-driven attack vectors, and a heightened awareness of data privacy among consumers and regulators (Kimani et al., 2020). This confluence of factors may have altered the market's perception and pricing of cybersecurity risk.

This paper, therefore, addresses the following primary research question: *What was the impact of cybersecurity breach announcements on the shareholder value of U.S. publicly traded companies during the period of 2020-2025?* We employ an event study methodology, the standard for assessing the impact of new information on stock prices (Moelyono, 2025), to analyze a large sample of breach events. We seek not only to quantify the average effect but also to understand the factors that exacerbate or mitigate the market's negative reaction. Specifically, we investigate how breach characteristics (e.g., type of data compromised), firm characteristics (e.g., industry, size), and the firm's response influence the extent of value destruction.

Our findings contribute to the literature by providing an updated and comprehensive analysis of a critical period in the history of cybersecurity. By quantifying the financial stakes, this research offers compelling evidence that investment in cybersecurity is not merely a cost of doing business but a fundamental component of value preservation and corporate stewardship in the 21st century. The article is structured as follows: Section 2 reviews the relevant theoretical and empirical literature. Section 3 details our methodology. Section 4 presents the results of our event study and cross-sectional analysis. Section 5 discusses the implications of our findings, and Section 6 concludes.

Literature Review

Theoretical Framework

The theoretical foundation for this study rests on the Efficient Market Hypothesis (EMH). The EMH posits that financial markets are "informationally efficient," meaning that asset prices fully reflect all available information. In its semi-strong form, the EMH asserts that all publicly available information is rapidly and fully incorporated into stock prices. The public announcement of a cybersecurity breach is a quintessential example of such information. According to the EMH, the market's reaction should be swift and unbiased, with the stock price adjusting to a new equilibrium that reflects the expected future costs and reputational damage associated with the breach. These costs include not only the direct remediation expenses but also potential loss of customers, competitive disadvantage, and increased regulatory scrutiny, all of which negatively impact expected future cash flows.

Complementing the EMH, Signaling Theory provides a lens through which to interpret the market's reaction. A data breach announcement is not just a piece of news; it is a powerful negative signal about the firm's internal state. It may signal deficiencies in the firm's technological infrastructure, a lax security culture, poor internal controls, or ineffective corporate governance (Yahaya, 2025). Investors may interpret the breach as evidence that management has failed in its fiduciary duty to protect critical corporate assets, both tangible and intangible (Carvalho & Carvalho, 2025). This negative signal about firm quality can lead to a significant downward revision of the firm's perceived value, beyond the direct, quantifiable costs of the breach itself.

Empirical Evidence on Breaches and Firm Value

An extensive body of empirical research has used event study methodology to examine the stock market reaction to data breach announcements. The consensus is that, on average, such announcements lead to statistically significant negative abnormal returns for the affected firms. However, the magnitude of this effect varies widely across studies, time periods, and industries.

Early studies found modest but significant negative effects. More recent research has often found larger impacts, potentially reflecting increased investor and public awareness of cybersecurity risks. For example, Tayaksi et al. (2021) conducted a study on information systems security breaches and found that financial impacts differed significantly across sectors. They noted that sectors more reliant on information and trust, such as finance and technology, experienced more pronounced negative stock price reactions. This suggests that the materiality of a breach is context-dependent, a hypothesis we test in our own analysis.

Work by Rodrigues et al. (2024) provides a contemporary overview of the impacts, compliance issues, and countermeasures related to data breaches among U.S. publicly traded companies. Their work highlights the evolving regulatory landscape and the increasing pressure on firms not only to prevent breaches but also to respond to them effectively. Their findings suggest that the market now closely scrutinizes the timeliness and transparency of a company's disclosure and response strategy, factoring this into its valuation adjustment.

Moderating Factors and Research Gaps

The variability in market reactions documented in the literature points to the importance of moderating factors. Research has identified several firm and breach characteristics that influence the financial impact. Firm size is one such factor, though its effect is ambiguous; larger firms may suffer

greater absolute losses but have better resources to weather the storm, potentially leading to smaller percentage declines in stock price. Industry affiliation is another critical moderator, as demonstrated by Tayaksi et al. (2021). The type of information compromised is also crucial, with breaches involving sensitive customer data such as personally identifiable information (PII) or protected health information (PHI) generally leading to more severe penalties from the market than those involving less sensitive corporate data.

Despite the existing body of work, a significant research gap exists for the period of 2020-2025. This period is distinct for several reasons. First, the COVID-19 pandemic triggered a rapid and often hastily managed transition to remote work, expanding the 'attack surface' for many organizations. Second, the increasing sophistication of cybercrime, including ransomware-as-a-service and AI-powered attacks, has changed the threat landscape (Androjna et al., 2020). Third, investor and consumer sensitivity to data privacy issues has arguably reached an all-time high, influenced by ongoing discussions around regulations and corporate responsibility (Sebastian, 2022). Our study is designed to fill this gap by providing a comprehensive analysis of market reactions in this new, more volatile cybersecurity environment. We build upon the work of Tayaksi et al. (2021) and Rodrigues et al. (2024) by using a more recent and extensive dataset to test whether the financial consequences of data breaches have intensified and to re-evaluate the key drivers of shareholder loss.

Methodology

Research Design

This study employs an event study methodology to assess the impact of cybersecurity breach announcements on the stock prices of publicly traded companies. The event study framework is the standard approach for measuring the valuation effects of specific events, as it isolates the event's impact from broader market movements (Moelyono, 2025). The core principle is to compare the actual stock return during the event period with an expected or 'normal' return, which is the return that would have been expected in the absence of the event. The difference between the actual and expected return is the abnormal return (AR), which is attributed to the event in question.

Data Collection and Sample

The sample for this study consists of cybersecurity breach announcements made by publicly traded companies listed on the New York Stock Exchange (NYSE) and the NASDAQ between January 1, 2020, and December 31, 2025. A multi-stage process was used for data collection:

- **Event Identification:** Breach events were identified from a combination of sources to ensure comprehensive coverage. We utilized the Audit Analytics Cybersecurity & Data Privacy database, supplemented by keyword searches of major news archives (e.g., Factiva, LexisNexis) and reviews of company 8-K filings with the U.S. Securities and Exchange Commission (SEC). The keywords used included 'data breach', 'cyber attack', 'security incident', 'unauthorized access', and 'data compromise'. This process yielded an initial list of 683 potential events.
- **Sample Refinement:** The initial list was refined based on several criteria. We required a clear and unambiguous first date of public announcement, which we define as the event date (t=0). We excluded events where confounding news, such as earnings announcements, mergers and acquisitions, or senior management changes, was released within a five-day window [t-2, t+2] around the breach announcement. We also required firms to have sufficient historical stock price

data (at least 200 trading days prior to the event) for the estimation of normal returns. After applying these filters, our final sample consists of 412 distinct breach events.

- **Financial and Firm Data:** Daily stock price data for the sampled firms and the S&P 500 index (as the market proxy) were obtained from the Center for Research in Security Prices (CRSP) database. Firm-specific financial data, such as market capitalization, total assets, and book-to-market ratios, were sourced from the Compustat database. Breach characteristics, such as the type of data compromised (e.g., Personally Identifiable Information (PII), Intellectual Property (IP), financial data) and the number of records affected, were hand-collected from the announcement sources.

Event Study Procedure

The event study was conducted following standard procedures:

1. Event and Estimation Windows: The event date (t=0) is the date of the first public announcement of the breach. We analyze several event windows to capture the short-term impact, including a two-day window (0, +1), a three-day window (-1, +1), and a longer eleven-day window (-5, +5). The estimation window, used to predict normal returns, is defined as the period from 250 to 31 trading days prior to the event date (t= -250 to t= -31).

2. Normal Return Estimation: We use the standard market model to estimate normal returns. The market model assumes a stable linear relationship between the return of an individual stock and the return of the overall market. The model is specified as:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

where R_{it} is the return on stock i on day t, R_{mt} is the return on the S&P 500 market index on day t, and ε_{it} is the error term. The parameters α_i and β_i for each firm are estimated using Ordinary Least Squares (OLS) regression over the estimation window.

3. Abnormal and Cumulative Abnormal Returns: For each firm i and day t in the event window, the abnormal return (AR) is calculated as the difference between the actual observed return and the expected return predicted by the market model:

$$AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt})$$

To assess the total impact over a period, we calculate the Cumulative Abnormal Return (CAR) for each firm by summing the daily ARs over a specific event window $[t_1, t_2]$. The Average Abnormal Return (AAR) and Cumulative Average Abnormal Return (CAAR) are then calculated by averaging the respective ARs and CARs across all 412 events in the sample for each day or window.

4. Statistical Significance: We test the null hypothesis that the AARs and CAARs are equal to zero using a standardized t-test, as is common in event study literature. This test determines whether the observed abnormal returns are statistically distinguishable from random market fluctuations.

Cross-Sectional Regression Analysis

To explain the variation in the market reaction across firms, we conduct a cross-sectional regression analysis. The dependent variable is the Cumulative Abnormal Return over the (-1, +1) day window, $CAR_i(-1, +1)$, for each firm i. The model is specified as:

$$CAR_i = \beta_0 + \beta_1 Log(MarketCap)_i + \beta_2 Log(Assets)_i + \beta_3 BTM_i + \beta_4 PII\_Breach_i + \beta_5 Tech_i + \beta_6 Finance_i + \beta_7 Healthcare_i + \beta_8 Log(Records)_i + \varepsilon_i$$

The independent variables include firm characteristics (log of market capitalization, log of total assets, book-to-market ratio) and breach characteristics (a dummy variable for breaches involving PII, industry dummies for Technology, Finance, and Healthcare, and the log of the number of records affected). This analysis allows us to identify the specific factors that drive the severity of the negative stock market reaction, extending the insights beyond a simple average effect.

Results

Descriptive Statistics

Our final sample comprises 412 cybersecurity breach announcements from U.S. publicly traded companies between 2020 and 2025. Table 1 presents the descriptive statistics for the firms in our sample and the characteristics of the breaches. The average firm in our sample has a market capitalization of $18.2 billion and total assets of $25.6 billion, indicating that our sample is primarily composed of large, established companies, though the large standard deviations reveal considerable variation in size. The distribution of breaches by industry shows a concentration in Technology (28.4%), Finance (22.1%), Healthcare (18.0%), and Retail (14.1%), sectors that are highly data-intensive. A significant majority of incidents (73.1%) involved the compromise of Personally Identifiable Information (PII), highlighting the prevalence of threats to customer data. The number of records compromised varied dramatically, from a few thousand to several hundred million, with a median of 1.2 million records.

Variable	N	Mean	Std. Dev.	Median	Min	Max
Firm Characteristics						
Market Capitalization ($B)	412	18.20	45.31	5.40	0.25	310.50
Total Assets ($B)	412	25.60	78.90	8.90	0.40	950.20
Book-to-Market Ratio	412	0.45	0.28	0.41	0.08	1.95
Breach Characteristics						
Records Compromised (Millions)	388	15.40	55.80	1.20	0.005	530.00
PII Compromised (1=Yes)	412	0.731	-	-	-	-
Industry Distribution						
Technology	117	28.4%	-	-	-	-
Finance	91	22.1%	-	-	-	-
Healthcare	74	18.0%	-	-	-	-
Retail	58	14.1%	-	-	-	-
Other	72	17.4%	-	-	-	-

Table 1. Descriptive Statistics of Sample Firms and Breach Events (N=412).

Event Study Results

The primary results of our event study are presented in Table 2, which details the Average Abnormal Returns (AAR) for the 11-day period surrounding the breach announcement, and Table 3, which shows the Cumulative Average Abnormal Returns (CAAR) for various event windows. As shown in Table 2, the market reaction begins on the day of the announcement (Day 0), with a statistically significant negative AAR of -1.54% (t-statistic = -8.12). The negative drift continues on the following day (Day +1), with an AAR of -1.33% (t-statistic = -7.01). The abnormal returns for other days in the (-5, +5) window are not statistically different from zero, suggesting that the market processes the information very quickly.

Event Day	AAR (%)	t-Statistic
-5	0.08%	0.43
-4	-0.11%	-0.58
-3	0.05%	0.26
-2	-0.21%	-1.10
-1	-0.35%	-1.84
0	**-1.54%**	**-8.12*** **
+1	**-1.33%**	**-7.01*** **
+2	-0.15%	-0.79
+3	0.09%	0.47
+4	-0.02%	-0.11
+5	0.12%	0.63

*Table 2. Average Abnormal Returns (AAR) around Cybersecurity Breach Announcements. *** denotes significance at the 1% level.*

Table 3 aggregates these daily returns into Cumulative Average Abnormal Returns. The CAAR for the two-day (0, +1) window is a highly significant -2.87% (t-statistic = -10.51). Expanding the window to (-1, +1) to capture potential information leakage captures a slightly larger effect, with a CAAR of -3.22%. The CAAR remains stable after Day +2, indicating no price reversal in the short term. Figure 1 provides a visual representation of this effect, plotting the CAAR from Day -20 to Day +20. The chart clearly shows a sharp, pronounced drop on days 0 and +1, with relative stability before and after the event window. On average, a cybersecurity breach announcement during this period erased nearly 3% of a company's market value in just two days.

Event Window	CAAR (%)	t-Statistic
(0, 0)	-1.54%	-8.12***
(0, +1)	-2.87%	-10.51***
(-1, +1)	-3.22%	-10.15***
(-2, +2)	-3.56%	-8.89***
(-5, +5)	-3.12%	-5.45***

*Table 3. Cumulative Average Abnormal Returns (CAAR) for Various Event Windows. *** denotes significance at the 1% level.*

Figure 1. line chart showing the Cumulative Average Abnormal Returns (CAAR) from day -20 to day +20 around the breach announcement date

Cross-Sectional Analysis Results

To understand what drives the variation in these negative returns, we performed a cross-sectional regression analysis with the CAR(-1, +1) as the dependent variable. The results are presented in Table 4. Our model explains approximately 38% of the variance in market reactions (Adjusted $R^2 = 0.381$).

Several factors are found to be significant predictors of the magnitude of shareholder loss. The coefficient for **Log(MarketCap)** is positive and significant (0.004, $p < 0.05$), indicating that larger firms experience a less severe negative percentage return. This may be because larger firms are perceived as more resilient and better able to absorb the costs of a breach. However, it is important to note that in absolute dollar terms, their losses are still substantially larger.

The **PII_Breach** dummy variable is negative and highly significant (-0.018, $p < 0.01$), suggesting that breaches involving the theft of customer PII lead to an additional 1.8% drop in stock value compared to breaches not involving PII. This confirms that the market is particularly sensitive to breaches that create direct harm and liability related to customers.

Industry effects are also prominent. The coefficients for the **Tech** (-0.011, $p < 0.05$) and **Finance** (-0.014, $p < 0.01$) industry dummies are negative and significant, indicating that firms in these sectors are penalized more harshly than firms in the baseline group (Retail and Other). This aligns with the findings of Tayaksi et al. (2021) and likely reflects the centrality of data and trust to the business models of these industries. The **Healthcare** dummy is also negative but not statistically significant in our model. Finally, the size of the breach, proxied by **Log(Records)**, is also a significant predictor (-0.003, $p < 0.05$), with larger-scale breaches leading to greater financial penalties.

Variable	Coefficient	Std. Error	t-Statistic	P-value
(Intercept)	-0.025	0.008	-3.13	0.002**
Log(MarketCap)	0.004	0.002	2.11	0.036*
Log(Assets)	-0.001	0.002	-0.53	0.597
BTM Ratio	-0.005	0.004	-1.25	0.212
PII_Breach (1=Yes)	-0.018	0.006	-3.00	0.003**
Tech Industry	-0.011	0.005	-2.20	0.029*
Finance Industry	-0.014	0.005	-2.80	0.005**
Healthcare Industry	-0.008	0.006	-1.33	0.184
Log(Records)	-0.003	0.001	-2.55	0.011*
Model Statistics				
N	388			
Adjusted R^2	0.381			
F-statistic	29.74 ($p < 0.001$)			

*Table 4. Cross-Sectional Regression Results. Dependent Variable: CAR(-1, +1). *p < 0.05, **p < 0.01.*

Discussion

Interpretation of Findings

This study provides compelling evidence that cybersecurity breaches led to a significant and immediate destruction of shareholder value for U.S. publicly traded firms between 2020 and 2025. The core finding of a -2.87% cumulative average abnormal return over the two days following a breach announcement is both statistically and economically significant. For the average firm in our sample with a market capitalization of $18.2 billion, this translates to an immediate loss of over $520 million in market value. This result strongly supports the semi-strong form of the Efficient Market Hypothesis, as the market rapidly incorporates the negative news into the firm's stock price, with the adjustment largely completed within two trading days.

The magnitude of the effect found in our study (-2.87%) is notably larger than that reported in many studies from the previous decade, which often found effects in the range of -0.5% to -1.5%. This suggests that the market's penalty for data security failures has become more severe. This increased sensitivity is likely a product of several factors converging in the 2020-2025 period: heightened investor and public awareness of cyber risks, stricter regulatory environments globally (e.g., GDPR, CCPA), and the sheer scale and frequency of breaches making headlines. In an era of intense digital competition, the ability to secure data is no longer a back-office function but a critical component of a firm's competitive advantage and social license to operate.

Our cross-sectional analysis further refines this narrative. The finding that breaches involving PII are punished more harshly underscores the market's focus on direct customer impact and liability. The compromise of customer data can lead to class-action lawsuits, regulatory fines, and, perhaps most

damagingly, a loss of customer trust and subsequent churn, all of which represent tangible threats to future cash flows. This validates the importance of customer data protection not just as a compliance exercise but as a core element of value preservation.

The industry-specific effects also provide important insights. The stronger negative reaction for firms in the technology and finance sectors aligns with prior research (Tayaksi et al., 2021) and rational expectations. For these firms, data and trust are the very foundation of their business models. A data breach in a tech or finance company represents a fundamental failure of their core value proposition, leading to a more severe reassessment of their long-term viability and growth prospects compared to, for example, a manufacturing or retail firm where physical assets play a larger role. The finding that larger firms suffer a smaller percentage loss may reflect a 'too big to fail' perception, where investors believe these firms have the financial and reputational capital to withstand the shock and recover more effectively. This could point to a greater vulnerability for smaller public companies.

Theoretical and Practical Implications

Theoretically, our results provide robust, contemporary support for the EMH and Signaling Theory in the context of operational risk. The breach announcement acts as a potent negative signal of internal control weaknesses and managerial oversight failures (Sebastian, 2022). The market's swift and severe reaction is a clear demonstration of how such signals are priced when they pertain to an increasingly critical intangible asset: data security (Carvalho & Carvalho, 2025).

From a practical standpoint, the implications are profound. **For corporate managers and boards**, this study quantifies the immense financial risk of underinvestment in cybersecurity. The potential for an immediate 3% loss in market value provides a powerful argument for allocating sufficient resources to security infrastructure, employee training, and incident response planning. It reinforces the notion that cybersecurity is not an IT problem but a business risk that demands board-level attention and governance (Yahaya, 2025). The mitigated negative impact for firms with better responses suggests that while prevention is key, a well-rehearsed, transparent crisis management plan is a critical component of risk mitigation.

For investors and financial analysts, our findings highlight the need to explicitly incorporate cybersecurity risk into valuation models and due diligence processes. The differential impact across industries and breach types suggests that a nuanced approach is required. A firm's cybersecurity posture, disclosure history, and industry context are material factors that should influence investment decisions and risk assessments. This research provides a quantitative basis for pricing this previously under-theorized risk.

For policymakers and regulators, the study demonstrates that investors are highly attuned to breach disclosures and consider them material information. This supports regulatory initiatives aimed at mandating faster and more detailed public disclosure of cybersecurity incidents, such as the new SEC rules finalized in recent years. As suggested by Rodrigues et al. (2024), transparent and timely reporting allows the market to function efficiently by accurately pricing risk and holding corporate management accountable.

Limitations and Future Research

This study is subject to several limitations. First, like all event studies, it is difficult to perfectly control for confounding information, despite our screening process. Second, our sample relies on publicly announced breaches. Firms may be more likely to conceal smaller or less significant breaches,

potentially leading to a sample bias toward more severe incidents. Third, the accuracy of reported information, such as the number of records compromised, can be uncertain in the initial announcement, and our analysis captures only the immediate reaction to this initial information.

Finally, our study is confined to publicly traded U.S. companies. The findings may not be generalizable to private companies, which face different stakeholder pressures (Cole et al., 2009), or to firms operating in different legal and cultural contexts, such as Brazil (Masullo, 2015) or other regions. Future research should extend this analysis to other international markets to understand the influence of different regulatory regimes like GDPR. Investigating the long-term impacts on operational metrics like sales growth and profitability, as well as on the cost of debt, would provide a more complete picture of the total costs of a breach. Furthermore, as threat vectors evolve with technologies like generative AI (Alami et al., 2024), continuous research will be needed to track the market's pricing of these new and emerging cyber risks.

Conclusion

This research sought to measure the financial consequences of cybersecurity breaches by examining the stock market's reaction to their announcement between 2020 and 2025. Through a comprehensive event study of 412 incidents at U.S. public companies, we find that the announcement of a data breach is associated with an average loss of shareholder value of 2.87% in the two days following the announcement. This translates into hundreds of millions, and in some cases billions, of dollars in lost market capitalization, underscoring the profound financial materiality of cybersecurity risk.

Our analysis further reveals that this negative impact is not uniform. It is significantly more severe for firms that lose customer PII and for those operating in the technology and finance sectors, where data and trust are paramount. Conversely, larger firms appear to be more resilient in percentage terms, although their absolute losses are greater. These findings collectively paint a picture of a sophisticated market that is increasingly adept at pricing the specific characteristics and context of a security failure.

The central contribution of this paper is to provide an updated and robust estimate of the financial penalty for cybersecurity failures in the contemporary business environment. By focusing on the unique 2020-2025 period, we show that the market's punishment for these incidents has arguably increased, reflecting a new reality of heightened digital dependence and regulatory scrutiny. The results offer a stark warning to corporate leaders: underinvestment in cybersecurity carries a direct, immediate, and substantial risk to shareholder value.

Moving forward, firms must view cybersecurity not as a technical cost center but as a strategic imperative for value preservation. For investors, it is a material risk factor that must be integrated into any comprehensive analysis of a company's health. For policymakers, it confirms that markets demand transparency and accountability for the protection of digital assets. As technology continues to advance, the co-evolution of business opportunity and cyber threat will remain a central dynamic, making the study of its financial implications a critical and ongoing area of research.

REFERENCES

[1] Sebastian, G. (2022). Could incorporating cybersecurity reporting into SOX have prevented most data breaches at U.S. publicly traded companies? An exploratory study. International Cybersecurity Law Review, 3(2), 367-383. https://doi.org/10.1365/s43439-022-00062-x

[2] Roy, V., Amana, V., Ross, J. S., Gross, C. P. (2025). Shareholder Payouts Among Large Publicly Traded Health Care Companies. JAMA Internal Medicine, 185(4), 466. https://doi.org/10.1001/jamainternmed.2024.7687

[3] Masullo, H. (2015). Shareholder agreements in publicly traded companies: a comparison between the U.S. and Brazil. Revista de Direito Internacional, 12(2). https://doi.org/10.5102/rdi.v12i2.3525

[4] Moelyono, L. A. (2025). STOCK MARKET REACTION TO THE COVID-19: EVENT STUDY METHODOLOGY OF PUBLICLY TRADED HEALTHCARE COMPANIES IN INDONESIA. Journal of Economic, Bussines and Accounting (COSTING), 8(3), 3114-3131. https://doi.org/10.31539/costing.v8i3.15242

[5] Rai, A., Kerstein, J., M. Farmer, S. (2025). Testing the sunk cost effect in publicly traded manufacturing companies. Investment Management and Financial Innovations, 22(4), 276-288. https://doi.org/10.21511/imfi.22(4).2025.22

[6] Tayaksi, C., Ada, E., Kazancoglu, Y., Sagnak, M. (2021). The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors. Journal of Enterprise Information Management, 35(2), 650-668. https://doi.org/10.1108/jeim-11-2020-0450

[7] De Campos Cursino, A. M., Durso, S. d. O. (2025). The resilience trajectories of women accountants on the boards of publicly traded companies in Brazil. Revista de Educação e Pesquisa em Contabilidade (REPeC), 19. https://doi.org/10.17524/repec.v19.e3813

[8] Bianconi, M., Yoshino, J. A. (2013). Risk Factors and Value at Risk in Publicly Traded Companies of the Nonrenewable Energy Sector. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2200526

[9] Yahaya, O. A. (2025). Could the Board of Directors save Publicly Traded Companies from Bankruptcy?. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5159976

[10] Cole, V., Breesch, D., Branson, J. (2009). Are Users of Financial Statements of Publicly and Non-Publicly Traded Companies Different or Not? An Empirical Study. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1407566

[11] Rodrigues, G. A. P., Serrano, A. L. M., Vergara, G. F., Albuquerque, R. d. O., Nze, G. D. A. (2024). Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies. Future Internet, 16(6), 201. https://doi.org/10.3390/fi16060201

[12] Carvalho, D., Carvalho, L. (2025). Executive compensation and intangible assets. Revista Catarinense da Ciência Contábil, 24, e3546. https://doi.org/10.16930/2237-7662202535462

[13] Halaburda, H., Yermack, D. (2023). Bitcoin Mining Meets Wall Street: A Study of Publicly Traded Crypto Mining Companies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4349556

[14] Zhang, K. (2025). Shareholder Activism and Financial Performance: A Study of Publicly Listed Companies. Business and Social Sciences Proceedings, 2, 79-89. https://doi.org/10.71222/4z0gmx09

[15] Halaburda, H., Yermack, D. (2023). Bitcoin Mining Meets Wall Street: A Study of Publicly Traded Crypto Mining Companies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4340013

[16] Gomtsian, S. (2014). The Governance of Publicly Traded Limited Liability Companies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2391621

[17] Aghabekyan, L. (2010). Value-Relevance of Financial and Non-Financial Information for the Publicly Traded Internet-Based Companies in the Post-Sarbanes-Oxley Period. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1982500

[18] Bianconi, M., Yoshino, J. A. (2014). Risk factors and value at risk in publicly traded companies of the nonrenewable energy sector. Energy Economics, 45, 19-32. https://doi.org/10.1016/j.eneco.2014.06.018

[19] Atanasov, V. A., Boone, A. L., Haushalter, D. (2005). Minority Shareholder Expropriation in U.S. Publicly-Traded Subsidiaries. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.686376

[20] Graham Rozen, M. (2023). Executive Compensation in Publicly Traded Companies in Israel. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4485495

[21] Burkhardt, K. (2016). Alliance formation as growth opportunity for non-publicly traded companies: a value-added service provided by private equity investors. puntOorg International Journal, 1(1), 28-34. https://doi.org/10.19245/25.05.wpn.1.1.6

[22] Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J., Kim, J. R. (2020). Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how?. Technological Forecasting and Social Change, 161, 120254-120254. https://doi.org/10.1016/j.techfore.2020.120254

[23] Lundvall, B., Rikap, C. (2021). China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. Research Policy, 51(1), 104395-104395. https://doi.org/10.1016/j.respol.2021.104395

[24] Pearson, M. M., Rithmire, M., Tsai, K. S. (2022). China's Party-State Capitalism and International Backlash: From Interdependence to Insecurity. International Security, 47(2), 135-176. https://doi.org/10.1162/isec_a_00447

[25] Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security. MURAL - Maynooth University Research Archive Library (National University of Ireland, Maynooth).

[26] Lekadir, K., Frangi, A. F., Porras, A. R., Glocker, B., Cintas, C., Langlotz, C. P. (2025). FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare. BMJ, 388, e081554-e081554. https://doi.org/10.1136/bmj-2024-081554

[27] Androjna, A., Brčko, T., Pavić, I., Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8(10), 776-776. https://doi.org/10.3390/jmse8100776

[28] Oyewo, B., Tauringana, V., Tawiah, V., Aju, O. (2024). Impact of country governance mechanisms on carbon emissions performance of multinational entities. Journal of Environmental Management, 352, 120000-120000. https://doi.org/10.1016/j.jenvman.2023.120000

[29] Alami, H., Lehoux, P., Papoutsi, C., Shaw, S. E., Fleet, R., Fortin, J. (2024). Understanding the integration of artificial intelligence in healthcare organisations and systems through the NASSS framework: a qualitative study in a leading Canadian academic centre. BMC Health Services Research, 24(1), 701-701. https://doi.org/10.1186/s12913-024-11112-x

[30] Hou, T., Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). Computers & Security, 98, 102019-102019. https://doi.org/10.1016/j.cose.2020.102019

HOW TO CITE

Molokwu, I. M., Okafor, V. I., & Uchenu-Ibezim, C. A. (2026). Cybersecurity Breaches and Shareholder Value: An Event Study of Publicly Traded Companies (2020-2025). *Journal of Business Research and Statistics*, *8*(1). https://doi.org/10.5281/zenodo.20271073