CYBERATTACKS AND BUSINESS PERFORMANCE: SECTORAL EVIDENCE FROM STOCK MARKET REACTIONS

Inna Tiutiunyk *, Iryna Pozovna **, Andrii Semenog ***

* *Corresponding author,* Department of Financial Technologies and Entrepreneurship, Academic and Research Institute of Business, Economics and Management, Sumy State University, Sumy, Ukraine
Contact details: Department of Financial Technologies and Entrepreneurship, Academic and Research Institute of Business, Economics and Management, Sumy State University, 112 Kharkivska st, Sumy, Ukraine
** Economic Cybernetics Department, Academic and Research Institute of Business, Economics and Management, Sumy State University, Sumy, Ukraine
*** Department of Financial Technologies and Entrepreneurship, Academic and Research Institute of Business, Economics and Management, Sumy State University, Sumy, Ukraine

OPEN ACCESS

How to cite this paper: Tiutiunyk, I., Pozovna, I., & Semenog, A. (2026). Cyberattacks and business performance: Sectoral evidence from stock market reactions. *Business Performance Review, 4*(1), 68–80.
https://doi.org/10.22495/bprv4i1p6

ISSN Online: 3005-6829
ISSN Print: 3005-6810

Received: 28.11.2025
Revised: 29.12.2025; 26.01.2026
Accepted: 04.02.2026

JEL Classification: D82, G14, G32, M21
DOI: 10.22495/bprv4i1p6

Abstract

The article examines the impact of cyberattacks on the market capitalization and short-term returns of leading companies in the finance, telecommunications, and information technology (IT) sectors. Using event analysis, abnormal return (AR), and cumulative abnormal return (CAR) estimation, the market sensitivity to cybersecurity incidents is determined for over 30 events over the period 2018–2024. The results indicate a short-term negative effect of cyberattacks, especially in the financial sector, while technology companies demonstrate a faster recovery of market positions. Differences in investor risk perception are identified depending on the industry, the duration of the attack, the history of previous incidents, and the reputational stability of the company. Cases of repeated attacks on one company are analyzed separately, indicating a change in the intensity of the market reaction over time. The findings complement existing empirical evidence on stock market sensitivity to cybersecurity incident disclosures documented in prior event-based studies (Cavusoglu et al., 2004; Romanosky, 2016) and provide insights for improving cyber risk management strategies, particularly with respect to disclosure practices and reputational shock monitoring systems.

Keywords: Cyberattack, Stock Volatility, Business Performance, Market Reaction

Authors' individual contribution: Conceptualization — I.T., I.P., and A.S.; Methodology — I.T. and I.P.; Validation — I.P.; Investigation — I.T. and I.P.; Writing — Original Draft — I.T., I.P., and A.S.; Writing — Review & Editing — I.T., I.P., and A.S.; Visualization — I.T., I.P., and A.S.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: This research was funded by the project "Modeling the mechanisms of combating organized and transnational cybercrime in war and post-war periods" (0124U000550), funded by the Ministry of Education and Science of Ukraine.

1. INTRODUCTION

The rapid digitalization of economic activity has substantially increased firms' dependence on information and communication technologies, transforming cybersecurity incidents into a critical source of financial and reputational risk. As cyberattacks have evolved from isolated technical

disruptions into complex incidents capable of halting operations, compromising sensitive data, and undermining stakeholder trust, their economic consequences increasingly extend beyond direct financial losses to include declines in market capitalization and structural shifts in investor expectations (Fotis, 2024; Vergara Cobos & Cakir, 2024a, 2024b; Rubab et al., 2025).

Public disclosures of cyber incidents are followed by immediate and significant declines in firm market value, reflecting heightened uncertainty and rapid reassessments of risk by investors (Cavusoglu et al., 2004; Acquisti et al., 2006; Alsadoun & Albaz, 2025). These market reactions are commonly explained through the lens of information asymmetry, as investors typically lack timely and complete information regarding the scope, duration, and long-term implications of cyber incidents at the time of disclosure. Consequently, even incidents with limited direct financial damage may trigger pronounced short-term valuation losses.

Importantly, the magnitude and persistence of market reactions to cyberattacks are not uniform across firms or industries. Companies operating in finance, telecommunications, and technology differ substantially in their digital intensity, regulatory exposure, reliance on trust-sensitive data, and perceived cyber-resilience (Eling & Wirfs, 2019; AlHares et al., 2024; Rubab et al., 2025; Kanyongo & Wadesango, 2025). Financial institutions and telecommunications providers are particularly vulnerable to reputational shocks due to their dependence on customer trust, regulatory scrutiny, and the continuous provision of digital services. In contrast, large technology firms often benefit from stronger reputational capital, greater experience in managing digital risks, and higher adaptive capacity, which may mitigate the persistence of negative market reactions.

These sector-specific differences suggest that market reactions to cyber incidents are shaped by distinct underlying mechanisms. From a theoretical perspective, these reactions can be explained through three interrelated mechanisms. First, disclosure timing shapes the degree of information asymmetry: delayed or incomplete disclosure amplifies uncertainty and intensifies negative abnormal returns (AR) immediately following public announcements (Cavusoglu et al., 2004; Acquisti et al., 2006; Romanosky, 2016; Alsadoun & Albaz, 2025). Second, attack duration and recurrence influence perceptions of managerial competence and organizational cyber-resilience, with repeated or prolonged incidents signaling structural weaknesses in risk management and governance systems (Gordon et al., 2011; Eling & Wirfs, 2019; Rubab et al., 2025). Third, reputational capital moderates market reactions by enabling firms with strong governance structures and transparent communication practices to restore investor confidence more rapidly following cyber-related shocks (Gordon et al., 2011; AlHares et al., 2024).

While the adverse market effects of cyber incidents are well documented, existing empirical evidence remains mixed regarding sectoral heterogeneity, recovery dynamics, and the role of repeated incidents. This study contributes to the literature by examining how sectoral characteristics, disclosure timing, attack duration, and the recurrence of cyber incidents jointly shape short-term stock market reactions. Focusing on firms operating in the finance, telecommunications, and technology sectors, the paper provides a more nuanced understanding of how investors interpret cybersecurity risks under conditions of increasing informational turbulence.

The structure of this paper is as follows. Section 2 reviews the literature on the economic and market effects of cyberattacks. Section 3 describes the research methodology, including the event study framework, data sources, and model specifications. Section 4 reports the empirical results of the AR and cumulative abnormal return (CAR) analysis. Section 5 discusses the findings in the context of previous empirical studies and highlights their implications for investors and corporate risk management. Finally, Section 6 concludes the paper and outlines limitations and directions for future research.

2. LITERATURE REVIEW

The growing scale and sophistication of cyberattacks have stimulated extensive research into their economic and financial market consequences, with cyber risk increasingly treated as an inherent component of business activity affecting firm valuation through operational disruptions, reputational damage, and heightened uncertainty among market participants (Romanosky, 2016; Eling & Wirfs, 2019; Arcuri et al., 2017; Osifodunrin & Lopes, 2023; AlHares et al., 2024).

A central mechanism through which cyber incidents affect stock prices is information asymmetry, particularly surrounding the disclosure of incident-related information. Prior research consistently demonstrates that the official disclosure date, rather than the technical occurrence of an attack, represents the moment of the strongest market reaction, as investors simultaneously receive and process new risk-relevant information (Cavusoglu et al., 2004). Delays in disclosure or incomplete reporting exacerbate uncertainty and intensify negative AR (Acquisti et al., 2006; Amir et al., 2018; Romanosky, 2016).

The regulatory environment further moderates this relationship. In jurisdictions with strict and standardized disclosure requirements, market reactions tend to be less volatile, as investors anticipate timely and transparent communication. In contrast, more flexible disclosure regimes, particularly in the USA, are associated with stronger negative reactions due to increased informational opacity and greater managerial discretion (Eling & Wirfs, 2019; Cao et al., 2024). These findings underscore disclosure timing as a key determinant of short-term market responses to cyber incidents.

Beyond disclosure, the characteristics of the cyberattack itself play an important role in shaping market reactions. Incidents involving the leakage of confidential or personal data generate the most pronounced negative market responses, reflecting heightened concerns over legal liability, regulatory sanctions, and long-term reputational damage (Campbell et al., 2003). In contrast, cyber

events such as DDoS attacks, which do not compromise sensitive information, typically trigger weaker and more transient stock price declines.

Recent research highlights the importance of attack duration and complexity as key determinants of economic impact. Prolonged cyber incidents are associated with greater operational disruptions, higher recovery costs, and sustained informational uncertainty, contributing to stronger CAR (Eling & Wirfs, 2019). Although the true duration of an incident often remains unknown at the time of disclosure, subsequent revelations during internal investigations may intensify reputational losses and generate secondary business shocks (Romanosky, 2016).

Empirical evidence further suggests that even short-term attacks targeting complex digital infrastructure can produce disproportionate financial consequences, particularly when core business processes are affected (Mustofa et al., 2024). Moreover, the persistence of market reactions varies by incident type: while personal data breaches tend to cause sharp immediate price declines, attacks on industrial or operational systems are associated with more prolonged negative effects (Morse et al., 2011; Goel & Shawky, 2009). Collectively, these findings emphasize the role of attack duration, severity, and complexity in shaping cumulative market losses.

A distinct line of research examines the recurrence of cyber incidents and their implications for investor perceptions. According to the "cyber breach history effect", repeated cyberattacks generate cumulative reputational damage, signaling persistent structural vulnerabilities and ineffective risk management practices (Campbell et al., 2003). As a result, firms experiencing multiple incidents are penalized more severely by the market than those facing isolated events.

Empirical studies confirm that repeated cyberattacks are associated with sharper stock price declines and slower recovery dynamics, as investors interpret recurrence as evidence of chronic cyber insecurity (Amir et al., 2018; Muktadir-Al-Mukit & Ali, 2025; Palkar & Figueiredo, 2025). This effect extends beyond equity markets: successive incidents erode trust not only among investors but also across broader stakeholder networks, including clients, suppliers, and business partners (Hovav & Gray, 2014; Martin et al., 2017). Additionally, attack recurrence influences credit risk assessments, affecting firms' credit ratings, cost of capital, and long-term investment attractiveness (Florackis et al., 2023).

The literature also reports pronounced sectoral heterogeneity in market responses to cyber incidents, driven by differences in digital intensity, regulatory exposure, and reliance on trust-sensitive data. Financial institutions experience the most substantial stock price declines following cyberattacks, reflecting their dependence on digital channels, strict regulatory oversight, and the central role of trust in financial intermediation (Tweneboah-Kodua et al., 2018; Kammoun et al., 2019). Telecommunications firms are similarly vulnerable due to the critical importance of service continuity and customer data protection. In contrast, industrial firms tend to exhibit more moderate market reactions, which may be attributed to lower levels of digital integration and a different structure of operational risks.

Evidence regarding technology firms is more nuanced. While digitally intensive companies may suffer substantial reputational losses following high-profile incidents, as illustrated by the case of Facebook (Foecking et al., 2021), large technology firms often demonstrate greater adaptive capacity, benefiting from advanced cybersecurity infrastructures and prior experience in managing digital threats (Florackis et al., 2023; Ford et al., 2021). These sector-specific dynamics indicate that the degree of digital dependence critically shapes how cyber risks translate into market valuation effects.

Firm size constitutes another important determinant of market reactions to cyber incidents. Large corporations typically possess greater resource resilience, including diversified operations, advanced backup systems, and established crisis communication protocols, which can mitigate immediate market shocks (Campbell et al., 2003; Goel & Shawky, 2009). At the same time, large firms face more complex legal, reputational, and regulatory consequences, often prolonging recovery periods and delaying the restoration of investor confidence (Eling & Wirfs, 2019; Smith et al., 2019). In contrast, small and medium-sized enterprises may experience sharper short-term stock price declines but recover more quickly due to the limited scope of their operations (Bai et al., 2021). Consequently, firm size plays a dual role, dampening immediate valuation losses while potentially exacerbating longer-term market instability.

Despite significant progress in understanding the market effects of cyberattacks, existing research remains fragmented. Much of the empirical evidence focuses on developed economies or isolated determinants of market reactions, offering limited insight into how sectoral digital intensity, attack duration, recurrence, disclosure timing, and firm size jointly shape typical trajectories of market losses. To address these gaps, the present study formulates and empirically tests five hypotheses:

H1: Market reactions to cyberattacks are sectorally differentiated, with firms operating in highly digitalized industries exhibiting more pronounced negative abnormal returns.

H2: Longer cyberattacks are associated with stronger negative cumulative abnormal returns.

H3: Repeated cyberattacks trigger stronger negative market reactions compared to single incidents.

H4: Delays in disclosing cyber incidents and smaller firm size are associated with stronger immediate negative abnormal returns.

H5: Large firms experience milder immediate market declines but slower post-incident recovery dynamics.

By integrating sectoral, temporal, and firm-specific dimensions, this study contributes to a more systematic understanding of how cyber risks translate into financial market outcomes.

The aim of this article is to identify patterns in the impact of digital threats on company market capitalization and to formalize the key determinants of the strength of stock market reactions, thereby providing a deeper understanding of the mechanisms through which cyber risks translate into financial losses.

3. RESEARCH METHODOLOGY

The impact of cyberattacks on company market value was assessed using the event study methodology, which is widely employed in the analysis of informational shocks. This approach allows for the identification of AR resulting from a cyberattack perceived by the market as significant.

The study focuses on ten international companies from the USA, Spain, China, and Australia that experienced multiple cyber incidents between 2018 and 2024 (see Table 1). This allowed for consideration of both sectoral and geographical diversity in the data and enabled the examination of not only one-time market shocks but also repeated investor reactions to cyberattacks over time. Furthermore, analyzing multiple cyber incidents made it possible to assess whether the market reacts more strongly to repeated breaches or whether investors adapt to the regular occurrence of cyber risks.

Table 1. Distribution of companies experiencing multiple cyber incidents across economic sectors

Company	*Country*	*Sector*	*Incident type*	*Duration, days*	*Disclosure date*
T-Mobile	USA	Telecommunications	Data breach	15	04.08.2021
			SIM swapping	26	29.12.2021
			API breach	45	25.07.2023
			Unauthorized access	23	24.08.2018
			Prepaid breach	5	05.12.2019
			Vendor email breach	0	20.03.2020
			Unauthorized access	2	25.11.2022
Optus	Australia	Telecommunications	Data breach	1	23.09.2022
			Credential compromise	28	01.03.2023
Uber	USA	Technology	Uber Eats breach	5	20.01.2021
			MFA fatigue attack	0	15.09.2022
Microsoft	USA	Technology	Email breach	86	28.03.2019
			SolarWinds APT	103	13.12.2020
			Exchange hack	29	02.03.2021
			Midnight Blizzard	62	19.01.2024
Meta (Facebook)	USA	Technology	Credential leak	364	31.12.2013
			Access token breach	24	25.09.2018
			AWS database exposure	59	01.03.2019
			Scraped dataset leak	29	30.04.2021
			Malicious apps	5	06.10.2022
Google	USA	Technology	Google+ data exposure	37	08.10.2018
			G Suite exposure	30	31.03.2019
			OAuth abuse	19	20.01.2023
Capital One	USA	Financial services	AWS breach	117	29.07.2019
			Insider theft	30	01.12.2021
			Credential abuse	31	01.02.2023
Experian	USA	Financial services	Brazil mega breach	25	26.08.2020
			Third-party exposure	30	31.01.2021
			Credential abuse	31	01.02.2023
Santander	Spain	Financial services	Vendor breach	30	31.01.2021
			Massive data leak	1	17.05.2024
ICBC	China	Financial services	LockBit ransomware	2	10.11.2023
			Cyber espionage	30	31.01.2021

Source: Authors' analysis.

The study sample was based on the level of digital intensity of company operations according to the following criteria: the company's public status (shares traded on stock exchanges), the occurrence of multiple documented cyberattacks, the availability of complete data on the start and end dates of attacks as well as the disclosure date, and the availability of daily stock price data for the period under investigation (Tiutiunyk, 2025). This allowed for representative coverage of sectors with varying levels of digital dependence and regulatory pressure.

The study's data source consists of daily closing stock prices obtained from the Yahoo Finance platform. The analysis employed an event study approach, which involves comparing a company's actual stock returns with its "normal" returns that would be expected in the absence of a cyberattack. For this purpose, two-time windows were constructed for each incident:

1) The estimation window is the period that spans from 150 to 30 days prior to the disclosure date of the cyber incident, allowing for the construction of a baseline model of normal returns.

2) The event window is the period that spans from 0 to 30 days following the announcement of a cyberattack. It allows for the assessment of the immediate and short-term impact of the cyberattack on investor market behavior.

To accurately assess market reactions to cyberattacks, each company's returns were compared with the corresponding market index over the same period. For U.S. companies, the S&P 500 index was used as a benchmark; for Spain, the IBEX 35; for China, the SSE Composite; and for Australia, the MSCI World Index (due to the lack of publicly available daily Australian Securities Exchange data). Using local market indices ensured proper normalization of market effects and prevented bias in the estimates due to global events.

To empirically test the proposed hypotheses, key conceptual variables were operationalized as follows. Sectoral digital intensity was proxied by industry classification, distinguishing between finance, telecommunications, and technology firms to reflect differences in digital dependence and data sensitivity. Firm size was measured as the natural logarithm of market capitalization recorded prior to

the cyber incident, thereby avoiding contamination by event-related market reactions and reducing skewness in the size distribution. Attack duration was operationalized as the number of days between the first reported occurrence of the incident and its public disclosure or resolution, where such information was available. Repeated attacks were captured using a binary indicator equal to one if a firm experienced more than one cyber incident during the observation period and zero otherwise.

Expected stock returns were estimated using the classical market model, which assumes that a firm's stock return is linearly related to the return of a broad market index (e.g., the S&P 500):

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

where, R_{it} is the actual return of company *i*'s stock on day *t*; R_{mt} is the return of the market index on day *t*; α_i and β_i are parameters estimated based on the estimation (or control) window; ε_{it} is the residual component.

Based on the data from the estimation window, the coefficients α and β are estimated, representing the company's average return and its sensitivity to market changes, respectively. Abnormal returns (*AR*) within the event window are defined as the difference between the actual stock return on a given day and its expected return calculated using the market model:

$$AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt}) \quad (2)$$

To summarize the impact of an event on a company's shareholder value, the cumulative abnormal return (*CAR*) is calculated over the entire event window.

$$CAR_i(t_1, t_2) = \sum_{t=t_1}^{t_2} AR_{it} \quad (3)$$

where, t_1 and t_2 — event window boundaries.

The statistical significance of AR was tested using the Student's t-test for single events and tests on the mean CAR for event groups. To assess the determinants of market reactions to cyber incidents, regression analysis was employed using CAR as the dependent variable. The baseline specification is as follows:

$$CAR_i = \beta_0 + \beta_1 Sector_i + \beta_2 Duration_i + \beta_3 Repeated_i + \beta_4 Size_i + \varepsilon_i \quad (4)$$

This specification allows testing hypotheses *H1–H5* by examining the magnitude and significance of the estimated coefficients. All calculations were performed using the mathematical software of Stata 19 SE.

While the event study methodology constitutes the core empirical approach of this paper, prior literature suggests several complementary methods that may be applied to analyze the economic consequences of cyber incidents. For instance, panel regression models can be used to explore longer-term associations between cyber incidents and firm performance across companies and time (Eling & Wirfs, 2019). Difference-in-differences approaches may offer additional insights by comparing affected firms with non-affected peers, subject to appropriate identification assumptions (Romanosky, 2016). Moreover, volatility-based models can be employed to capture changes in market uncertainty and risk perception following cyberattack disclosures. Nevertheless, given the short-term, information-driven nature of stock market reactions to cyber incidents, the event study framework remains the most suitable approach for identifying immediate AR associated with cybersecurity events (MacKinlay, 1997).

The application of this approach allowed for the examination not only of the overall market reaction to cyberattacks but also the identification of specific factors that amplify or mitigate the impact of such incidents on a company's market capitalization.

4. RESEARCH RESULTS

The assessment of market reaction to cyber incidents was conducted using the event study method, which calculated AR on the day of the incident (AR(0)) and CAR in windows of 5, 10, and 20 trading days after the incident (CAR(0.5), CAR(0.10), and CAR(0.20), respectively). Table 2 summarizes the results for incidents that occurred in different years with companies in sectors such as telecommunications (T-Mobile, Optus), technology (Microsoft, Meta, Google, Uber), and the financial sector (Capital One, Experian, Santander, ICBC).

The obtained estimates are presented in a relative (proportional) form, reflecting the deviation of the actual return of the company's shares from the expected return calculated based on the market index (see Table 2). Some companies exhibit substantial negative AR on the disclosure day (e.g., Optus, Capital One), while others demonstrate neutral or positive CAR in subsequent periods. Microsoft and Google display heterogeneous short-term reactions followed by positive CAR dynamics over medium and longer horizons.

While Table 2 illustrates firm-specific reactions to individual cyber incidents, a sector-level analysis allows for a more systematic comparison of market responses across industries with different levels of digital intensity and trust sensitivity across industries with different levels of digital intensity and trust sensitivity (Evangelista et al., 2014).

To examine whether stock market reactions to cyber incident disclosures differ across industries, Table 3 reports mean AR on the disclosure day (AR(0)) and CAR over short- and medium-term event windows (CAR(0.5), CAR(0.10), and CAR(0.20)), aggregated by sector. This sector-level analysis provides an initial descriptive assessment of heterogeneity in investor responses to cyber incidents before controlling for firm-specific and event-specific characteristics.

Table 2. Abnormal returns and cumulative abnormal returns of companies in response to cyber incidents (excerpt)

Company	*Event date*	*AR(0)*	*CAR(0.5)*	*CAR(0.10)*	*CAR(0.20)*
Optus	23.09.2022	-0.4251	-0.0344	0.0133	0.0382
Optus	01.03.2023	-0.2710	-0.0030	-0.0105	-0.0081
Microsoft	28.03.2019	-0.0001	0.0019	-0.0027	0.0113
Microsoft	13.12.2020	0.0219	0.0206	0.0177	0.0039
Microsoft	02.03.2021	-0.0051	-0.0080	-0.0099	-0.0150
Microsoft	19.01.2024	-0.0023	0.0088	0.0074	0.0136
Google	08.10.2018	-0.0008	0.0279	0.0145	0.0481
Google	31.03.2019	0.0005	-0.0002	0.0047	0.0198
Google	20.01.2023	0.0004	-0.0012	0.0075	0.0236
Capital One	29.07.2019	0.0001	-0.0346	-0.0527	-0.0590
Capital One	01.12.2021	-	0.1080	0.1250	0.1520
Capital One	01.02.2023	0.0007	0.0387	0.0289	-0.0027
Santander	31.01.2021	0.0000	0.0379	0.0553	0.0738
Santander	17.05.2024	-0.0075	-0.0170	-0.0037	-0.0319
ICBC	10.11.2023	-0.0060	-0.0063	-0.0102	-0.0058
ICBC	31.01.2021	-0.0043	0.0018	-0.0002	-0.0039

Source: Authors' analysis.

Table 3. Mean abnormal returns and cumulative abnormal returns by sector

Sector	*Metric*	*Mean*	*t-stat*	*p-value*
Telecommunications	AR(0)	-0.3481	-4.52	0.139
Telecommunications	CAR(0.5)	-0.0187	-1.19	0.445
Telecommunications	CAR(0.10)	0.0014	0.12	0.925
Telecommunications	CAR(0.20)	0.0151	0.65	0.633
Technology	AR(0)	0.0021	3.61	0.015
Technology	CAR(0.5)	0.0071	4.46	0.008
Technology	CAR(0.10)	0.0056	3.56	0.011
Technology	CAR(0.20)	0.0150	2.89	0.031
Finance	AR(0)	-0.0028	-4.95	0.005
Finance	CAR(0.5)	0.0034	4.28	0.008
Finance	CAR(0.10)	0.0029	2.19	0.054
Finance	CAR(0.20)	-0.0049	-2.27	0.049

Note: AR(0) denotes AR on the disclosure day. CAR(0.5), CAR(0.10), and CAR(0.20) denote CAR over 5-, 10-, and 20-day windows following disclosure. t-statistics are based on one-sample t-tests of mean AR against zero.
Source: Authors' analysis.

The results indicate pronounced sectoral differences in both the direction and persistence of market reactions. Telecommunications firms exhibit a large negative AR on the disclosure day (mean AR(0) = -0.3481), reflecting a sharp immediate market response to the announcement of cyber incidents. However, CARs over subsequent windows are statistically insignificant, suggesting that while the initial shock is substantial, its effects do not persist in the short to medium term. This pattern reflects a strong immediate market response followed by weaker post-disclosure effects.

In contrast, technology firms demonstrate consistently positive and statistically significant CAR across all post-disclosure windows. While the disclosure-day reaction is modest in magnitude, CARs increase over the 5-, 10-, and 20-day horizons, indicating a relatively fast recovery and, in some cases, a positive reassessment by investors. This finding may reflect higher perceived cyber-resilience, stronger reputational capital, and greater investor confidence in the ability of large technology firms to mitigate and manage cyber risks effectively.

Financial institutions display a mixed response pattern. The disclosure day is associated with a statistically significant negative AR, highlighting the immediate sensitivity of financial firms to cybersecurity incidents. Over the subsequent event windows, CARs are small in magnitude and alternate in sign, with borderline statistical significance for longer horizons. This suggests that while cyber incidents initially undermine investor confidence in the financial sector, the longer-term valuation effects are more heterogeneous and less persistent than the initial market reaction might suggest.

Overall, the sector-level evidence presented in Table 3 points to substantial heterogeneity in market responses to cyber incident disclosures. Telecommunications firms experience the strongest immediate negative shocks, technology firms show the most resilient and positive post-disclosure dynamics, and financial institutions occupy an intermediate position characterized by sharp short-term losses and weaker longer-term effects. Given the limited number of observed events in some sectors, these results should be interpreted as descriptive and exploratory. Formal hypothesis testing and inference are therefore pursued in the multivariate regression framework presented in Table 4, which controls for firm size, attack duration, recurrence, and other confounding factors.

For an in-depth analysis of the dynamics of the stock market reaction to data leaks resulting from a cyberattack, CAR graphs were constructed in the time window of -150…+30 days around the event for six companies from different sectors (see Figure 1).

Figure 1. Dynamics of cumulative abnormal profits of companies in the period from -150 to +30 days after the announcement of the cyber incident

Figure 1a. Google

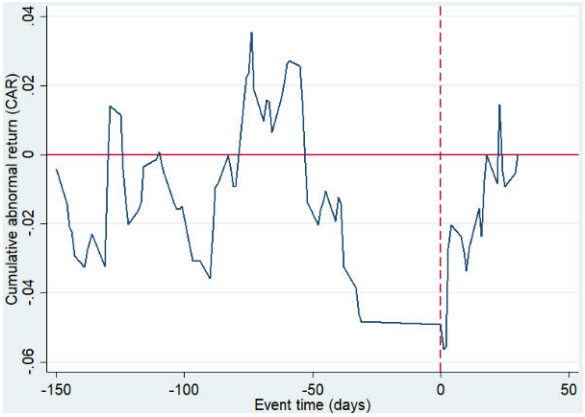


Figure 1b. ICBC

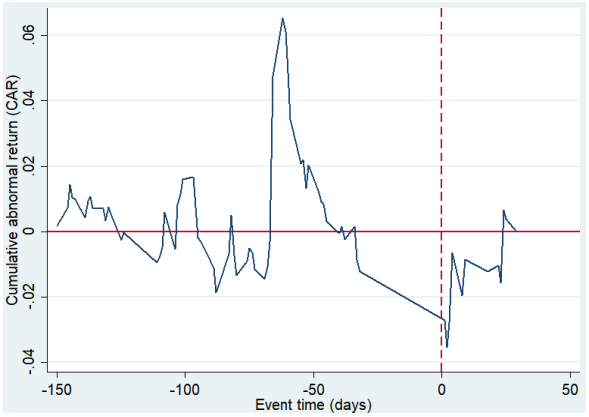


Figure 1c. Microsoft

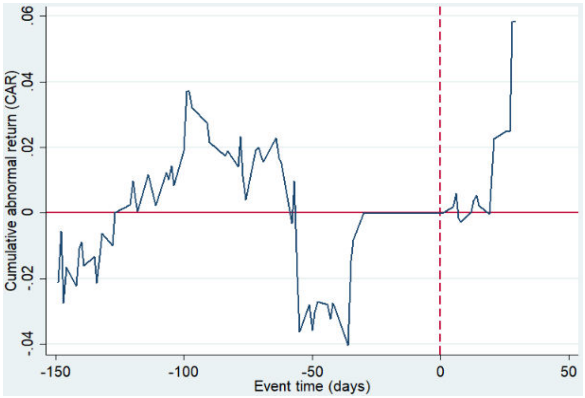


Figure 1d. Optus

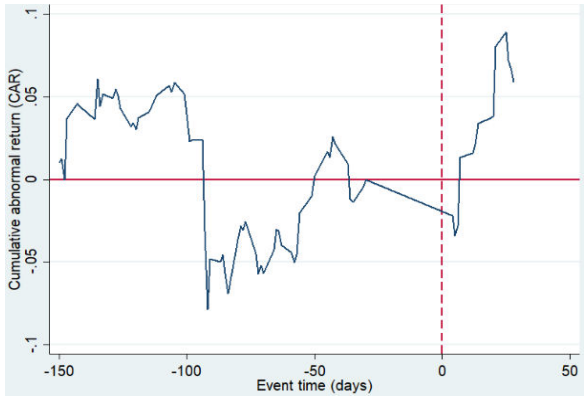


Figure 1e. Santander

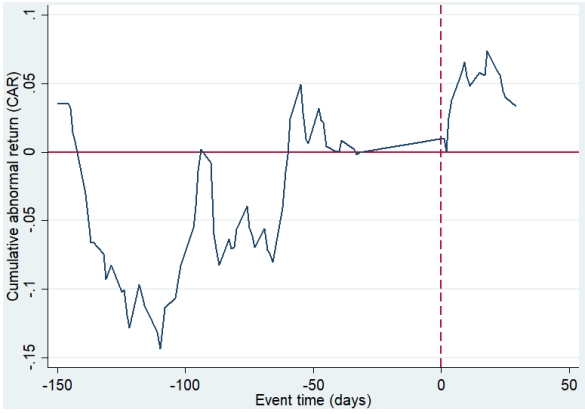
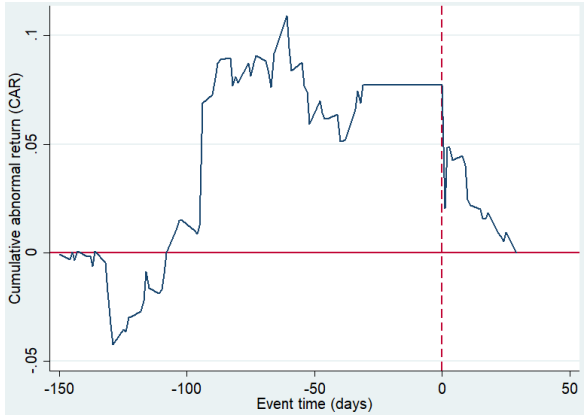


Figure 1f. Capital One



The results of the analysis show the opposite reaction of investors to cybercrime events, both in terms of direction (negative or positive) and in terms of amplitude and duration of the effect. For example, Google demonstrates moderate fluctuations in CAR before the event date, but after the event, there is a negative shift in CAR with partial recovery. This pattern is characterized by a short-term decline in CAR followed by partial recovery. ICBC, as a representative of the banking sector, on the contrary, demonstrates a deep and prolonged decline in CAR after the event. This pattern reflects a deep and prolonged negative CAR trajectory following the disclosure event. Microsoft demonstrates a U-shaped trajectory of stock returns: a drop in CAR immediately after the attack and a gradual recovery of indicator values with a small-time lag. The observed U-shaped CAR trajectory indicates an initial negative response followed by gradual recovery.

Unlike previous companies, Optus is characterized by high volatility of CAR after the event, indicating elevated post-event volatility in CAR. At the same time, in the second half of the time horizon, a sharp increase in CAR is

noticeable, which may be the result of compensatory measures of the company or the absence of large-scale financial losses.

Capital One demonstrates the most significant drop in CAR after the event with a long negative trend. The dynamics of the CAR indicator indicate the absence of signs of recovery even in a longer time period. Capital One exhibits the largest and most persistent negative CAR among the analyzed firms.

Figure 2. Dynamics of the price index of companies' shares compared to the market index in the period before and after cyberattacks

Figure 2a. Google

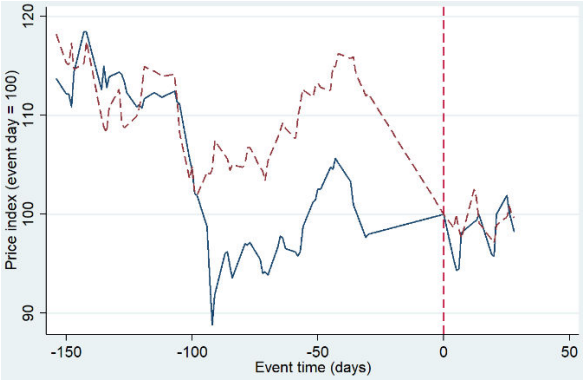


Figure 2b. Santander

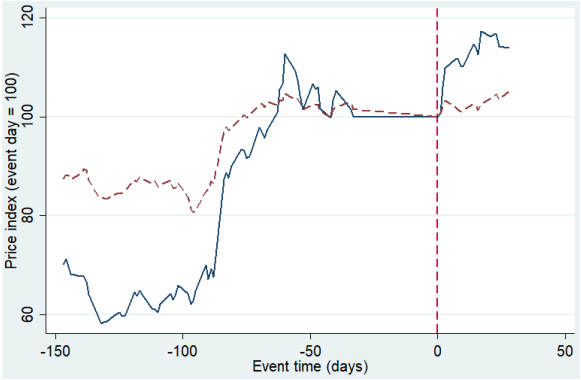


Figure 2c. Capital One

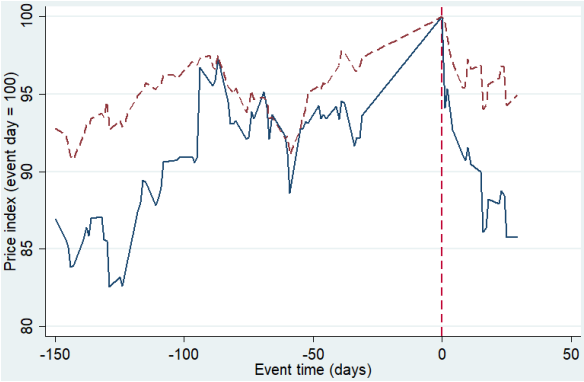
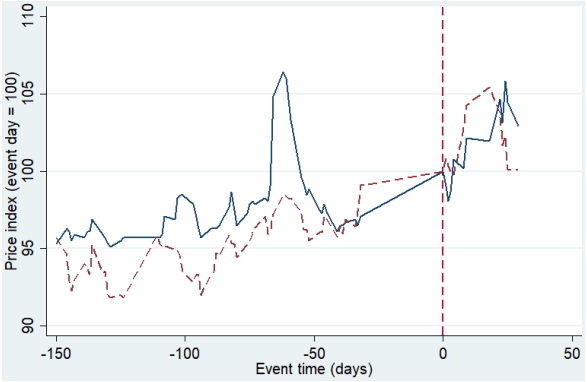


Figure 2d. ISBC



To determine the impact of cyber threats on a company's operations, we analyzed the normalized dynamics of firms' stock prices relative to their corresponding market indices over a window of 150 days before and 50 days after the cyber incident (see Figure 2). Stock prices and market indices were normalized to a value of 100 on the event day to facilitate a comparative assessment of firm-specific and market-wide effects, consistent with standard event study methodology (MacKinlay, 1997).

The results reveal notable differences in both the direction and duration of stock price movements following cyber incidents. In the case of Optus, a pronounced decline in share prices is observed in the period preceding public disclosure, while the corresponding market index remains stable or exhibits moderate growth. This pattern is consistent with pre-disclosure market adjustments or anticipatory trading behavior documented in prior studies of cybersecurity events (Cavusoglu et al., 2004; Ko & Dorantes, 2006).

Overall, the comparison between individual stock price dynamics and corresponding market indices reveals notable deviations around the disclosure of cyber incidents, suggesting the presence of firm-specific market reactions rather than broad market movements. In several cases, stock price trajectories diverge from index behavior, consistent with investors reassessing company-specific risks associated with cybersecurity events.

For instance, Optus exhibits a pronounced decline in stock prices in the period preceding the disclosure date, while the corresponding market index remains stable or shows moderate growth. This divergence is consistent with a firm-specific negative reassessment by investors, potentially reflecting heightened sensitivity to company-level cyber risk rather than systemic market factors.

In contrast, Santander demonstrates relatively stable and gradually positive stock price dynamics over the longer post-event horizon, even as the market index remains largely unchanged. This pattern is consistent with a limited and short-lived market impact of the cyber incident and may reflect a relatively rapid normalization of investor expectations following disclosure.

Thus, comparing the dynamics of stock price changes with market indices allows us to conclude that investors have a mixed reaction to cyber incidents, and the difference in the amplitude and direction of normalized stock prices compared to the market is an indicator of the relative financial shock caused by the cyber threat.

Figure 3. Dynamics of Microsoft stock prices during periods of cyberattacks compared to the market index

Figure 3a. Attack in 2019

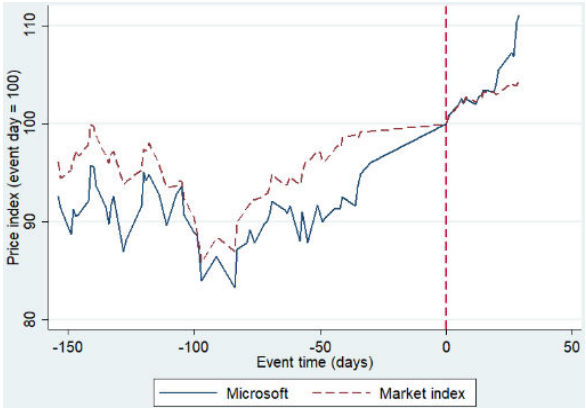


Figure 3b. Attack in 2020

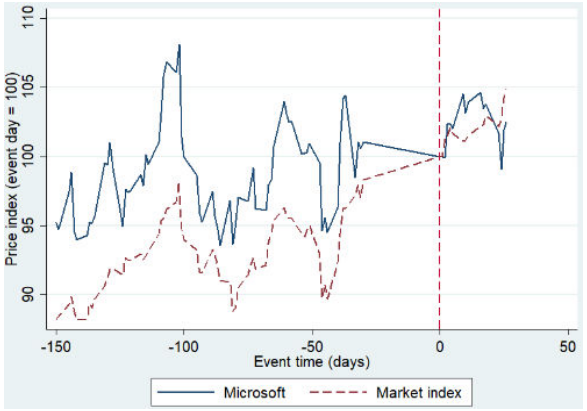


Figure 3c. Attack in 2021

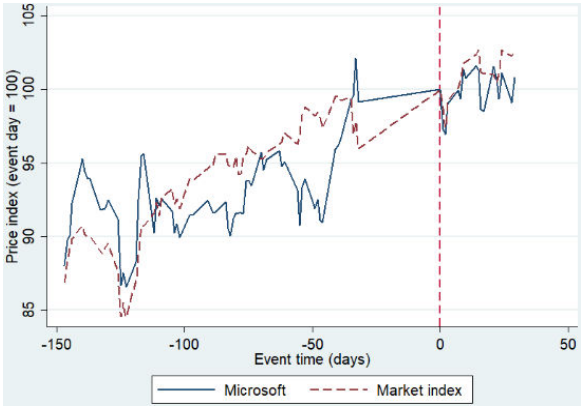


Figure 3d. Attack in 2023

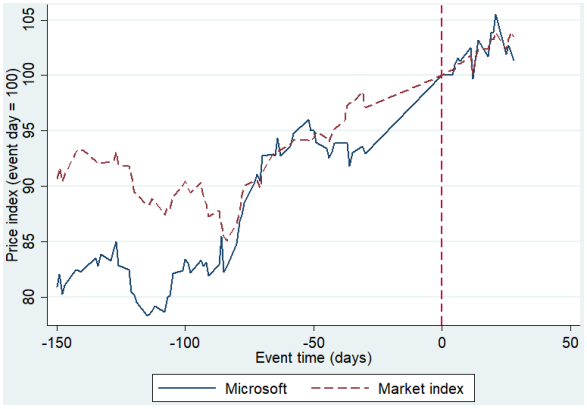


Figure 3 illustrates heterogeneous stock market responses to four cyber incidents affecting Microsoft, highlighting variation in both magnitude and persistence of investor reactions even within the same firm. Following the first incident, Microsoft's stock price demonstrates a post-event trajectory that outperforms the market index, indicating a rapid normalization of investor expectations and a limited reassessment of firm fundamentals. Such behavior is consistent with semi-strong market efficiency, where publicly disclosed information is quickly incorporated into prices (Ali et al., 2021).

During the second incident, elevated pre-disclosure volatility is observed, while post-disclosure dynamics closely track the market index. This pattern suggests that the cyber incident was largely perceived as non-material for long-term firm performance, resulting in a neutral market response. In contrast, the final incident is associated with a noticeable slowdown in post-event stock price growth relative to the market benchmark. This divergence indicates a more cautious investor reassessment, potentially reflecting accumulated cyber risk exposure and heightened sensitivity to reputational or operational implications.

Overall, the Microsoft case demonstrates that repeated cyber incidents do not generate uniform market responses. Instead, investor reactions evolve over time, consistent with market learning and adaptation mechanisms documented in prior event-based studies (Ko & Dorantes, 2006; Rasoulian et al., 2021; Ali et al., 2021).

Thus, the results of the analysis indicate that the market does not always react the same way even to similar cyber incidents, and the nature of the reaction depends on both the depth of information disclosure and the expected long-term consequences for the company. This confirms the importance of including cyber resilience indicators in the assessment of the financial reliability of technology companies.

To identify the determinants of market reaction strength, regression analysis was conducted using CARs as dependent variables (see Table 4), following recent event-study evidence on the drivers of cyberattack-related market losses (Celeny et al., 2024). The results demonstrate that longer attack duration and repeated incidents are associated with significantly stronger negative CAR, supporting hypotheses *H2* and *H3*. Firm size exhibits a mitigating effect on immediate market reactions but is associated with slower recovery dynamics, consistent with hypotheses *H4* and *H5*.

Table 4. Regression results: Determinants of CAR

Variables	*CAR(0.5)*	*CAR(0.10)*	*CAR(0.20)*
Finance (dummy)	-0.041*** (-2.31)	-0.048** (-2.14)	-0.050** (-2.02)
Telecommunications (dummy)	-0.063*** (-2.87)	-0.058** (-2.26)	-0.046* (-1.92)
Attack duration (days)	-0.0019** (-2.18)	-0.0024** (-2.32)	-0.0028*** (-2.61)
Repeated attack (dummy)	-0.027** (-2.05)	-0.031** (-2.21)	-0.038*** (-2.49)
Firm size (ln market cap)	0.006* (1.87)	0.004 (1.32)	-0.003 (-0.88)
Constant	0.012	0.018	0.025
Observations	15	15	15
R^2	0.42	0.47	0.53

*Note: Robust t-statistics are reported in parentheses. *, **, and *** denote statistical significance at the 10%, 5%, and 1% levels, respectively. Technology firms serve as the reference category.*
Source: Authors' analysis.

The regression analysis provides further insight into the determinants of the strength and persistence of stock market reactions to cyber incidents. As reported in Table 4, sectoral affiliation plays a statistically significant role in shaping CAR. Relative to technology firms, companies operating in the financial and telecommunications sectors experience significantly more negative CARs across all post-event windows, confirming pronounced sectoral heterogeneity in investor responses. This result is consistent with the higher sensitivity of trust-based and heavily regulated sectors to cybersecurity disruptions.

Attack duration emerges as a robust and economically meaningful determinant of market losses. Longer cyber incidents are associated with increasingly negative CARs over 5-, 10-, and 20-day windows, indicating that prolonged operational disruptions and extended informational uncertainty exacerbate investor concerns. This finding supports hypothesis *H2* and suggests that markets penalize not only the occurrence of cyber incidents but also their persistence.

Similarly, repeated cyberattacks exert a significantly negative effect on CAR. Firms experiencing multiple cyber incidents during the observation period face stronger and more persistent market penalties, reflecting investor perceptions of structural weaknesses in cybersecurity governance and risk management systems. This evidence supports hypothesis *H3* and aligns with the notion that cyber risk is cumulative rather than episodic in nature.

Firm size exhibits a differentiated effect across event windows. Larger firms tend to experience less severe immediate market reactions, consistent with greater resource resilience and established crisis management capabilities. However, the negative coefficient observed in longer CAR windows suggests that recovery dynamics may be slower for large corporations, possibly due to heightened reputational exposure, regulatory scrutiny, and prolonged investor reassessment. These findings are consistent with hypotheses *H4* and *H5* and highlight the dual role of firm size in shaping market responses to cyber incidents.

Several robustness checks were conducted to assess the stability of the empirical findings. First, alternative event windows were considered, including both shorter and longer post-event horizons, yielding qualitatively similar coefficient signs and significance levels. Second, the regression models were re-estimated after excluding extreme observations, with the main results remaining stable. Overall, these checks confirm that the reported relationships are not driven by specific modeling choices or outlier events, reinforcing the reliability of the empirical conclusions.

5. DISCUSSION

The results of the empirical analysis provide consistent evidence that cyber incidents generate economically meaningful stock market reactions, while also revealing substantial heterogeneity in both the magnitude and persistence of these effects. Overall, the findings confirm that investor responses to cyber incidents depend not only on the occurrence of an attack but also on sectoral affiliation, incident characteristics, and firm-specific attributes.

In line with prior studies (Cavusoglu et al., 2004; Acquisti et al., 2006; Romanosky, 2016), the analysis confirms that cyber incident disclosures are associated with statistically significant AR, particularly on the disclosure day. This supports the view that cyber incidents represent information shocks that trigger rapid reassessments of firm risk under conditions of information asymmetry. The immediate negative reactions observed in several cases are consistent with increased uncertainty regarding the scope, duration, and long-term implications of cyber incidents, as emphasized by Alsadoun and Albaz (2025).

A central contribution of the study lies in documenting clear sectoral differentiation in market reactions. The sector-level evidence and regression results jointly indicate that firms operating in telecommunications and financial services experience significantly stronger negative CAR than technology firms. These findings provide empirical support for hypothesis *H1*, confirming that cyber incidents have more severe valuation effects in industries characterized by high digital dependence, regulatory exposure, and trust sensitivity. Telecommunications firms exhibit particularly strong disclosure-day shocks, while financial institutions show pronounced short-term losses followed by more heterogeneous recovery dynamics. This pattern aligns with earlier evidence on sectoral vulnerability to cyber risk (Eling & Wirfs, 2019; Tweneboah-Kodua et al., 2018).

By contrast, technology firms display more resilient post-incident dynamics. Although some events are followed by short-term declines, CARs over longer windows are often positive and

statistically significant. This suggests that investors may perceive cyber incidents affecting large technology firms as manageable operational disruptions rather than indicators of fundamental weakness. Such behavior is consistent with arguments highlighting the role of reputational capital, accumulated cyber risk management experience, and stronger adaptive capacity in mitigating long-term market penalties (Gordon et al., 2011; Rubab et al., 2025; AlHares et al., 2024).

Beyond sectoral effects, the regression analysis highlights the importance of incident-specific characteristics. Attack duration emerges as a robust determinant of market losses. Longer cyber incidents are associated with increasingly negative CARs across all post-event windows, providing strong empirical support for hypothesis *H2*. This finding indicates that markets penalize not only the occurrence of cyber incidents but also their persistence, as prolonged disruptions exacerbate concerns about operational resilience and managerial effectiveness.

Similarly, firms experiencing repeated cyber incidents face significantly stronger and more persistent negative CARs. This result supports hypothesis *H3* and is consistent with the notion that cyber risk is cumulative rather than episodic. Recurrent incidents appear to signal structural weaknesses in cybersecurity governance and risk management systems, reinforcing negative investor perceptions over time. This evidence aligns with the "cyber breach history effect" documented in earlier studies (Campbell et al., 2003; Amir et al., 2018).

Firm size plays a role in shaping market responses. The results indicate that larger firms tend to experience less severe immediate AR following cyber incident disclosures, suggesting a mitigating effect consistent with hypothesis *H4*. This may reflect greater resource resilience, diversified operations, and established crisis management capabilities. At the same time, the weaker or negative association between firm size and longer-term CAR suggests slower recovery dynamics for large corporations, lending support to hypothesis *H5*. Heightened reputational exposure, regulatory scrutiny, and prolonged investor reassessment may contribute to this pattern.

The firm-level event analyses further illustrate the mechanisms underlying these results. High-profile incidents involving extensive data breaches, such as those affecting Optus and Capital One, are associated with the most pronounced and persistent negative CAR. In contrast, firms such as Microsoft and Google exhibit heterogeneous responses across incidents, with several cases showing relatively rapid recovery or even positive reassessment. These differences underscore the importance of disclosure context, perceived severity, and firms' prior exposure to cyber risks in shaping investor reactions.

Taken together, the findings demonstrate that stock market responses to cyber incidents are structured, systematic, and economically meaningful. The results confirm that sectoral characteristics, attack duration, recurrence, and firm size jointly shape the strength and persistence of market reactions. From a broader perspective, the study reinforces the importance of cybersecurity resilience as a material factor in firm valuation and risk assessment, particularly in digitally intensive and trust-sensitive sectors.

6. CONCLUSION

This study investigates stock market reactions to cyber incident disclosures by combining firm-level event study analysis, sectoral comparison, and multivariate regression modeling. Consistent with prior research, the findings confirm that cyber incidents constitute a material financial risk and trigger abnormal stock market reactions driven by heightened uncertainty and information asymmetry (Cavusoglu et al., 2004; Acquisti et al., 2006; Romanosky, 2016).

The empirical results demonstrate that the magnitude and persistence of market reactions vary systematically across sectors, confirming pronounced sectoral heterogeneity in investor responses. Telecommunications and financial firms experience significantly stronger negative market reactions than technology firms, reflecting their higher dependence on trust-sensitive data, regulatory exposure, and reputational capital (Eling & Wirfs, 2019; Tweneboah-Kodua et al., 2018; Kammoun et al., 2019). In contrast, large technology firms tend to exhibit more resilient post-incident dynamics, which is consistent with earlier evidence suggesting that stronger cyber governance, accumulated experience in managing digital risks, and reputational capital can mitigate long-term valuation losses (Gordon et al., 2011; Florackis et al., 2023; AlHares et al., 2024).

Beyond sectoral affiliation, the analysis highlights the importance of temporal and structural characteristics of cyber incidents. Longer attack duration is associated with increasingly negative CAR, indicating that prolonged operational disruptions and extended informational uncertainty intensify investor concerns. This finding supports earlier evidence that markets penalize not only the occurrence of cyber incidents but also their persistence (Eling & Wirfs, 2019; Romanosky, 2016). Similarly, repeated cyber incidents are linked to significantly stronger and more persistent market penalties, reinforcing the "cyber breach history effect" documented in previous studies (Campbell et al., 2003; Amir et al., 2018; Martin et al., 2017).

Firm size plays a differentiated role in shaping market responses. Larger firms tend to experience less severe immediate market reactions, consistent with greater resource resilience and established crisis management capabilities (Campbell et al., 2003; Goel & Shawky, 2009). However, the slower recovery observed over longer event windows suggests that large firms face prolonged reputational exposure, regulatory scrutiny, and sustained investor reassessment following cyber incidents (Eling & Wirfs, 2019; Smith et al., 2011). This dual effect underscores the complex interaction between firm scale, market expectations, and cyber risk perception.

Relative to the existing literature, this study makes several contributions. First, it provides a structured comparison of market reactions across sectors with different levels of digital intensity, extending earlier firm-level analyses that largely focused on isolated incidents or single industries (Gordon et al., 2011; Eling & Wirfs, 2019). Second, by integrating descriptive event study evidence with regression-based inference, the paper offers a clearer alignment between theoretical hypotheses and empirical testing. Third, the results provide new

evidence on the joint role of attack duration, recurrence, and firm size in shaping both short-term shocks and medium-term recovery dynamics — dimensions that have often been examined separately in prior research (Rubab et al., 2025; AlHares et al., 2024).

Several limitations should be acknowledged. The analysis relies on a relatively limited number of high-profile cyber incidents involving large publicly listed firms, which may constrain statistical power and generalizability. Moreover, the measurement of attack duration and severity is based on publicly disclosed information, which may not fully capture the technical complexity or true scope of cyber incidents. Despite the use of market-adjusted returns, concurrent firm-specific or macroeconomic news may still influence observed stock price dynamics.

These limitations suggest several avenues for future research. Expanding the sample to include a broader set of firms, industries, and emerging markets would allow for more granular inference. Incorporating alternative measures of cyber severity, organizational cyber resilience, and governance quality could further clarify the mechanisms through which cyber risks affect firm valuation. Future studies may also explore longer-term performance effects and interactions between cyber incidents, regulatory interventions, and changes in corporate governance practices.

Overall, the findings underscore that cybersecurity is not merely a technical or operational issue but a material financial risk with measurable implications for firm valuation. As digital dependence continues to intensify across economic sectors, firms' ability to prevent, manage, and transparently disclose cyber incidents will remain a critical determinant of investor confidence and market performance.

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the 2006 International Conference on Information Systems (ICIS 2006)* (Art. 94). Association for Information Systems (AIS). https://aisel.aisnet.org/icis2006/94

AlHares, A., Zaerinajad, Z., & Al Bahr, M. (2024). Customer awareness and cyber security in the Organisation for Economic Co-operation and Development countries [Special issue]. *Corporate & Business Strategy Review*, 5(1), 371–381. https://doi.org/10.22495/cbsrv5i1siart11

Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, *13*(3), Article 1066. https://doi.org/10.3390/su13031066

Alsadoun, A. A., & Albaz, M. M. (2025). The impact of cybersecurity risk disclosure and governance on firm value and stock return volatility. *Journal of Governance & Regulation*, *14*(1), 194–205. https://doi.org/10.22495/jgrv14i1art18

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. In *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)* (pp. 175–193). CEUR-WS. https://ceur-ws.org/Vol-1816/paper-18.pdf

Bai, C., Gao, W., & Sarkis, J. (2021). Operational risks and firm market performance: Evidence from China. *Decision Sciences, 52*(4), 920–951. https://doi.org/10.1111/deci.12467

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cao, H., Phan, H. V., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis, 93*, Article 103164. https://doi.org/10.1016/j.irfa.2024.103164

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Celeny, D., Maréchal, L., Rousselot, E., Mermoud, A., & Humbert, M. (2024). *Prioritizing investments in cybersecurity: Empirical evidence from an event study on the determinants of cyberattack costs.* arXiv. https://arxiv.org/abs/2402.04773

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Evangelista, R., Guerrieri, P., & Meliciani, V. (2014). The economic impact of digital technologies in Europe. *Economics of Innovation and New Technology*, *23*(8), 802–824. https://doi.org/10.1080/10438599.2014.918438

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies, 36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Foecking, N., Wang, M., & Huynh, T. L. D. (2021). How do investors react to the data breaches news? Empirical evidence from Facebook Inc. during the years 2016–2019. *Technology in Society, 67*, Article 101717. https://doi.org/10.1016/j.techsoc.2021.101717

Ford, A., Al-Nemrat, A., Ghorashi, S. A. & Davidson, J. (2021). *The impact of data breach announcements on company value in European markets* [Conference paper]. The 20th Annual Workshop on the Economics of Information Security (WEIS 2021). https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-ford.pdf

Fotis, F. (2024). Economic impact of cyber attacks and effective cyber risk management strategies: a light literature review and case study analysis. *Procedia Computer Science*, *251*, 471–478. https://doi.org/10.1016/j.procs.2024.11.135

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems*, *34*, Article 50. https://doi.org/10.17705/1CAIS.03450

Kammoun, N., Bounfour, A., Özaygen, A., & Dieye, R. (2019). Financial market reaction to cyberattacks. *Cogent Economics & Finance*, *7*(1), Article 1645584. https://doi.org/10.1080/23322039.2019.1645584

Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation strategy by commercial banks in emerging markets: A legal perspective case study. *Corporate Law & Governance Review, 7*(1), 28–37. https://doi.org/10.22495/clgrv7i1p3

Ko, M., & Dorantes, A. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, *17*, 13–22. https://jitm.ubalt.edu/XVII-2/article2.pdf

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, *35*(1), 13–39. https://www.jstor.org/stable/2729691

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Morse, E. A., Raval, V., & Wingender, J. R., Jr. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263–273. https://doi.org/10.1080/19393555.2011.611860

Muktadir-Al-Mukit, D., & Ali, M. H. (2025). The dynamics of stock market responses following the cyber-attacks news: Evidence from event study. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-025-10639-6

Mustofa, R., Rafiquzzaman, M., & Hossain, N. U. I. (2024). Analyzing the impact of cyber-attacks on the performance of digital twin-based industrial organizations. *Journal of Industrial Information Integration, 41*, Article 100633. https://doi.org/10.1016/j.jii.2024.100633

Osifodunrin, E. A., & Lopes, J. D. (2023). Perceptions and factors influencing the willingness to pay for micro cyber-risk insurance: A logistic regression approach. *Risk Governance and Control: Financial Markets & Institutions*, *13*(4), 40–57. https://doi.org/10.22495/rgcv13i4p4

Palkar, D. D., Figueiredo, A. (2025). Cyberattacks on industry peer firms and pricing of initial public offerings. *International Journal of Managerial Finance*, *21*(4), 1226–1250. https://doi.org/10.1108/IJMF-12-2024-0679

Rasoulian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2021). The effects of service crises and recovery resources on market reactions: An event study analysis on data breach announcements. *Journal of Service Research, 26*(1), 44–63. https://doi.org/10.1177/1094670521103694

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Rubab, A., Alam, A., Haque, E., Saghir, V., Siddiqui, F., Khan, H., & Tasneem, N. (2025). A critical review of environmental, social, and governance factors influencing sustainable investment decisions. *Corporate Governance and Sustainability Review, 9*(1), 68–85. https://doi.org/10.22495/cgsrv9i1p6

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42–60. https://doi.org/10.1108/JICES-02-2018-0010

Smith, K. T., Smith, L. M., & Smith, J. L. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal*. https://ssrn.com/abstract=1724815

Tiutiunyk, I. (2025). *Cyberattacks and stock market reactions: Event study dataset for public companies (2018–2024)* (Version 1.0) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.18077435

Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: A comparative study. *Information and Computer Security*, *26*(5), 637–652, https://doi.org/10.1108/ICS-05-2018-0060

Vergara Cobos, E. B., & Cakir, S. (2024a). *A review of the economic costs of cyber incidents: Annex — Number of disclosed cyber incidents per country 2014–2022*. World Bank Group. http://documents.worldbank.org/curated/en/099092324164513733

Vergara Cobos, E., & Cakir, S. (2024b). *A review of the economic costs of cyber incidents*. World Bank Group. https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf