

The Influence of Cyberattacks on Abnormal Stock Returns: Evidence from a Sample of Firms Listed on the Financial Market

Oumeima Boukhezar¹, Ali Djekrif²

¹(Affiliated with ECOFIMA Laboratory) Management Sciences, University of 20 August 1955 Skikda, Algeria; o.boukhezar@univ-skikda.dz

²(Affiliated with ECOFIMA Laboratory) Management Sciences, University of 20 August 1955 Skikda, Algeria. djekrifali@yahoo.fr

Article Information

Article history

Received: 21 January 2026

Accepted: 22 March 2026

Published: 31 March 2026

Corresponding Author

Oumeima Boukhezar

Email: o.boukhezar@univ-skikda.dz

Copyright © 2026, University of Abdelhafid Bousof, Mila. This is an open access article under the CC BY-NC-ND license.

Suggested Citation

Boukhezar, O & Djekrif ,A. (2026). The Influence of Cyberattacks on Abnormal Stock Returns: Evidence from a Sample of Firms Listed on the Financial Market, Finance and Business Economics Review, Vol. 10, No. 1, pp. 64-74. DOI : 10.58205/fber.v10i1.2078

Abstract: This study aims to analyze the impact of cyberattacks on abnormal stock returns between 2013–2024. We employed a descriptive–analytical econometric approach and the event study methodology to measure stock price reactions to new information. An estimation window of 120 days with a 10-day gap was adopted, and the event window was defined from $t = -5$ to $t = +5$ around the announcement day ($t = 0$). Abnormal Returns (AR), Cumulative Abnormal Returns (CAR), and their averages (AAR and CAAR) were calculated, and their statistical significance was tested using the t -test. The results indicate that stock prices record negative and statistically significant abnormal returns on the announcement day of a cyberattack, reflecting an immediate and adverse investor reaction. The findings further confirm that the impact of cyberattacks is short and primarily occur around the announcement date.

Keywords: Cybersecurity; Cyberattacks; Market Efficiency; Stock Prices.

1. Introduction

The rapid pace of digital transformation has rendered information technologies a core component of organizational activities. But this increasing reliance has been accompanied by a growth in cyber risks, which have emerged as an increasingly significant economic and financial threat. These risks are no longer purely technical in nature; rather, they have acquired a clear financial dimension due to their direct impact on corporate stability and investor confidence. Cyberattacks represent economic events that are capable of generating uncertainty in financial markets, which may be reflected in stock prices through declines or temporary reactions associated with asset revaluation. This effect is particularly pronounced for listed firms, given the sensitivity of their market values and the speed with which prices respond to information. Thus, examining the relationship between cyber risks and stock prices has become a fundamental issue in modern financial economics, as it contributes to understanding how shocks originating in the technological domain are transmitted to financial markets.

1.1. Research Problem

In the context of rapid digital transformation, cyber risks have become one of the most critical challenges that face financial markets and the firms listed therein. With the increasing frequency and expanding scope of cyberattacks over the past decade, questions have arisen regarding the extent to which these incidents are reflected in the stock prices of affected firms.

Accordingly, the central research problem addressed in this study can be formulated as follows:

To what extent do cyberattacks affect the abnormal returns of publicly listed companies' stocks?

To address this main question, the following sub-questions are raised:

- Do daily abnormal returns (AR) exhibit positive or negative values around the announcement date of cyberattacks?
- Do cumulative abnormal returns (CAR) exhibit positive or negative values over the event window?
- Is there a statistically significant effect of average abnormal returns (AAR) for firms listed in the financial market around the event?
- Is there a statistically significant effect of cumulative average abnormal returns (CAAR) for firms listed in the financial market over the event window?

1.2. Research Aim:

The study aims to establish a conceptual framework for cybersecurity, to analyze the efficiency of financial markets in incorporating cyberattacks-related-information, and to examine the impact of cyberattack announcements on abnormal stock returns before and after the event.

1.3. Research Hypotheses

To answer the main research problem, the following primary hypothesis is suggested:

- There is a statistically significant effect of cyberattacks on the abnormal returns of publicly listed companies' stocks.
- So as to address the sub-questions, the following subsidiary hypotheses are tested:
- H1: Daily abnormal returns (AR) take positive or negative values around the announcement date of cyberattacks.
 - H2: Cumulative abnormal returns (CAR) take positive or negative values over the event window.
 - H3: There is a statistically significant effect of average abnormal returns (AAR) for firms listed in the financial market.
 - H4: There is a statistically significant effect of cumulative average abnormal returns (CAAR) for firms listed in the financial market.

1.4. Significance of the Study

The importance of this study stems from the raising prevalence of cyber risks amid the accelerated digital transformation of financial markets and the potential implications for the stability of markets and listed firms. From a theoretical perspective, the study contributes to the financial literature by enriching the understanding of the relationship between cyberattacks and stock prices, particularly within the Arab context, where empirical research in this field remains limited. From a practical standpoint, the study is important in that it measures the actual impact of cyberattacks on stock prices using the event study methodology, thereby supporting decision-makers and investors in understanding market reactions and in adopting effective strategies for cyber risk management and the improvement of confidence in financial markets.

1.5. Research Methodology

FBER

65

The study has adopted a descriptive–analytical approach in the theoretical part through an analysis of concepts related to cybersecurity and financial markets. In the empirical part, an econometric approach is employed using the event study methodology to measure the impact of cyberattacks on the stock prices of listed firms, based on historical data and appropriate statistical techniques to test the significance of this impact.

1.6. Structure of the Study

The study is organized as follows:

- Chapter One: Cybersecurity and cyber risks.
- Chapter Two: Financial market efficiency.
- Chapter Three: An empirical study of a sample of firms listed in the financial market over the period between 2013–2024.

2. Cybersecurity and Cyber Risks

Cybersecurity is one of the most prominent contemporary fields aimed to protect information and digital systems from electronic threats and attacks, which have come to pose a real risk to individuals, organizations, and states.

2.1. Cybersecurity and Related Concepts

2.1.1. Cybersecurity

Cybersecurity is the practice that consists of defending computers, mobile devices, electronic systems, networks, and data against malicious attacks. It is also used to denote the security of networks, information systems, data and information, and internet-connected devices. Accordingly, it refers to the field that deals with the measures and protection standards that must be adopted or complied with so as to confront threats, prevent attacks, or at least mitigate their effects (Benberghout, 2023, p. 447)

2.1.2. Cybersecurity Tasks

Some of the most important tasks of cybersecurity include (Touahri, 2023, p. 282)

- Protecting users and ensuring the security of electronic devices: Via special protocols like encrypting emails, files, and other important data, which helps safeguard information during transmission and from theft.
- Protecting computer systems from viruses: As viruses can lead to serious problems.
- Reducing cybercrime: Cybercrime is increasing, especially with rapid technological development. Cybersecurity also protects organizations and companies from malicious software aimed at fraud and prevents extortion attempts.
- Preventing the illegal use of information: To protect individuals and entities from harm.
- Maintaining the safety and security of society: By the protection of private information across all sectors (health, education, financial, industrial, etc.).
- Contributing to national security: As countries increasingly rely on digitalization across various fields, including the military—where information and certain weapons require specialized software—cybersecurity has become crucial for national security. It is now considered an integral part of it, not only for protecting the military but for safeguarding all sectors.

2.1.3. Types of Cyber Risks

Cyber risks differ depending on their source and nature, and can arise either from within the organization or from external parties.

2.1.3.1. Internal Cyber Risks

About 61% of cyberattacks originate from within organizations; employees, visitors, customers, suppliers, service providers, trainees or residents, and maintenance personnel who may have access to technological, commercial, or financial secrets and could potentially leak this information. A substantial amount of information can be retrieved from the recycle bin, as deleted data are not permanently erased. The recycle bin functions as a folder from which various types of sensitive information can be recovered, including draft contracts, restructuring plans, stock market data, as well as

financial and accounting records. This calls for greater awareness of such issues. (Chamby, 2023, p. 242)

2.1.3.2. External Cyber Risks

The most significant external risks result from attacks targeting different types of information systems (Chamby, 2023, p. 242) including:

- Distributed Denial-of-Service (DDoS) attacks: A widely used technique in which hackers overwhelm websites by flooding them with large volumes of unnecessary data, sent remotely,
- Malicious software (Malware): Malware is defined as any code covertly embedded within a system to cause harm without the user's consent. Through such software, critical operations are disrupted, sensitive information is exfiltrated, and unauthorized entry into private networks is secured. Various malicious entities including viruses, Trojans, logic bombs, backdoors, and computer worms are widely identified as the primary drivers of these digital threats.
- Trojan: This category of malicious software is designed so that a personal computer or device can be controlled remotely once the program is opened or installed by the user.
- Spyware Keyloggers: This type of malware is capable of capturing all information entered by the victim and covertly sending it to the attacker
- Ransomware: The files of an organization or individual are encrypted once the malicious program is opened, after which a ransom is demanded by the attacker to restore access to the files.
- New-generation advanced viruses (e.g., Pegasus): Pegasus is a sophisticated spyware program that was developed by NSO Group and was sold to governments for alleged security purposes. However, recent reports indicate that it has been used to infiltrate and monitor officials in neighboring countries.

FBER

67

3. Financial Market Efficiency

Financial markets play a crucial role in the modern economy, as they are fundamental infrastructures through which financial resources are efficiently distributed and investment and economic growth are fostered. Through these markets, savings are transformed into productive investments, and the necessary capital can be accessed by firms and individuals to support their activities and projects. Moreover, liquidity is provided, and the transfer and distribution of risk among various economic agents is effectively facilitated.

3.1. The Concept of Financial Market Efficiency

Efficient financial markets are defined as “a market in which security prices respond to changes resulting from the analysis of data and information flowing into the market, with such responses occurring rapidly enough to equate the market value of a stock with its intrinsic value. Under these conditions, no group of investors can achieve abnormal profits at the expense of others by identifying stocks that are under- or overvalued. In an efficient market, all investors earn the same rate of return for a given level of risk” (Satouri, 2010, pp. 166-167)

3.2. Characteristics of an Efficient Market

According to the concept of stock market efficiency, a set of characteristics can be derived that distinguish an efficient market: (Maftah & Maarfi, 2009, p. 182)

- Participants in such a market are characterized by rationality in making their diverse investment decisions, which motivates them to strive to maximize their wealth;
- Information is available to everyone—lenders, investors, management, government

agencies, and auditors—at no cost, leading to similar expectations regarding company performance in the coming periods;

- There is complete freedom to trade securities without any tax restrictions, and no trading costs are imposed on them;

- The presence of a large number of participants means that no single investor can influence prices in such a market;

- In such a market, no investor can achieve a higher return than other investors because the return is sufficient to compensate each investor for the risks involved in investing in the specific stock being traded.

The efficiency of the stock market depends on the efficiency of financial information systems. Therefore, the success of the stock market requires information built upon a set of elements, including:

- The visibility of financial disclosure and its role in regulating the movement of the financial market, known as public disclosure, which provides sufficient information that can be used to compare different investment opportunities.

- The availability of financial information that reflects the financial position of the institution in question to calculate its true value.

3.3. Levels of Financial Market Efficiency

Efficiency is considered as a relative rather than an absolute concept. As a consequence, researchers typically divide efficiency into three levels. (Saadaoui, 2014, pp. 11-12) :

- A- Weak level: At this level, prices are observed to follow a random pattern, implying that past price movements are not considered to provide guidance for future price behavior. Under weak-level efficiency, abnormal returns cannot be achieved by investors through reliance on historical price data.
- B- Semi-strong level: At this level, prices reflect both historical and publicly available current information. Investors are consequently unable to achieve abnormal returns through the analysis of published accounting reports or other publicly available information, as such information has already been incorporated into prices.
- C- Strong level: At this level, prices reflect all information—historical, public, and private. Thus, market participants cannot earn abnormal returns even by using private or insider information, as such information is fully reflected in prices.

4. An Empirical Study of a Sample of Firms Listed in the Financial Market over the Period 2013–2024

4.1. Data and Methodology

4.1.1. Data

Data collection tools are considered a fundamental element in ensuring the credibility and reliability of research findings. Within the framework of this study, the population and sample were precisely defined to include firms that were subjected to cyberattacks during the period from 2013 to 2024

Table.1. List of Companies Listed on the Financial Market that Were Subject to Cyberattack

Company's name	Company's code	Date of the cybersecurity attack announcement	Type of announcement
Sony	SONY	14/11/2014	Officially documented press release
Adobe	ADBE	03/10/2013	Official announcement
Intel	INTC	06/08/2020	Officially documented

			press release
Amazon	AMZN	12/11/2024	Official announcement
Hewlett Packard Enterprise	HPE	29/01/2023	Official announcement
Facebook	META	28/09/2018	Official announcement
Microsoft	MSFT	02/03/2021	Officially documented press release

Source: Prepared by the researcher based on websites

Historical stock price data for the sampled firms were collected from the website *finance.yahoo.com*.

4.1.2. Event Study Methodology

The event study methodology is one of the most prominent quantitative approaches used in the analysis of financial market reactions to specific events and to measure the economic impact of such events on security prices. This methodology is grounded in the efficient market hypothesis, under which stock prices are assumed to immediately reflect all available information. Accordingly, any abnormal price change can be attributed to the event itself. (MacKinlay, 1997, S. 35)

FBER

69

A- Event Window

The event window was defined to measure the impact of the cyberattack on stock prices around the announcement date. The official announcement date or the date on which the information was leaked was taken as the reference point ($t = 0$). A short-term event window extending from five days before the event to five days after the event ($t = -5$ to $t = +5$), comprising 11 trading days, was selected in order to capture abnormal returns generated by the event.

B- Estimation Window

The estimation window was set at 120 trading days to estimate the market model parameters (α and β) required to compute expected returns. This window extends from $t = -135$ to $t = -16$. In addition, a 10-day gap was introduced between the estimation window and the event window to isolate the effect of the cyber event and to prevent information leakage into the estimation period. This approach ensures accurate estimation of normal returns and objective calculation of abnormal returns, in line with standard methodological practices in event study research.

C- Market Index

The use of a single market index, such as the S&P 500, is generally preferred in event studies, as a unified and reliable benchmark for measuring normal and abnormal returns is thereby provided. Comprehensive market representation is also ensured, while methodological complexity is reduced. Moreover, the comparability of results with previous studies is enhanced, given that the index is widely recognized and commonly used as a benchmark in financial research.

D- Abnormal Returns

the abnormal return is calculated as the difference between the actual return of the stock after the occurrence of the event and the expected (normal) return that would have prevailed in the absence of the event. In other words, the abnormal return on day

t —that is, the cyberattack announcement day—is defined as the difference between the actual stock return and the expected normal return. This relationship is expressed by the following equation. (Arcuri, Brogi, & Gandolfi, 2018, p. 74).

$$AR_{it} = R_{it} - ER_{it}$$

Where:

- AR_{it} = Abnormal return of stock i on day t ;
- R_{it} = Actual return of stock i on day t ;
- ER_{it} = Expected (normal) return of stock i on day t .

Average Abnormal Return (AAR)

The Average Abnormal Return (AAR) represents the mean abnormal return of all stocks at time t within the event window. It is calculated for each day using the following formula (Faizil & Anggoro , 2019, p. 307)

$$AAR_t = \frac{1}{N} \sum_{i=1}^n AR_{it}$$

Where:

- AAR = Average Abnormal Return,
- N = Number of events (stocks) in the sample.

Cumulative Abnormal Return (CAR)

The Cumulative Abnormal Return (CAR) over the period from $t1_{t_1}$ to $t2_{t_2}$ represents the sum of the abnormal returns included within that period. It is expressed by the following equation (MacKinlay, 1997, S. 21)

$$CAR_{i(t1, t2)} = \sum_{t=t2}^{t2} AR_{it}$$

Cumulative Average Abnormal Return (CAAR)

The Cumulative Average Abnormal Return (CAAR) is calculated by summing the Average Abnormal Returns (AAR) for each day within the event period. It can be expressed succinctly using the following formula (Faizil & Anggoro , 2019, p. 307)

$$CAAR_{t1, t2} = \sum_{t=t2}^{t1} AAR_t$$

4.2. Results Analysis

4.2.1. Calculation of Daily Abnormal Returns (AR)

The analysis of Abnormal Returns (AR) constitutes one of the most important steps in applying the Event Study methodology. It allows for estimating the direct impact of the studied event—namely, cyberattacks—on the performance of stocks of firms listed in the financial market.

Table .2. Percentage of Daily Abnormal Returns of Companies Listed on the Financial Market that Were Subject to Cyberattacks

Stock code	AR (t=-5)	AR (t=-4)	AR (t=-3)	AR (t=-2)	AR (t=-1)	AR (t=0)	AR (t=+1)	AR (t=+2)	AR (t=+3)	AR (t=+4)	AR (t=+5)
SONY	-0,34	3,96	0,94	-0,24	-1,11	0,98	-1,92	4,43	-2,2	-1,74	3,13
ADBE	0,08	0,26	0,42	0,12	-1,7	-0,36	0,63	-0,62	-1,24	-0,34	1,24
INTC	0,39	-1,35	0,44	1,38	-1,1	-0,71	-1,08	2,21	-1,04	0,5	-0,95
AMZN	0,25	0,25	0,48	-1,3	-0,65	1,55	2,55	-0,22	-2,23	-0,88	0,99
HPE	-0,87	-0,28	1,63	0,5	-0,39	-1,08	0,72	-1,94	-0,9	-0,83	-0,46
META	-1,71	2,12	0	1,81	0,86	-2,51	-1,63	-1,75	1,94	-0,96	-0,07

Source: Prepared by the researcher based on EXCEL and EVIEWS outputs

A- Analysis of Daily Abnormal Returns (AR)

Based on Table 2, which presents the Abnormal Returns (AR) for a sample of listed firms over the event window from $t=-5$ to $t=+5$ (with the event occurring at $t=0$), a wide variation across firms was observed. Notably, values differed significantly on the event day ($t=0$), with some firms recording positive ARs while others registered negative ARs. Extreme values, both high and low, were observed on certain days, and the distribution of positive and negative returns was uneven across the event window. Some firms experienced larger shocks on specific days before or after $t=0$, while others maintained relative stability throughout the same period.

Overall, Table 2 indicates that the market did not respond uniformly to the cyberattack event. Reactions varied across firms: some were negatively impacted due to the risks associated with the event, while others managed to record positive abnormal returns.

B- Calculation of Cumulative Abnormal Returns (CAR)

After computing the daily abnormal returns for each firm during the event period, the Cumulative Abnormal Return (CAR) is calculated by aggregating the daily ARs over the specified period. This measure captures the total impact of the event across the entire event window, providing insight into the overall effect of the cyberattack on the stock performance of each firm.

Table .3. Percentage of Cumulative Abnormal Returns of Companies Listed on the Financial Market that Were Subject to Cyberattacks

Stock code	CAR (-5,-4)	CAR (-5,-3)	CAR (-5,-2)	CAR (-5,-1)	CAR (-5,0)	CAR (-5,+1)	CAR (-5,+2)	CAR (-5,+3)	CAR (-5,+4)	CAR (-5,+5)
SONY	3,62	4,56	4,32	3,21	4,19	2,27	6,7	4,5	2,76	5,89
ADBE	0,34	0,76	0,88	-0,82	-1,2	-0,55	-1,17	-2,41	-2,75	-1,51
INTC	-0,96	-0,52	0,86	-0,24	-1	-2,03	0,18	-0,86	-0,36	-1,31
AMZN	0,5	0,98	-0,3	-0,97	0,58	3,13	2,91	0,68	-0,2	0,79
HPE	-1,15	0,48	0,98	0,59	-0,5	0,23	-1,71	-2,61	-3,44	-3,9
META	0,41	0,41	2,22	3,08	0,57	-1,06	-2,81	-0,87	-1,83	-1,9
MSFT	-1,54	-0,8	1,3	0,31	0,25	0	1,39	1,11	-0,02	1,01

Source: Prepared by the researcher based on EXCEL output

Table 3 reflects the overall changes in stock prices across the event window for each firm, showing a clear variation in the intensity of the impact among companies. Some firms recorded positive values, while others exhibited negative values, with notable differences in the direction of returns throughout the event period. Extreme positive and negative values were concentrated on specific days, whereas some firms tended to show gradual stability or a continuous decline following the event.

C- Calculation of Average Abnormal Returns (AAR)

To analyze the market's overall response, the Average Abnormal Return (AAR) was computed across the entire sample. This allowed for the assessment of the general trend of the event's impact on the listed firms. Subsequently, the statistical significance of these averages was tested using the *t*-test to determine whether the observed effects were statistically meaningful, thereby establishing whether the cyberattack event had a significant impact on stock prices.

Table .4. T-stat for the average of abnormal returns (% AAR)

T	(AAR%)	T-stat	Sig
(t=-5)	-0,41	-1,461	
(t=-4)	0,58	0,832	
(t=-3)	0,66	3,404	**
(t=-2)	0,62	1,358	
(t=-1)	-0,73	-2,369	*
(t=0)	-0,31	-0,617	
(t=+1)	-0,14	-0,235	
(t=+2)	0,50	0,573	
(t=+3)	-0,85	-1,588	
(t=+4)	-0,77	-2,915	**
(t=+5)	0,70	1,367	

*Statistically significant at $\alpha = 0,05$, **Statistically significant at $\alpha = 0,01$

Source: Prepared by the researcher based on SPSS output

Table 4 presents the Average Abnormal Returns (%AAR). The results indicate that the AAR was positive and statistically significant at the 0.01 level on day $t=-3$, and negative and statistically significant at the 0.01 level on day $t=+4$. Additionally, a negative AAR was observed on day $t=-1$, which was statistically significant at the 0.05 level. For the remaining days within the event window, no statistically significant effects were detected.

D- Calculation of Cumulative Average Abnormal Returns (CAAR)

The analysis of Cumulative Average Abnormal Returns (%CAAR) provides insights into the nature of firms' responses to cyber risks, indicating whether these reactions are temporary or persist over time. By aggregating the daily AARs across the event window, CAAR allows for an assessment of the total impact of the cyberattack events on the stock performance of the sampled firms, helping to determine the overall magnitude and duration of the market's reaction.

Table.5. T-stat for the average of cumulative abnormal returns (% CAAR)

T	(CAAR%)	T-stat	Sig
(-1, +1)	-1,18	-1,399	
(-2, +2)	-0,05	-0,062	
(-3, +3)	-0,24	-0,359	
(-5, +5)	-0,13	-0,112	

*Statistically significant at $\alpha = 0,05$, **Statistically significant at $\alpha = 0,01$

Source: Prepared by the researcher based on SPSS output

The results for the sampled firms showed that the Cumulative Abnormal Returns (%CAAR) were negative across all event windows, with values of -1.18% in the (-1, +1) window, -0.05% in (-2, +2), -0.24% in (-3, +3), and -0.13% in (-5, +5). Corresponding *t*-values were weak and statistically insignificant across all windows.

4.3. Interpretation of Results

4.3.1. Abnormal Returns (AR) and Cumulative Abnormal Returns (CAR)

The analysis of daily abnormal returns (AR) and cumulative abnormal returns (CAR) over the event window from $t=-5$ to $t=+5$ revealed that the impact of cyberattacks was not uniform across listed firms, with considerable variability observed. Some firms recorded positive abnormal returns, particularly on the event day or immediately after, reflecting their ability to absorb shocks or for investors to capitalize on market opportunities. Conversely, other firms exhibited negative returns, indicating direct adverse effects of the event and a short-term decline in investor confidence. Peak positive and negative values were concentrated on specific days within the event window, demonstrating periods of strong market reaction versus intervals of relative stability.

Cumulative abnormal returns (CAR) were also observed to display notable differences in magnitude and direction. For some firms, gradual recovery and stabilization were observed following the event, while successive declines continued to be experienced by others, reflecting differences in information assimilation and resilience across firms. This indicates that the impact of cyberattacks is influenced by firm-specific characteristics..

4.3.2. Average Abnormal Returns (AAR) and Cumulative Average Abnormal Returns (CAAR)

The results for the sample firms showed that the Average Abnormal Returns (AAR%) were positive and statistically significant at the 0.01 level on day $t=-3$, negative and significant at the 0.05 level on day $t=-1$, and negative and significant at the 0.01 level on day $t=+4$. This pattern can be explained by the nature of the technology sector, which is affected by rapidly evolving and interrelated factors. Positive returns prior to the event may reflect investors' anticipatory expectations or early signals related to the attack, rather than information leakage, especially given the 10 day event isolation window. The continued negative impact on day +4 likely reflects a gradual re-evaluation by investors of the attack's magnitude rather than delayed reaction to the information.

Cumulative Average Abnormal Returns (CAAR%) were negative across all windows but not statistically significant, suggesting that the market perceived the cyberattacks as having limited impact within this highly capable technological sector, where potential losses are mitigated by advanced security measures.

5. Conclusion:

This study analyzed Cyberattacks on Abnormal Stock Returns of U.S.-listed firms during the period 2013–2024, in light of a noticeable increase in cyberattacks and market sensitivity to such events. Using the Event Study methodology, abnormal and cumulative abnormal returns were measured around the announcement date of cyberattacks. The main findings are summarized as follows:

- Individual Abnormal Returns (AR%) were predominantly negative on the event day ($t = 0$), indicating that a negative market reaction to cyberattack announcements was observed.
- Cumulative Abnormal Returns (CAR%) varied across firms, with some recording positive returns and others negative. Peak impacts occurred on specific days within the event window, reflecting differences in recovery speed and information assimilation.
- Average Abnormal Returns (AAR%) were positive and significant at 0.01 on day $t=-3t = -3t=-3$, negative and significant at 0.05 on day $t=-1t = -1t=-1$, and negative and significant at 0.01 on day $t=+4t = +4t=+4$. These results are consistent with the dynamic and interrelated nature of the technology sector.
- Cumulative Average Abnormal Returns (CAAR%) were negative across all windows but statistically insignificant, indicating that the market viewed the cyberattacks as having limited overall impact.

Based on the findings, the following recommendations are to be suggested:

- ✓ Cyber risk assessments should be integrated into financial models and performance evaluations to allow better analysis of firms' intrinsic value.
- ✓ Encourage financial regulatory authorities to implement mandatory disclosure standards for cyber incidents.
- ✓ Investors' awareness should be raised vis-a-vis the importance of evaluating cybersecurity alongside traditional financial indicators.
- ✓ Promote collaboration between firms and technology companies to share expertise and information on cyber threats.

FBER

74

6. References :

- Maftah, S., & Maarfi, M. (2009). A Study of the Reality of Arab Securities Markets and Ways to Enhance Their Efficiency. *Majalt ElBahit*, 181-194.
- Saadaoui, Y. (2014). Requirements for financial market efficiency: Analytical study of the Algerian stock exchange. *Majallat al-Iqtisad wa Tanmiya al-Bashariya*, 7-20.
- Satouri, E. (2010). Requirements for enhancing capital market efficiency: Case study Algeria. *Majallat al-Ulum al-Ijtima'iya wa al-Insaniya*, 164-195.
- Touahri, A. (2023). Cybersecurity Strategies as a Challenge to Digital Transformation in Government Organizations: Reference to the Experience of the United Arab Emirates. *Majlat Al-Risala for Media Studies*, 291-279.
- Benberghout, L. (2023). Cybersecurity and data privacy protection in Algeria in the era of digital transformation and AI: Threats, technologies, challenges, countermeasures. *Majallat al-Ittisal al-Duwaliyya*, 457-443.
- Chamby, B. (2023). Cyber risk insurance. *Majallat Herodot lil-Ulum al-Insaniya wa al-Ijtima'iya*, 257-237.
- Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The Effect of Cyber-Attacks on Stock Returns. *Corporate Ownership & Control (Virtus Interpress)*, 83-70.
- Faizil, I., & Anggoro, B. (2019). Cumulative Average Abnormal Return and Semistrong Form Efficiency Testing in Indonesian Equity Market over Restructuring Issue. *International Journal of Economics and Financial Issues*, 107-114.
- MacKinlay, C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, 39-13.