THE EFFECT OF CYBERATTACKS ON EUROPEAN FINANCIAL INSTITUTIONS: AN EVENT STUDY APPROACH

Filippo Gervasutti *, Fabio M. Manenti **

* Department of Economics and Management "M. Fanno", University of Padua, Padua, Italy
** *Corresponding author,* Department of Economics and Management "M. Fanno", University of Padua, Padua, Italy
Contact details: Department of Economics and Management "M. Fanno", University of Padua, Via del Santo, 33, 35123 Padua, Italy

OPEN ACCESS

How to cite this paper: Gervasutti, F., & Manenti, F. M. (2026). The effect of cyberattacks on European financial institutions: An event study approach. *Corporate Ownership & Control, 23*(1), 84–94. https://doi.org/10.22495/cocv23i1art8

ISSN Online: 1810-3057
ISSN Print: 1727-9232

Received: 26.11.2025
Revised: 24.02.2026; 05.03.2026
Accepted: 13.03.2026

JEL Classification: G14, G21
DOI: 10.22495/cocv23i1art8

Abstract

This paper investigates how cyberattacks affect the market valuation of European financial institutions. Using an event study methodology on a sample of 31 cyber incidents affecting European financial firms between 2016 and 2024, we document a clear and statistically significant negative market reaction concentrated on the announcement day. Importantly, we find no evidence of abnormal price movements prior to disclosure, which is inconsistent with systematic insider trading. In contrast to prior studies that report pre-announcement abnormal returns (ARs) around cyber incident disclosures, our findings suggest that information leakages and insider trading may be less of a concern in the European financial sector. A time-trend analysis reveals diverging patterns: while the impact of non-confidential attacks has intensified, the market response to confidentiality breaches has weakened, consistent with improved disclosure and crisis management practices.

Keywords: Cybersecurity, Event Study, Abnormal Returns, Stock Market

Authors' individual contribution: Conceptualization — F.G. and F.M.M.; Methodology — F.G.; Formal Analysis — F.G.; Investigation — F.G.; Writing — Original Draft — F.G. and F.M.M.; Writing — Review & Editing — F.G. and F.M.M.; Supervision — F.M.M.; Funding Acquisition — F.M.M.

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

Acknowledgements: This study was carried out within the project "Cyber resilience: Markets, investments and regulation", funded by the European Union, Next Generation EU within the PRIN 2022 PNRR program (D.D.1409 del 14/09/2022 Ministero dell'Università e della Ricerca), Code P20229EL9W.

1. INTRODUCTION

The increasing digitalization of the financial sector has profoundly amplified its exposure to cyber threats. Financial institutions rely heavily on interconnected technologies and sensitive data, making cybersecurity not merely an operational concern but a central determinant of market confidence and systemic stability. In this context, the sector has become a prime target for malicious actors: in 2024, finance ranked as the third most attacked industry in the European Union, following the public sector and transportation (Council of the European Union, 2025). Understanding how cyber incidents affect the market valuation of financial firms is, therefore, of critical importance to managers, regulators, and investors alike.

In the present study, we revisit prior evidence within a focused and updated context by analysing cyber incidents affecting European financial institutions between 2016 and 2024. Employing robust parametric and non-parametric event study techniques and carefully delineating short event windows to minimize contamination (Pastorello, 2001), our work provides a more recent and sector-specific reassessment of the market impact of

cyberattacks on financial firms. We find that the negative market reaction is concentrated around the announcement day and the immediate aftermath, with no evidence of abnormal price movements in the days preceding disclosure — thus rejecting any indication of insider trading. Moreover, our results indicate that non-confidential breaches are associated with clearer and more pronounced valuation losses.

Our analysis introduces an innovative dimension by examining the temporal evolution of market reactions to cyberattacks. Leveraging our relatively long observation period (from 2016 to 2024), we explore whether the intensity of the impact has changed over time — an aspect that may reflect either firms' improved resilience or an increase in sophistication of cyber threats. Furthermore, we provide a preliminary investigation into whether this evolution differs across attack typologies, distinguishing between confidential and non-confidential incidents. This dynamic and disaggregated perspective contributes to a deeper understanding of how financial markets internalize cyber risk and how the salience of different types of attacks has evolved in recent years.

The paper is structured as follows. Section 2 reviews the related literature. Section 3 presents the research framework, briefly outlining the event study methodology and the dataset used for our estimations. Section 4 presents and discusses the results, and Section 5 concludes.

2. LITERATURE REVIEW

To quantify the economic consequences of cybersecurity incidents, the academic literature has long employed the event study methodology, which assesses the stock market's reaction to specific announcements. Several early contributions have offered general analyses, without focusing on specific sectors; they consistently found that security breaches tend to generate negative abnormal returns (ARs), especially when involving unauthorized access to confidential data. For instance, Campbell et al. (2003) reported significant market losses following breaches that compromised sensitive information, whereas incidents without data disclosure produced no measurable effects. Similarly, Hovav and D'Arcy (2003) showed that denial-of-service attacks — i.e., attacks that aim to make a machine or network resource unavailable — were particularly detrimental for firms heavily dependent on online operations. Subsequent studies, such as Garg et al. (2003), Cavusoglu et al. (2004), Acquisti et al. (2006), and Gatzlaff and McCullough (2010), confirmed these short-term negative reactions, reinforcing the idea that cybersecurity failures are perceived by investors as adverse informational shocks.

However, evidence across studies remains heterogeneous. Gordon et al. (2011), examining a longer time span, observed a decline in the market's sensitivity to security breaches, possibly due to firms' improved remediation capabilities or investors' greater familiarity with cyber risk. A noteworthy work is Tweneboah-Kodua et al. (2018). Their sample includes about one hundred firms from various industrial sectors that announced cyberattacks between 2013 and 2017; the authors show that cyberattack announcements do not generate significant ARs for the overall sample but sector-level differences matter greatly. Interestingly, financial firms experience clear and significant short-term losses around the event date, while most other sectors show little to no reaction.

The main conclusion of Tweneboah-Kodua et al. (2018) is that aggregating all firms masks meaningful heterogeneity, making sector-specific analysis essential to understanding market responses to cyberattacks[1]. For this reason, in this paper, we focus specifically on financial firms. A contribution of particular relevance in this field is Colivicchi and Vignaroli (2019), who show that financial firms experience larger market losses than companies in other sectors. The authors attribute this heightened vulnerability to a dual challenge: safeguarding vast amounts of confidential customer data while ensuring uninterrupted business continuity.

One paper that is particularly relevant to the present work is Arcuri et al. (2018). While their analysis was not exclusively focused on the financial sector, they devoted specific attention to it. The authors documented, first, that negative cumulative abnormal returns (CARs) emerged before the public disclosure of attacks — suggesting the possibility of insider trading, an outcome that contrasts with standard efficient market predictions. Second, they found that non-confidential incidents, such as funds theft and denial-of-service attacks, generated larger market losses than confidential breaches involving the theft of sensitive data. These findings challenge prevailing intuitions about how markets process cybersecurity information and provide a natural motivation for further empirical scrutiny.

3. RESEARCH METHODOLOGY

3.1. Method

We conduct an event study to measure the effect of cyberattacks on stock returns. The null hypothesis is that the event has no impact on the distribution of returns[2].

An event study requires the calculation of ARs. An *AR* is the actual *ex post* return of the security over the event window, minus the normal return of the firm over the event window. The *AR* of a generic firm *i* in the period *t* is thus defined as:

$$AR_{i,t} = R_{i,t} - E(R_{i,t}|X_t) \quad (1)$$

where, $R_{i,t}$ is the actual ex post return and $E(R_{i,t}|X_t)$ is the expected return conditioned on information X_t from period *t*, unrelated to the event. We follow the approach detailed by MacKinlay (1997) to estimate these ARs and test their significance. In particular, the established list of steps is the following:

1) definition of the event window;

2) computation of the normal returns: a) definition of the estimation window, b) choice of the estimation model;

3) estimation of the ARs;

4) statistical testing for the significance of the ARs.

[1] More recently, Maréchal et al. (2024) questioned the robustness of standard event study findings, showing that once controlling for event-induced variance and cross-sectional correlation, many previously significant results lose statistical strength. These methodological concerns are particularly relevant for cyberattack studies, where events tend to be clustered in time and often affect multiple firms simultaneously.

[2] We perform our event study in Stata using the e-study command. In particular, we follow the guidelines given by Pacicco et al. (2021, 2018).

The event window usually spans one or more days. As it is well known, the choice of the window is crucial and has a decisive influence on the results of the analysis. Windows can include the date of the event or other dates surrounding it (Spanos & Angelis, 2016; El Ghoul et al., 2023); typically, windows are chosen that include days before and after the event to allow for the possibility of news leaks or insider trading (Arcuri et al., 2018; Colivicchi & Vignaroli, 2019). According to Pastorello (2001), the event window should be as small as possible to increase the power of the study while also limiting contamination of the event window returns by other events; for this reason, we opted not to include windows longer than 10 trading sessions[3].

In light of all this, we ultimately chose the following fifteen event windows: (-5, 5), (-3, 3), (-2, 2), (-1, 1), (0, 0), (-5, -1), (-3, -1), (-2, -1), (0, 1), (0, 2), (0, 3), (0, 5), (-1, 2), (-1, 3), (-1, 5). Hence, we consider symmetric windows — i.e., windows of different lengths centered on the event day — and asymmetric windows. The latter category includes windows that are entirely antecedent to the event day, windows that start on the event day, and windows that start on the day prior to the event but end, asymmetrically, after the event. As is typical of event studies on cyberattacks, pre-event windows are analyzed to check whether abnormal price movements occur before the public announcement of the incident. If significant negative returns appear before disclosure, this may indicate information leakage or insider trading, suggesting that some investors had access to the news in advance and acted on it.

We also include the (0, 0) window, i.e., the event day window, as it is common in the cybersecurity event study literature (Chang et al., 2020; Gatzlaff & McCullough, 2010; Acquisti et al., 2006; Cavusoglu et al., 2004; Hovav & D'Arcy, 2004; Garg et al., 2003).

To define an AR, the expected security performance is first needed. This requires an estimation window, meaning a sample period prior to the event window. A buffer of at least one month is often used to exclude market returns that may be influenced by the event, thereby avoiding contamination of normal returns by anticipation effects (Pacicco et al., 2018). Although some estimation windows go as far back as 25 trading days before the event (Chang et al., 2020), we opted for the one used by Arcuri et al. (2018), which corresponds to (-141, -21).

ARs can be estimated using different models. The most common approach (MacKinlay, 1997; Pastorello, 2001; Sorokina et al., 2013) relies on Sharpe's (1963) market model. This method, known as the single index model (SIM), assumes that the return of each security is linearly related to the return of a market index through a single factor. Formally, $AR_{i,t}$ are computed as follows:

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i R_{m,t}) \tag{2}$$

where, $R_{i,t}$ is the observed return of security *i* on day *t*, and $R_{m,t}$ is the corresponding return of the market index on the same day. The term α_i captures the security's average performance independent of market movements, while β_i measures its sensitivity to market returns. The expected (or normal) return of the security, $\alpha_i + \beta_i R_{m,t}$, is, therefore, estimated based on the market return observed in the estimation window. Parameters α_i and β_i are obtained using the ordinary least squares (OLS) method. In our study, the STOXX 600 index is used as the market index. This benchmark consists of 600 securities representing large, midand small-capitalization companies in 17 European countries. It covers approximately 90% of the free-float market capitalization of the European stock market.

Once the expected returns are computed, it is possible to calculate the ARs. When the event window comprises more than one period, which in our case is one day, it becomes necessary to aggregate *AR*s over time, obtaining the *CAR*s:

$$CAR_i(T_2, T_3) = \sum_{t=T_2}^{T_3} AR_{i,t} \tag{3}$$

where, $t \epsilon [T_2, T_3]$ is the event window. When the effect of the event is analyzed on a pool of firms instead of a single firm, cross-sectional aggregation becomes necessary. This involves calculating the average abnormal returns (*AAR*s) as follows:

$$AAR_i = \frac{1}{N} \sum_{i=1}^{N} AR_{i,t} \tag{4}$$

where, $AR_{i,t}$ represents the abnormal return for the *i*-th security and *N* is the number of securities in the sample. Finally, when analyzing the average effect over multiple days, as in our study, both time series and cross-sectional aggregation are required, resulting in the cumulative average abnormal returns (*CAAR*s).

The final step in an event study consists of testing the statistical significance of ARs estimated in the previous stages. In cross-sectional studies, it is common to test the significance of AARs or CAARs rather than ARs at the individual firm level (El Ghoul et al., 2023). The literature generally distinguishes between two main classes of statistical tests: parametric and nonparametric methods (Pacicco et al., 2018).

Parametric tests assume that security returns are normally distributed and independent and identically distributed, with ARs centered around zero and constant variance σ^2. However, these assumptions may not hold in real-world event studies, especially in the presence of event induced volatility and cross-sectional correlation, which can lead to inflated Type I error rates (Ng et al., 2018). To address this issue, Patell (1976) proposed a standardized Z-test, where observations are weighted inversely by their volatility. This improves statistical power but makes the interpretation of scaled ARs less intuitive. As a result, scaled ARs are typically used for significance testing, while raw *AR*s are used for economic interpretation (Kolari & Pynnönen, 2010). Building on Patell's (1976) work, Boehmer et al. (1991) developed the Boehmer, Musumeci, and Poulsen (BMP) test, which adjusts for heteroskedasticity during the event window. However, Kolari and Pynnönen (2010) later showed that even moderate cross-sectional correlation can lead the BMP test to over-reject the null hypothesis. To correct for this, they introduced the adjusted

[3] Additionally, small windows are consistent with the specific findings of Tweneboah-Kodua et al. (2018) on financial firms.

BMP test (ADJ-BMP), which accounts for both cross-sectional correlation and volatility varying over time. We adopt the ADJ-BMP test as our parametric approach due to its robustness in such settings.

Nonetheless, parametric tests are sensitive to violations of normality assumptions. Given that financial return distributions are rarely normal, Pastorello (2001) strongly recommends complementing parametric tests with non-parametric alternatives. Campbell et al. (2010) also highlight their utility in multi-country event studies, such as ours. According to Nguyen and Wolf (2023), when an event study covers a large number of firms or days, the central limit theorem can justify relying on parametric tests alone. However, our study does not include a large number of firms or long event windows, reinforcing the need for a nonparametric robustness check. We, therefore, complement the ADJ-BMP with a nonparametric test proposed by Kolari and Pynnönen (2011): the generalized rank test (GRANK). As the name suggests, this test is suitable for both single-day and CARs. The authors demonstrate that GRANK outperforms traditional rank-based tests (e.g., Wilcoxon) and is robust to serial correlation and volatility clustering. Empirically, GRANK also exhibits superior power compared to several popular parametric methods.

3.2. Data

We define a cyberattack event as the first public disclosure of a firm's security breach in official media outlets. We collected data on security breach events using a combination of two resources: online databases and targeted web searches. Specifically, we used the Timeline of Cyber Incidents Involving Financial Institutions database (https://carnegieendowment.org/features/fincyber-timeline), the Significant Cyber Incidents database (Center for Strategic and International Studies [CSIS], n.d.), and the GDPR Enforcement Tracker (https://www.enforcementtracker.com); data collection — including the identification and coding of security-breach events — was conducted between November 2024 and March 2025. With regard to targeted web searches, we searched for the following keywords: "data breach", "cyberattack", "security breach", "denial of service attack", and "hacker", in combination with "Europe", "European bank", "European financial institution", and "European insurance firm". Through this procedure, we compiled an initial list of events, consisting of successful cyberattacks aimed at European financial firms from 2016 to 2024. We then checked this initial list for events that could not fit in the event study due to: target firm not publicly traded, event date uncertainty, undefinable attack type, or other firm-related events possibly affecting stock returns in the event window.

As for the type of attack, we categorize the events into five types:

- Data breach: unauthorized access, acquisition, or disclosure of sensitive information residing within a system or database.
- Theft: unauthorized appropriation of currency or assets.
- Distributed denial of service (DDoS): disruption of a system or network through excessive traffic that renders it inaccessible.
- Malware: software designed to infiltrate, damage, or compromise computer systems without the user's consent.
- Phishing: a social engineering technique wherein attackers manipulate individuals into divulging sensitive information, such as passwords or financial details.

To classify each cyberattack, we analyzed in detail the descriptions of each event that appeared in online news articles; for details, see Appendix A.

Table 1. Cyber incidents: European financial firms (2016–2024)

Organization	*Event date*	*News Source*	*Attack type*	*Disclosed information*
HSBC Holdings p.l.c.	29/01/2016	The Guardian	DDoS	Non-confidential
National Bank of Belgium	22/02/2016	Politico EU	DDoS	Non-confidential
UniCredit S.p.A.	26/07/2016	Bloomberg	Data breach	Confidential
Tesco p.l.c.	07/11/2016	BBC	Theft	Non-confidential
Lloyds Bank p.l.c.	11/01/2017	The Guardian	DDoS	Non-confidential
ABN AMRO Bank N. V.	29/01/2018	Reuters	DDoS	Non-confidential
ING Bank N. V.	29/01/2018	Reuters	DDoS	Non-confidential
AXA S.A.	23/10/2018	Reuters	Theft	Non-confidential
HSBC Holdings p.l.c.	06/11/2018	BBC	Data breach	Confidential
Bank of Valletta p.l.c.	13/02/2019	Reuters	Theft	Non-confidential
UniCredit S.p.A.	28/10/2019	Il Sole 24 Ore	Data breach	Confidential
Edenred S.E.	21/11/2019	The Brussels Times	Malware	Non-confidential
Banca Monte dei Paschi di Siena S.p.A.	11/04/2020	Reuters	Phishing	Non-confidential
AXA S.A.	16/05/2021	Reuters	Malware	Non-confidential
Deutsche Bank A.G.	04/06/2021	Reuters	DDoS	Non-confidential
Commerzbank A.G.	04/06/2021	Reuters	DDoS	Non-confidential
OP Financial Group	09/01/2022	Daily Finland	Phishing	Non-confidential
Bank of Ireland Group p.l.c.	05/04/2022	RTE	Data breach	Confidential
Banca Monte dei Paschi di Siena S.p.A.	20/06/2022	Il Sole 24 Ore	Data breach	Confidential
Jyske Bank A/S	10/01/2023	Euronews	DDoS	Non-confidential
Sydbank A/S	10/01/2023	Euronews	DDoS	Non-confidential
Ringkjøbing Landbobank A/S	10/01/2023	Euronews	DDoS	Non-confidential
Deutsche Bank A.G.	11/07/2023	Bloomberg	Data breach	Confidential
Commerzbank A.G.	11/07/2023	Bloomberg	Data breach	Confidential
ING Bank N. V.	11/07/2023	Bloomberg	Data breach	Confidential
Intesa Sanpaolo S.p.A.	01/08/2023	La Repubblica	DDoS	Non-confidential
FinecoBank S.p.A.	01/08/2023	La Repubblica	DDoS	Non-confidential
Banca Monte dei Paschi di Siena S.p.A.	01/08/2023	La Repubblica	DDoS	Non-confidential
Banca Popolare di Sondrio S.p.A.	01/08/2023	La Repubblica	DDoS	Non-confidential
Banco Santander S.A.	14/05/2024	Reuters	Data breach	Confidential
ABN AMRO Bank N. V.	23/05/2024	Bloomberg	Data breach	Confidential

As they involve the disclosure of confidential information, data breaches are considered as "confidential" attacks while other types of attacks are considered as "non-confidential" (Arcuri et al., 2018; Campbell et al., 2003). Finally, consistently with previous research (Chang et al., 2020), an announcement containing news of security breaches in multiple companies was counted as announcing multiple events, each related to one of the breached firms.

Based on the above criteria, we identified a total of 31 security incidents; of these, 10 are confidential attacks, and 21 are non-confidential (see Table 1). The number of events puts us at the lower end of sample size in the literature, although still higher than other studies (Hinz et al., 2015; Ko & Dorantes, 2006; Hovav & D'Arcy, 2003). The small sample size is justified by our focus on a very specific set of firms, namely, European financial firms that are publicly traded.

We collected the daily closing prices of the involved companies and the market index (STOXX 600) from Yahoo Finance[4]. We used the adjusted closing prices of the companies for stock splits, dividends, and capital gain distributions, according to the guidelines set by Pastorello (2001), also employed by Furdui and Şfabu (2023), Colivicchi and Vignaroli (2019), and Arcuri et al. (2018).

4. RESEARCH RESULTS AND DISCUSSION

4.1. Market reaction to cyber attacks

Table 2 reports the *CAAR*s for the full sample[5]. Overall, we find a negative and statistically significant market reaction to cyber incident announcements by European financial firms. The effect materializes on the event day, with a CAAR(0, 0) of -0.64%, significant at the 10% level. This result is reassuring, as it aligns with prior evidence[6].

From Table 2, three main findings emerge:

1. All pre-event windows — namely, (-5, -1), (-3, -1), and (-2, -1) — show no significant ARs.

2. Event windows starting on the event day or on the day immediately preceding it — namely, (0, 1), (0, 2), (0, 3), (0, 5) and (-1, 1), (-1, 2), (-1, 3), (-1, 5) — display negative and mostly highly significant CAARs.

3. Windows that symmetrically include days both before and after the event — namely, (-5, 5), (-3, 3), and (-2, 2) — also exhibit negative and, to varying degrees, significant CAARs. However, when compared with windows that end on the same day but start on the event day — i.e., (0, 2), (0, 3), (0, 5) — their CAARs are smaller in absolute value.

Table 2. Event study results for the full sample of cyber incidents

Event window	*CAAR*	*KP*	*GRANK*
(-5, 5)	-1.4359%	**	**
(-3, 3)	-1.3845%	**	**
(-2, 2)	-1.0099%	*	*
(-1, 1)	-0.8199%	*	*
(0, 0)	-0.6414%	*	*
(-5, -1)	0.9354%		
(-3, -1)	0.3828%		
(-2, -1)	0.4086%		
(0, 1)	-0.7675%	**	*
(0, 2)	-1.4186%	***	***
(0, 3)	-1.7673%	***	***
(0, 5)	-2.3713%	***	***
(-1, 2)	-1.4709%	***	***
(-1, 3)	-1.8197%	***	***
(-1, 5)	-2.4237%	***	***

*Note: KP = Kolari-Pynnönen ADJ-BMP test. Significance levels: * p < 0.10, ** p < 0.05, *** p < 0.01.*

Finding 1 is particularly interesting. Analyzing returns prior to the announcement is crucial, as it helps detect potential insider trading. Abnormal price movements in these windows are typically interpreted as evidence of information leakages that allow some investors to trade ahead of the public disclosure. The evidence found here, therefore, supports the absence of insider trading.

Note that the presence of negative and significant CAARs in windows that include days prior to the event, such as (-5, 5) or (-3, 3) (finding 3), does not contradict this result. In fact, the ARs estimated for these windows are smaller in magnitude than those observed in the corresponding post-event windows. For example, the CAAR equals -1.4359% for the (-5, 5) window and -2.3713% for the (0, 5) window, indicating that the effect observed in (-5, 5) is entirely driven by the days immediately following the event. The lower magnitude simply reflects a dilution effect resulting from the need to AARs over a larger number of days.

This result stands in sharp contrast to other studies, such as Colivicchi and Vignaroli (2019) and Arcuri et al. (2018), which, unlike ours, find evidence of insider trading. Several factors may account for this divergence. One possible explanation concerns the geographical scope: while our analysis focuses exclusively on European financial firms, Arcuri et al. (2018) and Colivicchi and Vignaroli (2019) examine a broader and more heterogeneous global sample. Regulatory differences may also play a role: within the European Union, stricter transparency and market abuse regulations may reduce the likelihood of information leakages prior to public announcements. Finally, variations in sample period, data coverage, or event classification criteria could also contribute to the discrepancy.

The second key finding concerns the windows that start on or immediately before the event day. These windows display the largest (in absolute value) and most statistically significant CAARs, highlighting a pronounced negative impact of the event on firms' share prices. It should also be noted that the impact becomes increasingly negative as the window extends further into the post-event period. This pattern is consistent with previous studies showing that firm value continues to decline in the days following the disclosure (Chang et al., 2020; Gatzlaff & McCullough, 2010; Acquisti et al., 2006; Cavusoglu et al., 2004; Garg et al., 2003). Again,

[4] https://finance.yahoo.com
[5] Firm-level CARs are reported in Appendix B.
[6] Our estimate is consistent with Chang et al. (2020), Gatzlaff and McCullough (2010), and Acquisti et al. (2006), who report CAAR(0, 0) values of -0.23%, -0.57%, and -0.41%, respectively. Differences may reflect geographical, sectoral, or macroeconomic factors, as well as the greater sensitivity of listed financial firms to cyberattack disclosures relative to firms in the broader economy (Colivicchi & Vignaroli, 2019; Arcuri et al., 2018). Cavusoglu et al. (2004) and Garg et al. (2003) also document larger negative reactions (-0.86% and -2.70%, respectively), possibly because their data were collected during the Dot-com bubble.

the fact that windows starting just one day before the event also yield negative and significant CAARs does not support the insider trading hypothesis. In these cases — specifically, (-1, 1), (-1, 2), (-1, 3), and (-1, 5) — the estimated CAARs are almost identical to those obtained when the event day is used as the starting point [e.g., (-1, 1) vs. (0, 1) or (-1, 2) vs. (0, 2)]. Hence, the negative impact is entirely driven by the market's reaction to the disclosure rather than by pre-announcement trading activity.

With the aim of gaining a deeper understanding of the impact of cyberattacks on firms' stock prices, we repeated our estimations by distinguishing between confidential attacks, i.e., those involving unauthorized disclosure of sensitive or proprietary information, and non-confidential attacks, that is, those aimed at compromising the availability or operational continuity of systems and services. The results are reported in Table 3.

Table 3. Event study results on the confidentiality of the incident

Event window	*Non-confidential*			*Confidential*		
	CAAR	*KP*	*GRANK*	*CAAR*	*KP*	*GRANK*
(-5, 5)	-2.5844%	***	***	-0.9535%		
(-3, 3)	-1.9284%	**	**	-0.2551%		
(-2, 2)	-0.9590%			-1.1241%		
(-1, 1)	-0.5246%			-1.4454%	*	*
(0, 0)	-0.6955%	*	**	-0.5283%		
(-5, -1)	0.4982%			1.8460%		
(-3, -1)	0.0569%			1.0650%		
(-2, -1)	0.3525%			0.5266%		
(0, 1)	-0.4267%			-1.4886%		*
(0, 2)	-1.3115%	**	***	-1.6506%	*	
(0, 3)	-1.9853%	***	***	-1.3201%		
(0, 5)	-3.0826%	***	***	-0.8925%		
(-1, 2)	-1.4093%	**	*	-1.6074%	*	*
(-1, 3)	-2.0832%	***	***	-1.2769%		
(-1, 5)	-3.1805%	***	***	-0.8493%		

*Note: Significance levels: * p < 0.10, ** p < 0.05, *** p < 0.01.*

A first takeaway from Table 3 is that, even after distinguishing between the two types of attacks, the CAARs in the pre-event windows remain statistically insignificant for both categories. This result further reinforces the evidence against the presence of insider trading. Looking at the estimated CAARs across the remaining event windows, Table 3 reveals that confidential incidents do not appear to exert a statistically significant impact on firms' stock prices, except in a very limited number of windows and only marginally so. By contrast, non-confidential attacks exhibit substantially stronger and more pervasive effects across almost all event windows considered, and — consistent with the earlier discussion — these effects are particularly pronounced in post-event windows or in those starting immediately before the announcement day. This finding corroborates the evidence reported by Arcuri et al. (2018), while contrasting with the results of Campbell et al. (2003) and other earlier studies that identified confidentiality breaches as the main source of valuation losses.

4.2. Time trend in stock market reactions

An important question is whether the stock market's reaction to cyberattacks has changed over time. On the one hand, financial institutions may have learned to mitigate the effects of such events through improved defense mechanisms, disclosure practices, and investor communication. In this case, one would expect the negative ARs associated with cyberattacks to diminish over time. On the other hand, hackers may have become more sophisticated in selecting targets and refining their methods, potentially leading to stronger market penalties. Determining which of these forces dominates is an empirical matter.

In our event study, CAAR(-1, 5) and CAAR(0, 5) have emerged as the most robust indicators of the negative impact of cyberattacks; in order to ascertain whether there is a time trend, we focus on the firm-level CAARs reported in Appendix B. We construct the variable $Days_i$Daysi, defined as the number of days between event i and the first event in our sample (January 29, 2016), and estimate three different models with progressively richer specifications.

The baseline specification (Model 1) for testing for a time trend is:

$$CAAR_i = \alpha + \beta_1 Days_i + \varepsilon_i \quad (5)$$

where, $CAAR_i$ is the estimated cumulative abnormal return of event *i*; this specification tests for a simple linear trend in the impact of breaches over time. In order to verify any differences in the time trend between confidential and non-confidential attacks, in a second specification (Model 2), we include a dummy variable identifying attacks involving confidential information:

$$CAAR_i = \alpha + \beta_1 Days_i + \beta_2 Conf_i + \varepsilon_i \quad (6)$$

where, $Conf_i$ = 1 if the attack involved the release of sensitive or proprietary information.

Finally, to allow for heterogeneous time patterns, we add the interaction between $Days_i$ and the dummy identifying a confidential attack (Model 3):

$$CAAR_i = \alpha + \beta_1 Days_i + \beta_2 Conf_i + \beta_3 (Days_i \times Conf_i) + \varepsilon_i \quad (7)$$

In this specification, β_1 measures the time trend for non-confidential events, β_2 is the level difference between confidential and non-confidential events at the beginning of the sample, and β_3 captures whether the trend differs for confidential attacks. Hence, the effective slope for confidential events is given by $\beta_1 + \beta_3$.

Table 4. Time trend regressions for alternative event windows

Model	CAAR(1, 5)			CAAR(0, 5)		
	(1) Linear	(2) + Dummy	(3) + Interaction	(1) Linear	(2) + Dummy	(3) + Interaction
Days	-0.0004 (0.559)	-0.0007 (0.280)	-0.0019** (0.012)	-0.0003 (0.652)	-0.0006 (0.358)	-0.0017** (0.025)
Conf	—	2.77 (0.059)	-4.95* (0.094)	—	2.56* (0.072)	-4.39 (0.132)
Days × Conf	—	—	0.0039*** (0.006)	—	—	0.0035*** (0.011)
Intercept	-1.83 (0.199)	-2.12 (0.124)	-0.20 (0.881)	-1.96 (0.156)	-2.22* (0.098)	-0.50 (0.711)
R^2	0.02	0.07	0.35	0.01	0.12	0.31
Observations	31	31	31	31	31	31

*Note: p-values in parentheses. Significance levels: * p < 0.10, ** p < 0.05, *** p < 0.01.*

Table 4 reports the results for both event windows. As expected, the patterns are remarkably similar across the two, further confirming that pre-event trading activity does not influence the outcome. In Models 1 and 2, the estimated coefficient on *Days* is small and statistically insignificant, indicating no evidence of a systematic time trend in the overall market reaction to cyberattacks. For the dummy variable identifying confidential breaches (the dummy *Conf* in Model 2), the coefficient is weakly positive but remains statistically insignificant in the (-1, 5) window and only marginally significant in the (0, 5) window. Overall, Models 1 and 2 display very limited explanatory power, as reflected in the low R^2 values, suggesting that neither specification captures a meaningful temporal pattern in the data.

The introduction of the interaction term in Model 3 substantially improves model fit; interestingly, the estimation of this specification offers a novel interpretation. For both event windows, the coefficient on *Days* becomes negative and significant at the 5% level, implying that the negative impact on firms' values of non-confidential cyberattacks has intensified over time. Conversely, the positive and highly significant coefficient on the interaction term *Days* × *Conf* indicates an opposite trend for confidential breaches. The magnitude of the estimated coefficient on the interaction term is large enough to offset that on *Days*, resulting in an effective positive slope for confidential events (that is: $\beta_1 + \beta_3 > 0$). In other words, while non-confidential attacks have become increasingly damaging, the market response to confidential breaches has progressively weakened. This evidence is perfectly in line with what was discussed in the previous section, which shows that, overall and without considering any dynamic effects, confidential events do not have a significant impact on returns. The explanatory power of Model 3 has increased substantially: the R^2 value rises from approximately 0.02 in the baseline model to 0.35 and 0.31, respectively, for the (-1, 5) and (0, 5) windows.

Overall, the dynamics of CAAR(-1, 5) and CAAR(0, 5) point to a consistent pattern. The market has not become uniformly more or less sensitive to cyberattacks over time; instead, our evidence supports a process of selective learning and adaptation. Investors and firms appear to have become more resilient to breaches involving confidential information — perhaps due to improved disclosure and incident-management practices — while reactions to other forms of cyberattacks remain persistently negative or even worsening.

Our findings echo evidence in the literature that breach impacts have moderated over time (Gordon et al., 2011; McShane & Nguyen, 2020) but also align with studies that highlight continuing or even growing investor sensitivity to severe incidents (Arcuri et al., 2018; Akyildirim et al., 2024). However, given the relatively small sample size, our evidence should be interpreted as preliminary and calls for further, more in-depth investigation.

5. CONCLUSION

This paper investigates the stock market effects of cyberattacks targeting European financial institutions between 2016 and 2024, offering updated empirical evidence on the interaction between cybersecurity risk, disclosure, and market discipline in a sector of critical systemic relevance. The results show that the negative market reaction to cyber incidents is concentrated around the announcement day and the immediately following sessions, with no evidence of pre-announcement declines. This finding suggests that recent improvements in regulatory disclosure frameworks and corporate transparency may have reduced information asymmetries and limited the scope for insider trading.

When distinguishing between confidential and non-confidential incidents, our analysis confirms previous findings in the literature pointing to a systematic difference in market reactions for the two. In particular, evidence suggests that non-confidential incidents have a consistently stronger negative effect on market valuations.

The most innovative contribution of this study lies in the exploration of how market reactions to cyberattacks have evolved over time. In a simple yet informative time-trend analysis, we find preliminary evidence of diverging dynamics: while the impact of non-confidential attacks appears to have intensified in recent years, the negative effect of confidential breaches has weakened. Again, this is a further confirmation of the difference in the impact on returns between the two types of attacks. These patterns may reflect both improvements in firms' ability to manage and communicate data-related incidents and the increasing operational disruption

potential of attacks targeting business continuity, especially for financial firms. However, these findings should be interpreted with caution, given the relatively small number of identified events (31 incidents), which limits statistical power and constrains granular inference. Expanding the dataset by broadening the spectrum of cyber events considered would enable more robust tests of the time-trend patterns documented in this paper.

Future research should examine in greater depth how governance structures, regulatory environments, and institutional characteristics shape firms' exposure and market responses to cyber threats. Expanding the dataset, refining the typology of attacks, and exploring firm-level governance features would provide valuable insights into the mechanisms linking cyber risk, governance quality, and financial performance.

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *ICIS 2006 Proceedings*. Association for Information Systems (AIS). https://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Akyildirim, E., Conlon, T., Corbet, S., & Hou, Y. (2024). HACKED: Understanding the stock market response to cyberattacks. *Journal of International Financial Markets, Institutions and Money*, *97*, Article 102082. https://doi.org/10.1016/j.intfin.2024.102082

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership & Control, 15*(2), 70–83. https://doi.org/10.22495/cocv15i2art6

Boehmer, E., Masumeci, J., & Poulsen, A. B. (1991). Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics, 30*(2), 253–272. https://doi.org/10.1016/0304-405X(91)90032-F

Campbell, C. J., Cowan, A. R., & Salotti, V. (2010). Multi-country event study methods. *Journal of Banking & Finance, 34*(12), 3078–3090. https://doi.org/10.1016/j.jbankfin.2010.07.016

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

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

Center for Strategic and International Studies (CSIS). (n.d.). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chang, K.-C., Gao, Y.-K., & Lee, S.-C. (2020). The effect of data theft on a firm's short-term and long-term market value. *Mathematics*, *8*(5), Article 808. https://doi.org/10.3390/math8050808

Colivicchi, I., & Vignaroli, R. (2019). Forecasting the impact of information security breaches on stock market returns and VaR backtest. *Journal of Mathematical Finance*, *9*, 402–454. https://doi.org/10.4236/jmf.2019.93024

Council of the European Union. (2025, June 30). *Cyber threats in the EU: Facts and figures*. https://www.consilium.europa.eu/en/policies/top-cyber-threats/

El Ghoul, S., Guedhami, O., Mansi, S. A., & Sy, O. (2023). Event studies in international finance research. *Journal of International Business Studies*, *54*(2), 344–364. https://doi.org/10.1057/s41267-022-00534-6

Furdui, C., & Şfabu, D. T. (2023). The European banks under the shock of the Russian invasion of 2022: An event study approach. *Studia Universitatis Babes-Bolyai*, *68*(1), 62–77. https://doi.org/10.2478/subboec-2023-0004

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74–83. https://doi.org/10.1108/09685220310468646

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

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

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), 337–347. https://doi.org/10.1016/j.im.2014.12.006

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121. https://doi.org/10.1046/J.1098-1616.2003.026.x

Hovav, A., & D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. *Information Systems Security, 13*(3), 32–40. https://doi.org/10.1201/1086/44530.13.3.20040701/83067.5

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

Kolari, J. W., & Pynnönen, S. (2010). Event study testing with cross-sectional correlation of abnormal returns. *The Review of Financial Studies*, *23*(11), 3996–4025. https://doi.org/10.1093/rfs/hhq072

Kolari, J. W., & Pynnönen, S. (2011). Nonparametric rank tests for event studies. *Journal of Empirical Finance, 18*(5), 953–971. https://doi.org/10.1016/j.jempfin.2011.08.003

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

Maréchal, L., Celeny, D., Rousselot, E., Mermoud, A., & Humbert, M. (2024). *Reassessing the market impact of cyber incidents: A bias-adjusted event study approach*. https://doi.org/10.2139/ssrn.4717020

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *The Geneva Papers on Risk and Insurance — Issues and Practice, 45*, 580–615. https://doi.org/10.1057/s41288-020-00170-x

Ng, C.-P., Choo, W.-C., Bany-Ariffin, A. N., & Annuar, M. N. (2018). Contemporary event study test: Event-induced variance and cross correlation among abnormal returns in dividend. *International Journal of Economics and Management*, *12*(S2), 327–337. http://www.ijem.upm.edu.my/vol12_noS2/2)%20Contemporary%20Event%20Study%20Test.pdf

Nguyen, P. A., & Wolf, M. (2023). *A note on testing AR and CAR for event studies* (Working Paper No. 425). University of Zurich. https://www.econstor.eu/bitstream/10419/268859/1/1837159122.pdf

Pacicco, F., Vena, L., & Venegoni, A. (2018). Event study estimations using Stata: The estudy command. *The Stata Journal: Promoting Communications on Statistics and Stata*, *18*(2), 461–476. https://doi.org/10.1177/1536867X1801800211

Pacicco, F., Vena, L., and Venegoni, A. (2021). From common to firm-specific event dates: A new version of the estudy command. *The Stata Journal: Promoting Communications on Statistics and Stata*, *21*(1), 141–151. https://doi.org/10.1177/1536867X211000010

Pastorello, S. (2001). *Rischio e rendimento. Teoria finanziaria e applicazioni econometriche* [Risk and return. Financial theory and econometric applications]. Il Mulino.

Patell, J. M. (1976). Corporate forecasts of earnings per share and stock price behavior: Empirical test. *Journal of Accounting Research*, *14*(2), 246–276. https://doi.org/10.2307/2490543

Sharpe, W. F. (1963). A simplified model for portfolio analysis. *Management Science*, *9*(2), 277–293. https://doi.org/10.1287/mnsc.9.2.277

Sorokina, N., Booth, D. E., & Thornton, J. H. (2013). Robust methods in event studies: Empirical evidence and theoretical implications. *Journal of Data Science*, *11*(3), 575–606. https://doi.org/10.6339/JDS.2013.11(3).1166

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

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

APPENDIX A. DETAILED NEWS ARTICLES BY EVENT

Organization	*Announcement date*	*Online news article*
HSBC Holdings p.l.c.	29/01/2016	https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack
National Bank of Belgium	22/02/2016	https://www.politico.eu/article/belgium-government-agencies-plagued-hackers-downsec-ddos-attacks-cyber-crime/
UniCredit S.p.A.	26/07/2016	https://www.bloomberg.com/news/articles/2017-07-26/unicredit-says-400-000-clients-affected-by-security-breach#xj4y7vzkg
Tesco p.l.c.	07/11/2016	https://www.bbc.com/news/technology-37896273
Lloyds Bank p.l.c.	11/01/2017	https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack
ABN AMRO Bank N.V.	29/01/2018	https://www.reuters.com/article/us-netherlands-cyber/dutch-tax-office-banks-hit-by-ddos-cyber-attacks-idUSKBN1FI1LM/
ING Bank N.V.	29/01/2018	https://www.reuters.com/article/us-netherlands-cyber/dutch-tax-office-banks-hit-by-ddos-cyber-attacks-idUSKBN1FI1LM/
AXA S.A.	23/10/2018	https://www.reuters.com/article/mexico-centralbank-incident-idUSL2N1X403Z/
HSBC Holdings p.l.c.	06/11/2018	https://www.bbc.com/news/technology-46117963
Bank of Valletta p.l.c.	13/02/2019	https://www.reuters.com/article/us-bank-valetta-cyber/cyber-attack-on-malta-bank-tried-to-transfer-cash-abroad-idUSKCN1Q21KZ/
UniCredit S.p.A.	28/10/2019	https://www.ilsole24ore.com/art/unicredit-violati-dati-3-milioni-clienti-non-erano-sensibili-ACoTY0u
Edenred S.E.	21/11/2019	https://www.brusselstimes.com/80147/meal-voucher-provider-edenred-hit-by-malware-attack
Banca Monte dei Paschi di Siena S.p.A.	11/04/2020	https://www.reuters.com/article/us-monte-dei-paschi-italy-bank-hacker-id USKCN21T0H6/
AXA S.A.	16/05/2021	https://www.reuters.com/business/axa-division-asia-hit-by-ransomware-cyber-attack-2021-05-16/
Deutsche Bank A.G.	04/06/2021	https://www.reuters.com/technology/german-it-company-that-serves-banks-experiences-ddos-hack-attack-2021-06-04/
Commerzbank A.G	04/06/2021	https://www.reuters.com/technology/german-it-company-that-serves-banks-experiences-ddos-hack-attack-2021-06-04/
OP Financial Group	09/01/2022	https://www.dailyfinland.fi/business/25316/OP-online-banking-comes-under-cyber-attack
Bank of Ireland Group p.l.c.	05/04/2022	https://www.rte.ie/news/business/2022/0405/1290503-bank-of-ireland-fined-by-dpc/
Banca Monte dei Paschi di Siena S.p.A.	20/06/2022	https://www.ilsole24ore.com/art/attacco-informatico-danni-mps-trafugati-indirizzi-email-AE2XmAhB
Jyske Bank A/S	10/01/2023	https://www.euronews.com/next/2023/01/10/denmark-cenbank-cybersecurity
Sydbank A/S	10/01/2023	https://www.euronews.com/next/2023/01/10/denmark-cenbank-cybersecurity
Ringkjøbing Landbobank A/S	10/01/2023	https://www.euronews.com/next/2023/01/10/denmark-cenbank-cybersecurity
Deutsche Bank A.G.	11/07/2023	https://www.bloomberg.com/news/articles/2023-07-11/deutsche-bank-commerzbank-ing-data-breached-in-moveit-hack
Commerzbank A.G.	11/07/2023	https://www.bloomberg.com/news/articles/2023-07-11/deutsche-bank-commerzbank-ing-data-breached-in-moveit-hack
ING Bank N.V.	11/07/2023	https://www.bloomberg.com/news/articles/2023-07-11/deutsche-bank-commerzbank-ing-data-breached-in-moveit-hack
Intesa Sanpaolo S.p.A.	01/08/2023	https://www.repubblica.it/economia/2023/08/01/news/hacker_russi_attaccano_5_banche_italiane_lagenzia_cybersicurezza_massima_allerta_sistemi_integri-409730144/
FinecoBank S.p.A.	01/08/2023	https://www.repubblica.it/economia/2023/08/01/news/hacker_russi_attaccano_5_banche_italiane_lagenzia_cybersicurezza_massima_allerta_sistemi_integri-409730144/
Banca Monte dei Paschi di Siena S.p.A.	01/08/2023	https://www.repubblica.it/economia/2023/08/01/news/hacker_russi_attaccano_5_banche_italiane_lagenzia_cybersicurezza_massima_allerta_sistemi_integri-409730144/
Banca Popolare di Sondrio S.p.A.	01/08/2023	https://www.repubblica.it/economia/2023/08/01/news/hacker_russi_attaccano_5_banche_italiane_lagenzia_cybersicurezza_massima_allerta_sistemi_integri-409730144/
Banco Santander S.A.	14/05/2024	https://www.reuters.com/technology/cybersecurity/santander-reports-customer-employee-data-breach-spain-chile-uruguay-2024-05-14/
ABN AMRO Bank N.V.	23/05/2024	https://www.bloomberg.com/news/articles/2024-05-24/abn-amro-is-latest-bank-to-suffer-breach-after-hack-at-supplier

APPENDIX B. FIRM-LEVEL CARS

Event date	*Organization*	*CAAR(-5, 5)*	*CAAR(-3, 3)*	*CAAR(-2, 2)*	*CAAR(-1, 1)*	*CAAR(0, 0)*	*CAAR(-5, -1)*	*CAAR(-3, -1)*	*CAAR(-2, -1)*	*CAAR(0, 1)*	*CAAR(0, 2)*	*CAAR(0, 3)*	*CAAR(0, 5)*	*CAAR(-1, 2)*	*CAAR(-1, 3)*	*CAAR(-1, 5)*
29/01/2016	HSBC Holdings p.l.c.	-2.1563%	-3.2833%	-0.1885%	0.5024%	0.9568%	-0.4735%	1.2636%	1.8639%	-0.4805%	-2.0524%	-4.5470%	-1.6828%	-1.0694%	-3.5641%	-0.6998%
22/02/2016	National Bank of Belgium	1.1294%	-3.6068%	-1.2728%	0.7717%	-0.8982%	-0.9661%	-2.5428%	-0.9913%	0.2639%	-0.2815%	-1.0640%	2.0956%	0.2262%	-0.5562%	2.6033%
26/07/2016	UniCredit S.p.A.	-3.7247%	-0.1062%	-7.4163%	-6.3284%	-2.0400%	4.1468%	3.1892%	0.4518%	-6.7480%	-7.8682%	-3.2954%	-7.8715%	-7.4485%	-2.8758%	-7.4519%
07/11/2016	Tesco p.l.c.	-4.9371%	-8.4184%	-7.7736%	-5.6285%	-2.8467%	-3.0178%	-3.3519%	-2.5868%	-2.7817%	-5.1867%	-5.0665%	-1.9192%	-8.0335%	-7.9133%	-4.7660%
11/01/2017	Lloyds Bank p.l.c.	2.7933%	1.7336%	0.3265%	1.9689%	-0.6717%	4.0523%	3.8408%	1.7745%	0.0186%	-1.4480%	-2.1071%	-1.2589%	0.5022%	-0.1568%	0.6913%
29/01/2018	ABN AMRO Bank N.V.	-1.1919%	0.4505%	0.7560%	-0.0201%	0.4842%	-1.6038%	-0.1991%	0.6663%	0.0209%	0.0896%	0.6497%	0.4118%	0.0486%	0.6086%	0.3707%
29/01/2018	ING Bank N.V.	-1.5063%	-2.4822%	-1.3394%	-0.6739%	0.6371%	-1.2430%	-0.3635%	0.1339%	-0.1195%	-1.4734%	-2.1186%	-0.2632%	-2.0278%	-2.6730%	-0.8176%
23/10/2018	AXA S.A.	-2.8104%	-1.2079%	-1.0749%	-0.2546%	-0.2647%	-0.9535%	0.4807%	-0.0616%	-1.0266%	-1.0133%	-1.6887%	-1.8568%	-0.2413%	-0.9167%	-1.0848%
06/11/2018	HSBC Holdings p.l.c.	-0.2451%	-2.5642%	-0.0028%	-1.7296%	-0.3368%	-0.7461%	-1.0243%	0.2606%	-1.0723%	-0.2634%	-1.5399%	0.5010%	-0.9207%	-2.1972%	-0.1562%
13/02/2019	Bank of Valletta p.l.c.	0.6608%	0.5842%	0.9076%	-0.7575%	-0.4201%	1.1697%	0.8895%	1.5057%	-1.0894%	-0.5980%	-0.3052%	-0.5089%	-0.2661%	0.0266%	-0.1770%
28/10/2019	UniCredit S.p.A.	0.2507%	-2.7714%	-2.0656%	0.8117%	0.2477%	-0.8722%	-1.9201%	-1.6782%	1.5195%	-0.3874%	-0.8513%	1.1229%	-1.0952%	-1.5591%	0.4151%
21/11/2019	Edenred S.E.	-2.8848%	-3.8216%	-3.5642%	-0.9915%	-0.8632%	2.2920%	1.5443%	1.7289%	-2.2506%	-5.2932%	-5.3660%	-5.1769%	-4.0342%	-4.1069%	-3.9178%
11/04/2020	Banca Monte dei Paschi di Siena S.p.A.	-10.0697%	-11.4774%	-7.6975%	-5.8592%	-1.9723%	-3.9321%	-3.0347%	-1.1952%	-4.8856%	-6.5022%	-8.4427%	-6.1376%	-7.4757%	-9.4162%	-7.1111%
16/05/2021	AXA S.A.	-2.2743%	-3.5742%	-1.9352%	-1.7183%	-0.3211%	0.7365%	-1.0231%	-1.0004%	-1.4518%	-0.9347%	-2.5510%	-3.0109%	-1.2012%	-2.8175%	-3.2774%
04/06/2021	Deutsche Bank A.G.	-9.9330%	-6.0763%	-3.0839%	-1.5144%	-1.0691%	-0.5766%	-0.7635%	-0.1274%	-1.6957%	-2.9564%	-5.3127%	-9.3563%	-2.7751%	-5.1314%	-9.1750%
04/06/2021	Commerzbank A.G.	-4.8260%	-1.8488%	-0.6930%	-0.6425%	-1.6413%	2.0815%	2.6303%	2.2019%	-1.4727%	-2.8949%	-4.4792%	-6.9075%	-2.0647%	-3.6490%	-6.0773%
09/01/2022	OP Financial Group	0.5002%	-1.2374%	-0.1747%	-1.4788%	0.6520%	5.3744%	1.0218%	1.8143%	-1.5651%	-1.9890%	-2.2593%	-4.8741%	-1.9027%	-2.1731%	-4.7879%
05/04/2022	Bank of Ireland Group p.l.c.	1.7228%	-3.1810%	-3.2851%	-2.9520%	-5.1496%	-0.4023%	-0.4914%	0.2776%	-2.9671%	-3.5628%	-2.6895%	2.1252%	-3.5477%	-2.6744%	2.1403%
20/06/2022	Banca Monte dei Paschi di Siena S.p.A.	-8.3067%	-3.3578%	-0.9538%	-1.9832%	-1.0076%	1.4777%	1.1435%	1.5726%	-1.8363%	-2.5265%	-4.5014%	-9.7845%	-2.6734%	-4.6483%	-9.9314%
10/01/2023	Jyske Bank A/S	-2.3837%	-0.8663%	-1.4943%	0.3553%	-0.3793%	-0.6201%	-0.8142%	-3.4291%	2.6279%	1.9347%	-0.0521%	-1.7635%	-0.3377%	-2.3246%	-4.0361%
10/01/2023	Sydbank A/S	-2.0549%	-2.0694%	-4.0101%	-1.5042%	0.7950%	0.5478%	0.1376%	-2.3456%	1.3475%	-1.6645%	-2.2070%	-2.6027%	-4.5163%	-5.0588%	-5.4545%
10/01/2023	Ringkjøbing Landbobank A/S	-3.0224%	-1.6315%	-2.1834%	-1.1125%	-0.5135%	0.1188%	0.2574%	-1.6951%	0.5087%	-0.4883%	-1.8889%	-3.1413%	-2.1096%	-3.5102%	-4.7626%
11/07/2023	Deutsche Bank A.G.	8.4457%	6.2926%	4.6116%	0.6632%	2.0698%	8.2154%	6.9199%	3.7793%	-0.7958%	0.8323%	-0.6273%	0.2302%	2.2914%	0.8317%	1.6893%
11/07/2023	Commerzbank A.G.	2.9232%	0.7541%	0.1729%	-2.3966%	-0.7063%	2.4720%	3.4882%	3.4007%	-3.7612%	-3.2277%	-2.7341%	0.4511%	-1.8632%	-1.3696%	1.8156%
11/07/2023	ING Bank N.V.	4.0137%	2.0575%	0.9196%	-0.0505%	1.7003%	2.5225%	1.8076%	0.1850%	0.8927%	0.7345%	0.2499%	1.4912%	-0.2086%	-0.6933%	0.5479%
01/08/2023	Intesa Sanpaolo S.p.A.	-0.2138%	-0.7000%	1.1102%	1.8274%	-3.4673%	0.3018%	-2.3533%	1.5932%	0.9081%	-0.4830%	1.6532%	-0.5157%	0.4362%	2.5725%	0.4035%
01/08/2023	FinecoBank S.p.A.	-6.4127%	2.9484%	3.8674%	1.0932%	-1.3634%	1.1857%	0.5391%	1.8526%	1.1097%	2.0147%	2.4093%	-7.5985%	1.9982%	2.3928%	-7.6150%
01/08/2023	Banca Monte dei Paschi di Siena S.p.A.	-6.3636%	1.8612%	3.2410%	1.3332%	-0.8210%	1.4606%	1.3799%	2.1720%	0.8281%	1.0689%	0.4812%	-7.8243%	1.5741%	0.9863%	-7.3191%
01/08/2023	Banca Popolare di Sondrio S.p.A.	-0.0177%	2.9766%	5.2682%	2.6523%	-0.7460%	3.5322%	1.1164%	3.2448%	1.7641%	2.0234%	1.8601%	-3.5500%	2.9116%	2.7483%	-2.6618%
14/05/2024	Banco Santander S.A.	1.6933%	-0.2482%	-1.1532%	0.5385%	-0.3105%	0.7963%	-1.6787%	-1.3518%	0.1927%	0.1986%	1.4304%	0.8970%	0.5443%	1.7762%	1.2428%
23/05/2024	ABN AMRO Bank N.V.	1.2614%	-0.2385%	-2.6106%	-1.4378%	0.0683%	0.2471%	-1.0060%	-1.7518%	-0.6875%	-0.8587%	0.7675%	1.0142%	-1.6091%	0.0171%	0.2638%