Kammoun, Niaz; Bounfour, Ahmed; Özaygen, Altay; Dieye, Rokhaya

Article

Financial market reaction to cyberattacks

Cogent Economics & Finance

Provided in Cooperation with:
Taylor & Francis Group

Suggested Citation: Kammoun, Niaz; Bounfour, Ahmed; Özaygen, Altay; Dieye, Rokhaya (2019) : Financial market reaction to cyberattacks, Cogent Economics & Finance, ISSN 2332-2039, Taylor & Francis, Abingdon, Vol. 7, Iss. 1, pp. 1-20, https://doi.org/10.1080/23322039.2019.1645584

This Version is available at:
https://hdl.handle.net/10419/270671

Cogent Economics & Finance

ISSN: (Print) 2332-2039 (Online) Journal homepage: https://www.tandfonline.com/loi/oaef20

Financial market reaction to cyberattacks

Niaz Kammoun, Ahmed Bounfour, Altay Özaygen & Rokhaya Dieye |

To cite this article: Niaz Kammoun, Ahmed Bounfour, Altay Özaygen & Rokhaya Dieye | (2019) Financial market reaction to cyberattacks, Cogent Economics & Finance, 7:1, 1645584, DOI: 10.1080/23322039.2019.1645584

To link to this article: https://doi.org/10.1080/23322039.2019.1645584

Published online: 13 Aug 2019.

FINANCIAL ECONOMICS | RESEARCH ARTICLE

Financial market reaction to cyberattacks

Niaz Kammoun, Ahmed Bounfour, Altay Özaygen and Rokhaya Dieye

Cogent Economics & Finance (2019), 7: 1645584

cogent economics & finance

FINANCIAL ECONOMICS | RESEARCH ARTICLE

Financial market reaction to cyberattacks

Niaz Kammoun[1], Ahmed Bounfour[1]*, Altay Özaygen[1] and Rokhaya Dieye[1]

Abstract: Drawing upon an extensive dataset comprising 3,680 cyberattacks on firms listed in 5 stock markets, our main objective is to ascertain the financial market reaction based on a hybrid valuation inspired by the event study methodology and a counterfactual analysis. Analyses concern three dates that are specific to cyberattacks: 1) the accident date; 2) the first notice date; and 3) the original loss start date. Results indicate that there is a negative abnormal return for the NASDAQ after the accident date. The reactions of the NASDAQ and NYSE are similar, and negative for the first notice date but positive after the original loss start date. In the European context, cumulative abnormal returns are negative for French and German companies after the first notice date.

Received: 17 January 2019
Accepted: 14 July 2019
First Published: 26 July 2019

*Corresponding author: Ahmed Bounfour Laboratoire RITM, Université Paris Sud, Université Paris-Saclay, Faculté Jean Monnet 54, bd Desgranges, Sceaux 92330, France
Email: ahmed.bounfour@u-psud.fr

Reviewing editor:
David McMillan, University of Stirling, Stirling, UK

Additional information is available at the end of the article

Ahmed Bounfour

ABOUT THE AUTHORS

Niaz Kammoun is a researcher and assistant professor in management science. His research spans several fields; innovation, intangibles management and their valuation and employees' participation and company based savings covers. He was postdoctoral researcher at Université Paris-Sud, where he contributed to the impact of cyberattacks on listed firms.

Ahmed Bounfour is Professor at the Université Paris-Sud, Université Paris-Saclay and Holder of the European Chair on Intangibles (www.chairo-nintellectualcapital.u-psud.fr). His research focus principally on the assessment of firms' intangible value as well on the definition of policies targeting intangibles and digital transformation.

Altay Özaygen, is postdoctoral researcher at Université Paris-Sud, Université Paris-Saclay. He completed his PhD in management in 2014. His research interests are economics of information security, intellectual property rights, open innovation, patent analysis and software industry. Before his PhD, Altay worked as a programmer and Unix system administrator for nearly 10 years.

Rokhaya Dieye holds a PhD in economics and has expertise in econometrics, network economics, and impact evaluation methods. Prior to joining Deloitte Economic Advisory in 2018, Rokhaya worked as a postdoctoral researcher at the Grenoble Applied Economics Laboratory (GAEL) and Université Paris-Sud, Université Paris-Saclay, where she contributed to the macroeconomics of cyberattacks.

PUBLIC INTEREST STATEMENT

In this study, we measured the financial market reaction after a cyber-attack. We used an extensive dataset comprising 3,680 cyberattacks on firms listed in 5 different stock markets worldwide. Our approach is based on a hybrid valuation inspired by the event study methodology and a counterfactual analysis. The event study methodology attempts to measure the informative relevance of an event and analyze the response of stock prices following the release of new information. Finance theory suggests that the even study analysis helps to measure the value of a firm following the impact of a specific event, a release of new information. It is expected that the market provides a negative return after a data breach. However, this study shows different abnormal returns for various event dates related to data breaches for different markets. This research deepens our understanding of the market reaction to a data breach for a large, wide-ranging sample of markets.

Subjects: Engineering & Technology; Economics, Finance, Business & Industry; Information Science

Keywords: Cyberattacks; valorization; market sensitivity; event study methodology; cumulative average abnormal return; counterfactual analysis
JEL Classification: G11; G14; G15; G22

1. Introduction

Recent decades have seen the advent of the knowledge society, and the contribution of intellectual assets to value creation has become evident, due to the rapid development and widespread deployment of information technologies (Yayla & Hu, 2011). Increasing internet connectivity has created a dynamic platform for communication, collaboration and promoting innovation. However, our increasing dependency on internet-based platforms and services has significantly increased the exposure of individual users and corporations to criminal activities. In this context, information security and privacy are key issues for organizations (Luftman, Kempaiah, & Nash, 2008). From the financial angle, the average cost of data breaches and security incidents continues to increase. It was estimated at an average of US $350,000 for a single event in 2008 (Richardson & Director, 2008). Similarly, according to the 2018 Data Breach Study prepared by the Ponemon Institute for IBM, the total cost of a data breach to a company is staggering—with an estimated average of $3.86 million (+6.4% compared to 2017). The loss of 1% of customers due to a data breach incurs a total average cost of $2.8 million, rising to $6 million if 4% of customers are lost (Ponemon, 2018). These figures show that a data breach can have devastating effects, by damaging a firm's reputation and potentially paving the way for lawsuits from either shareholders or customers (Hasan & Yurcik, 2006). In the context of the United States, the Federal Trade Commission can fine a firm that it finds is responsible for a breach, or can recommend an expensive overhaul of processes to prevent future incidents. In the case of ChoicePoint, the company was forced to pay penalties of $15 million (Federal Trade Commission, 2006) following a privacy debacle.

From a different angle, Campbell, Gordon, Loeb, and Zhou (2003) identified a highly significant correlation between privacy and trust. Thus, a privacy incident can damage a relationship with a customer or partner that is built on trust. Economically, this can be measured in terms of the ramifications for the company's market share (Rhee & Haunschild, 2006). Moreover, the stock market can be very harsh with firms that it considers have been irresponsible (Acquisti, Friedman, & Telang, 2006). This was the case for ChoicePoint, whose share valuation decreased from $46.01 to $37.64 during the 2 weeks that followed the incident in 2005. Beyond the immediate costs, a privacy incident can have long term, indirect consequences. Consumers who retain a negative impression of companies that have been found to be negligent will alter their consumption patterns. This observation was underlined by Berezina, Cobanoglu, Miller, and Kwansa (2012), who demonstrated that data breaches negatively impact consumer perceptions, even in non-online companies, such as hotels. Moreover, firms can face higher insurance premia following a breach, and future business partners can be less inclined to trust them. Given these risks, most companies seek to secure their networks and protect sensitive customer information databases (Bianchi & Tosun, 2018). However, those that fail to take adequate measures can face the loss of customer data.

Although growing rapidly, the literature on the financial impacts of security breaches is rather sparse (Bianchi & Tosun, 2018). Smith, Milberg, and Burke (1996) identified four datarelated dimensions of privacy concerns: collection, errors, secondary use, and unauthorized access. Although their findings have remained robust (Stewart & Segars, 2002), Moor (1997) suggested that several privacy theories could be combined into the concept of "control/restricted access", indicating the situation where an individual expects to be able to control the flow of their personal information, and restrict access where appropriate. In practice, the proper treatment of consumer information is a part of an 'implied social contract' with the customer (Milne & Gordon, 1993). In this sense, a promise of the fair use of information can override a clear consumer aversion to sharing information (Culnan, 1999). Consequently, a violation of this promise is considered as a breach of the conceptualization of control/restricted access.

Our study is a step towards remedying the dearth of research on the question of financial market sensitivity to data breaches. The rest of the paper is organized as follows: Sections 2 describe the data and introduce our methodology. Section 3 presents the empirical findings, including the summary statistics. Section 4 discusses these results and presents some conclusions.

2. Data and methodology

We use the Advisen database. This database reports cybersecurity incidents that are made public and provides a range of information related to the target. The initial search identified 13,227 cyberattacks on 2,841 targets. However, 8,961 were removed as there was no matching financial data available in the Compustat (North America and Global) database. The final dataset therefore contained details of 4,266 cybersecurity incidents, related to 2,200 listed companies distributed across various financial markets. In our study, we consider major financial market response to 3,680 information on cybersecurity data breach incidents. Table 1 provides the distribution of the sample analyzed according to the stock markets. Table 2 summarizes the main date-related statistics concerning the event, which are analyzed in this study. Unsurprisingly, 95.6% of cases relate to companies in the United States (either listed in NASDAQ or the New York Stock Exchange). This is due to data breach notification laws that were first introduced in California in 2002 (California S.B. 1386 bill) before expanding to other states. Despite this dominance, we extend our empirical study to a few European countries (France, Germany and the United Kingdom).

Tables 2 and 3 report detailed date-related statistics for our five markets analyzed. Like Table 2, Figure 1 is based on the accident date and shows the yearly distribution of cyberattacks on firms listed in top five stock markets for the period 1984–2017. Table 4 shows the distribution of cyberattacks across economic sectors, and Figure 2 shows the annual change.

2.1. Propensity score matching

Our methodology closely follows the methods developed in the literature (Rosenbaum & Rubin, 1983). First, we construct counterfactuals, as we need to know what would have

Table 1. Cybersecurity data breach incidents in major financial markets (n = 3680)

Financial Market	Number of events	Frequency
Frankfurt Stock Exchange	32	0.87
Euronext Paris	46	1.25
London Stock Exchange	84	2.28
NASDAQ National Market	1695	46.06
New York Stock Exchange	1823	49.54
Total	3680	100.00%

Table 2. Main date-related statistics for the events analyzed in this study (n = 4266)

Accident Date		First Notice Date		Original Loss Start Date	
Min.:	1984-06-01	Min.:	1988-12-31	Min.:	1998-01-01
1st Qu.:	2009-04-20	1st Qu.:	2010-06-10	1st Qu.:	2008-01-01
Median:	2012-07-31	Median:	2013-05-21	Median:	2011-11-01
Mean:	2011-11-06	Mean:	2012-11-01	Mean:	2010-09-15
3rd Qu.:	2015-01-01	3rd Qu.:	2015-12-14	3rd Qu.:	2014-01-01
Max.:	2017-11-01	Max.:	2017-12-19	Max.:	2017-09-01
NA's:	641	NA's:	1666	NA's:	3104

Table 3. Event dates with respect to different stock markets analyzed in this study

stock.market	count	min_accident	max_accident	min_first_notice	max_first_notice	min_loss_start	max_loss_start
New York Stock Exchange	1823	1984-06-01	1984-06-01	1988-12-31	1988-12-31	1998-01-01	1998-01-01
NASDAQ	1695	1995-12-01	1995-12-01	1999-08-09	1999-08-09	2000-04-21	2000-04-21
London Stock Exchange	84	1998-11-01	1998-11-01	2007-01-09	2007-01-09	1998-11-01	1998-11-01
Euronext Paris	46	2005-02-14	2005-02-14	2007-05-07	2007-05-07	2005-02-14	2005-02-14
Frankfurt Stock Exchange	32	2001-01-01	2001-01-01	2004-05-05	2004-05-05	2015-02-02	2015-02-02

cogent economics & finance

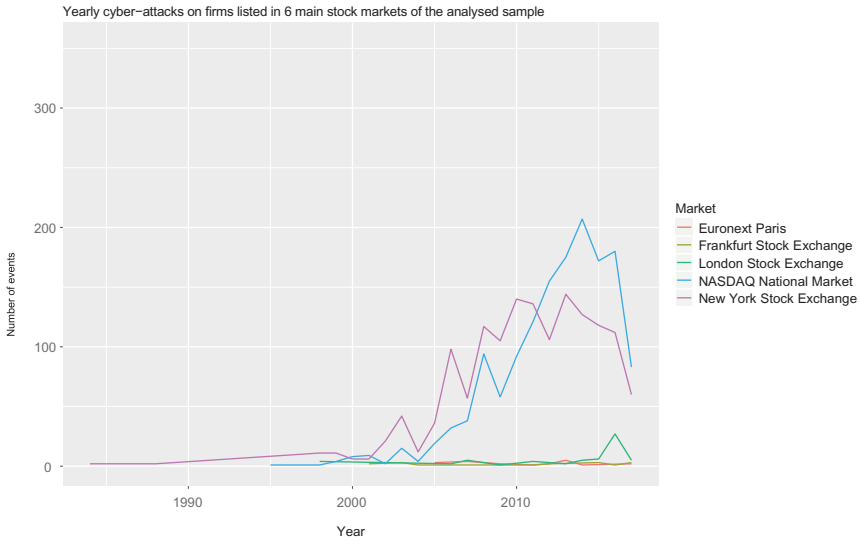


Figure 1. Annual distribution of cyberattacks (accident date) on firms listed in the top five stock markets (1984–2017).

Table 4. Cyber event distribution with respect to different economic sectors (SIC division), all markets combined

SIC	n
Finance, Insurance and Real Estate	1340
Services	1054
Manufacturing	497
Retail Trade	386
Transportation, Communications, Electric, Gas and Sanitary service	254
Wholesale Trade	71
Mining	32
Construction	27
Nonclassifiable	11
Public Administration	7
Agriculture, Forestry and Fishing	1

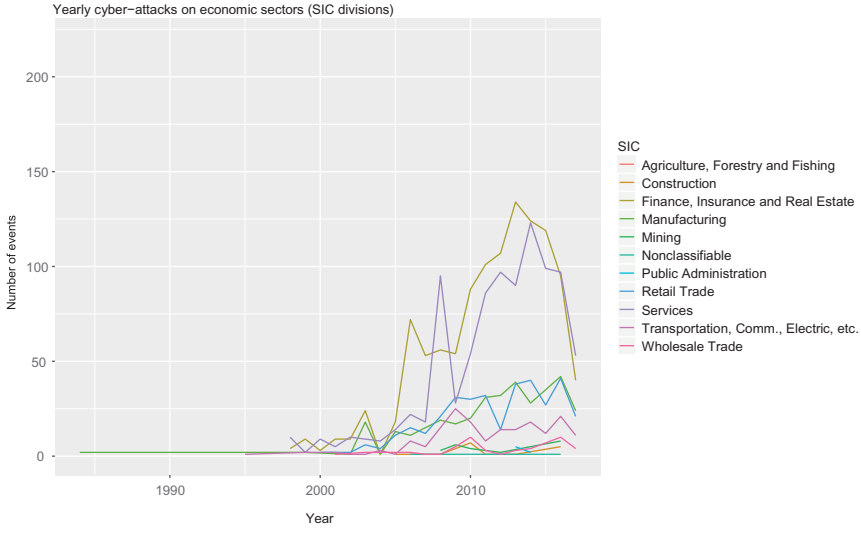


Figure 2. Annual distribution of cyberattacks (date) on firms listed in the top five economic sectors based on SIC division (1984–2017).

happened if the firm was not attacked. As this information is not available, we construct counterfactual enterprises at the sector level, with the help of propensity score matching (Dehejia & Wahba, 2002).

Specifically, we match each attacked firm with another with similar, observable characteristics (X), and use the latter as a counterfactual. In order to avoid heterogeneity amongst our panels, the matching characteristic vector (X) consists of the geographical implementation of the company, the financial market in which a company is listed, the industry sector, the size of the company (number of employees), and the reference year and firm's S&P sector index. Propensity score matching needs to respect two major hypotheses: the CIA (Conditional Independence Assumption) and common support assumptions. The CIA states the following:

$$(Y_A, Y_N) \perp D|X \tag{1}$$

where Y_A and Y_N respectively, for the outcomes of the attacked and not-attacked firms. D is the treatment indicator such that $D = 1$ if the firm is attacked, 0 otherwise. In other words, conditional on X, the assignment of firms to the treatment group (cyber-attacked) is random. The common support assumption states that for each value of X, there is a positive probability of being both treated and untreated, such that:

$$0 < P(D = 1|X) < 1 \tag{2}$$

Various algorithms are available for propensity score matching, including Mahalanobis matching, kernel matching, nearest neighbor matching, etc. In this study, we opted for the nearest neighbor algorithm, which resulted in two panels: Panel A, attacked firms (the treatment group); and Panel B, not-attacked firms (the control group). The Average Treatment Effect (ATT) or impact of cyberattacks on intangibles is given by the following formula:

$$ATT = E[EY_{iA}|D = 1 - EY_{iN}|D_i = 0|D = 1] \tag{3}$$

where Y_{iA} is the intangible capital of firm i that is attacked (panel A), Y_{iN} is the intangible capital value of firm i that is not attacked (panel B), and D_i is a dummy variable equal to 1 if firm i is attacked, 0 otherwise. Our dataset of perfectly matched pairs consisted of more than 800 firms within our final database. The result of our comparison of attacked and not-attacked firms' results are given in Figure 3. The matching method performed well and resulted in two panels of attacked and not-attacked firms.

2.2. Event study methodology

The effect of an economic event on a firm's value is a recurring theme in economics and management sciences. Finance theory suggests referring to financial market data in order to measure the impact of a specific event on the value of a firm based on the event study methodology. This has

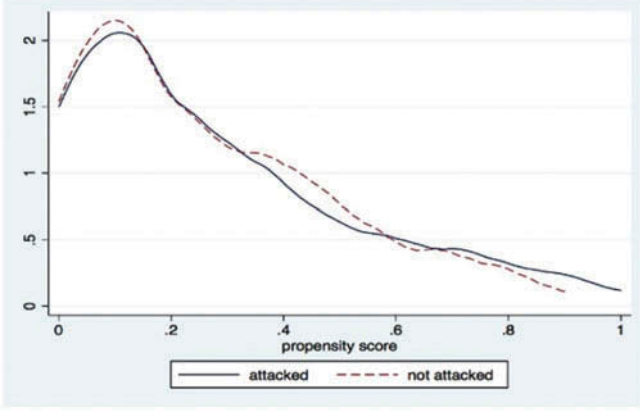


Figure 3. Results of propensity score matching for attacked and not-attacked firms.

become a classic approach in finance following the pioneering work of Ball and Brown (1968) and Fama, Richardroll, Jensen, and Roll (1969). The methodology attempts to measure the informative relevance of an event and analyze the response of stock prices following the release of new information. In this perspective, as in signal theory, favorable (unfavorable) information generates an increase (decrease) in prices and therefore positive (negative) abnormal returns. Furthermore, the magnitude of the variation is positively and highly correlated to the kind of information disclosed by the event. Since the work of Dolley (1933), which investigated the effect of stock splits on stock prices, the methodology has been adopted in many different fields: accounting and finance (Binder, 1998; MacKinlay, 1997), Management (Lambertides 2009) Marketing (Mase, 2009), information systems Roztocki and Weistroffer (2009). Our approach is consistent with earlier event study analyses, and is based on the following equations:

$$\begin{aligned} H_0 &: (R_i|y_i) - E(R_i) = E(AR_i|y_j) = 0 \\ H_1 &: (R_i|y_i) - E(R_i) = E(AR_i|y_j)\ 6 = 0 \end{aligned} \tag{4}$$

for all y_j. Where: y_i: Information likely to affect the valuation of stock i during the event period.

R_i: Stock's return i during the event period.

$E(R_i)$: Expected stock's yield i.

AR_i: Abnormal return of stock $i(AR_{i,\tau} = R_{i,\tau} - E[R_{i,\tau}|\omega_{i,\tau}])$

Defined as the difference between observed and theoretical profitability, the abnormal return is the crucial measure. In fact, security performance and/or profitability may only be considered as 'abnormal' relative to a defined benchmark or a theoretical model of an ex-ante expected return. Therefore, the choice of model that is adopted to run event studies has been widely discussed (Bhushan, 1994). Developed in the early 1960s by Sharpe (1964); Treynor (1961); Lintner (1965, 1975); Mossin (1966), the strength of the Capital Asset Pricing Model (CAPM) is that it is able to predict profound implications for asset pricing and investor behavior. Our review of the literature on event study models revealed a tendency to favor the CAPM, as performance is comparable to regression-based models, including the market model.

The estimation period refers to the window that begins before the analyzed event, during which researchers predict a return to normal. The length of this period plays a crucial role in event studies, since it may affect estimated parameters and therefore the power of statistical tests. However, there is no specific rule related to its length, and no consensus has emerged from existing empirical and theoretical research. However, a period of between 5 and 8 months is often used for daily studies, and between 20 and 60 months for monthly studies, to avoid estimation bias (Gajewski & Ginglinger, 2002; Hachette, 1991).

The event window refers to the period surrounding the date of the event, during which the event influences the market price. Like the estimation period, there is no consensus in the literature regarding its length, and a variety of windows have been used in previous works. For example, MacKinlay (1997) and Pirounias, Mermigas, and Patsakis (2014); Chen and Siems (2004) suggest using [1, 1] event window. On the other hand, Gewald and Gellrich (2007) use [3, 3] while, Cheng, Tsao, Tsai, and Tu (2007) use [5, 5]. Even longer periods have been used depending on the event studied: [−10, 10] and [−20, 20] for outsourcing (Gewald & Gellrich, 2007), or [−45, 5] and [−44, 10] for the impact of a data breach on reputation (Sinanaj, Muntermann, & Cziesla, 2015).

Although the length of the window varies (Peterson, 1989), researchers tend to try to shorten it, in order to ensure that measured effects are, in fact, due to the analyzed event. In this study, we follow Ahern (2009) and Andrade, Mitchell, and Stafford (2001), and opt for a five-day window, which seems to be long enough to reflect the information available until the publication of new events. Moreover, and in

order to control for potential leakage of information prior to the announcement, we include the day that precedes the reporting of an event. Consequently, we define [−1, 3] as our event window. Furthermore, we opt for the CAPM with data for a 120-trading day estimation period that ends fifteen (15) days before the event date, to prevent potential contamination by the event (King, 2011).

3. Results

The results presented in this section mainly relate to North American companies and extended to main European stock markets (specifically the French, German and London stock exchanges). Furthermore, we would like to emphasize main difference between the NYSE and NASDAQ markets which may generate an apparent discrepancy in event studies results[1]. In fact, the largest difference between these two markets results from their operational difference. In that sense, the NYSE is an auction market (transactions are typically elaborated between individuals within an auction) however the NASDAQ is a dealer market (dealers or trading technologies ensure an intermediary role between market participants). Meanwhile, the Nasdaq has more companies than the NYSE but has a wider spectrum in terms of the size of companies. In fact, the NYSE incorporate industrial companies characterized by their financial and economic stability and usually investors consider it as secure and less volatile. On the other side, the NASDAQ is typically known through its high-tech companies and is seen as a place for growth-oriented tech stocks.

3.1. Accident date

The *accident date* refers to the beginning of the cyber-attack. During the accident window, American companies were expected to generate a mean return of 0.49% for NASDAQ-listed

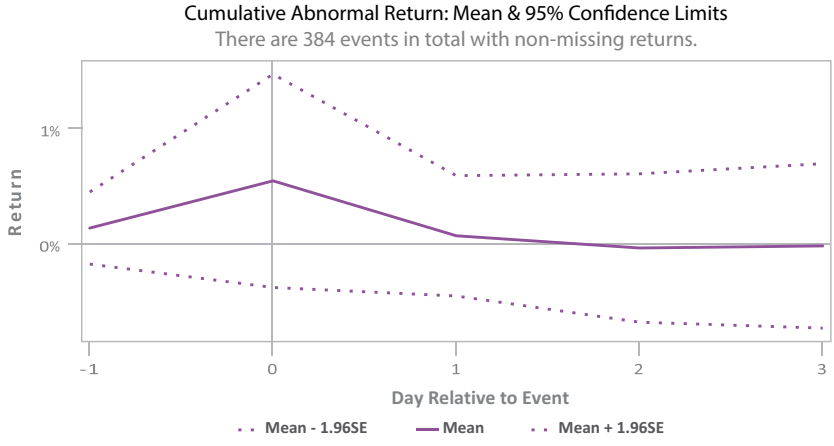


Figure 4. Accident date NASDAQ, whole sample containing attacked and non-attacked firms.

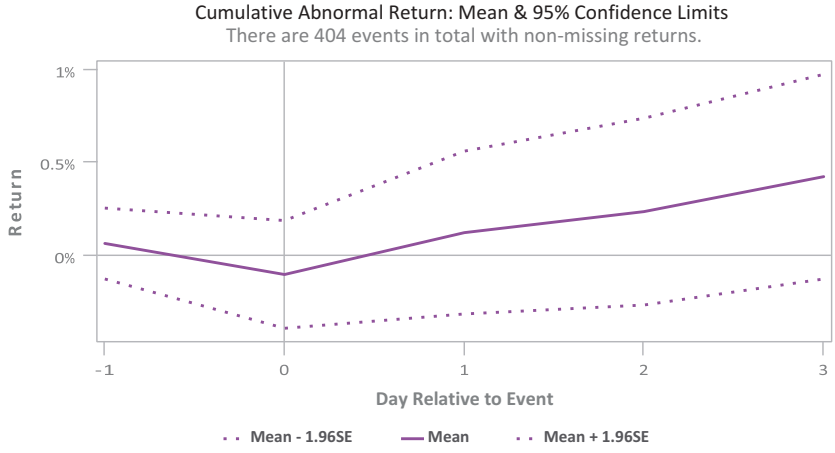


Figure 5. Accident date NYSE, whole sample containing attacked and non-attacked firms.

companies and almost 0.42% for those listed on the NYSE. However, following a cyber-attack, there are cumulative abnormal returns of −0.03% and 0.48% for NASDAQ and NYSE markets, respectively. However, the accident date is prior to the first notice date, the date in which the event is initially reported.

In order to deepen our analysis, we applied the counterfactual analysis methodology to the NASDAQ market. This found that counterfactual (not attacked) firms generated 0.9% cumulative abnormal returns, compared to −0.75% for attacked ones. As a result, cyberattacks created an average deficit of 1.65% in cumulative abnormal returns and 0.86% in average returns during the event window. Figure 4 and 5 show the cumulated **average** abnormal return for NASDAQ and NYSE respectively for the accident date **(further results are reported in Table A2. And A3.)**.

3.2. First notice date

The *first notice* date is the date on which the event was initially reported, or notice was received. Based on the market model, we expect that investing in our panel would generate a cumulative total return of 0.83% for the NASDAQ, and losses of 0.53% for the NYSE. However, in practice, an investment made on the first notice date of a cyber-attack created returns of 1.37% and 0.125%, respectively. In fact, if the company that was a victim of a cyber-attack was listed on the high-tech NASDAQ market, cumulative abnormal returns were 0.54%. On the other hand, such news is perceived adversely by the NYSE, and manifests in an average loss of 0.17% on both the first notice day and the following day. As a result, an average cumulative loss of 0.65% is generated during the event window. This result is consolidated by the counterfactual analysis, according to which not-attacked firms generate a cumulative total return of almost 1.3%, compared to a cumulative loss of 0.15% for attacked companies. Figure 6 and 7 show the cumulated **average** abnormal return for NASDAQ and NYSE respectively for the first notice date. Figure A.1 and A.2 show the cumulated **average** abnormal return for NASDAQ and NYSE respectively for the accident date issued through counterfactual analysis **(further results are reported in Table A4., A5., A6. And A7.)**. x`

Results related to the market reactions after a cyberattack found in the literature are mixed. Kannan, Rees, and Sridhar (2007) and Acquisti et al. (2006) show on the long run there is no significant negative impact of data breach. Kannan et al. (2007) show that firms which have reported some data breach during the dotcom era showed a higher negative abnormal return than cases after 9/11. Moreover, Gordon, Loeb, and Zhou (2011) show that there are insignificant results with some positive returns after 9/11 data-breach cases. However, most of the studies found a negative return after data-breach if the analyzed event-window is limited to few days

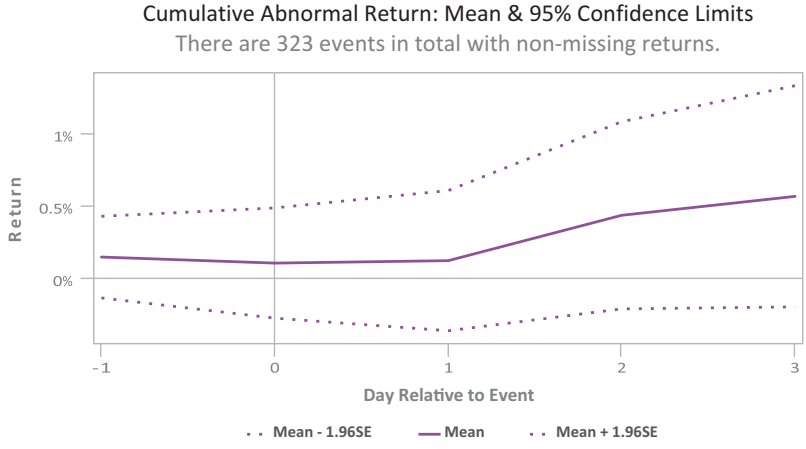
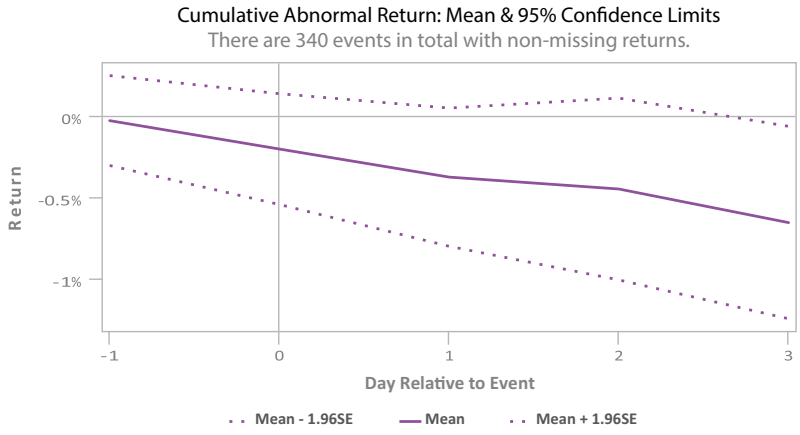


Figure 6. First notice date NASDAQ, whole sample containing attacked and non-attacked firms.

cogent economics & finance

Figure 7. First notice date NYSE, whole sample containing attacked and non-attacked firms.



Campbell et al. (2003); Cavusoglu, Mishra, and Raghunathan (2004); Yayla and Hu (2011); Pirounias et al. (2014).

3.3. Original loss start date

The *original loss* start date represents the date on which a loss due to a cyber-attack begins. For the NASDAQ, despite an average abnormal return of 0.016 on the day of the event, such events generate negative returns amounting to −0.015 the following day and −0.003 the day after. This observation is consolidated by the counterfactual analysis. In fact, the start of the loss is reflected in a fall in average abnormal returns from 0.192 to −0.213. Moreover, we note that average cumulative abnormal returns for not-attacked firms (0.19%) exceed attacked firms (−0.73%). However, NYSE-listed companies seem to be less sensitive to these events. In fact, the original loss start date is consistent with mean cumulative abnormal returns of 0.4% during the event window, and a spread of 0.3% based on the counterfactual analysis. By the end of the loss period, financial markets generate 0.22% and 0.39% average cumulative abnormal returns for the NASDAQ and the NYSE, respectively, during the event window. In the case of changes to the original loss start (end) date due to court proceedings, the loss start (end) date reports the beginning (end) of the period during which damages from cyberattacks were incurred. Empirically, the original loss start date is associated with an average cumulative abnormal return of 1.31% for the NASDAQ and 0.36% for the NYSE. Indeed, the announcement of the loss end date (if different from the original loss end date) generates average cumulative abnormal returns of 0.09% and 0.47%, respectively.

3.4. Extension and robustness of our results

3.4.1. Cyberattacks on European countries (France, Germany, and UK)

Applied to the European context, cyberattacks generate negative cumulative abnormal returns of 0.77% during the event window [0, 3] for British companies. Moreover, average total returns for attacked French firms fall during the event window [0, 3] (from 0.006 to −0.001) and from 0.0001 to −0.006 for German firms. Furthermore, as soon as the cyberattack is reported, average total returns fall to 0.0002 (from 0.00435). This observation is consistent for both French and German companies, where we see cumulative abnormal returns of −0.445% and −0.98%, respectively. In France, the announcement of the original loss period (start and end dates) is associated with two main observations. On the one hand, a decrease in cumulative average abnormal returns of almost 0.37% during the original loss start date window. On the other hand, a decrease of 0.2% in cumulative average abnormal returns for the original loss end date window. However, German and British financial markets do not react immediately to such announcements and the analysis of the original loss start (end) dates reveal positive cumulative abnormal returns of 0.76% (−0.54%) and 0.34% (0.2%). In case of adjustments to loss start or end dates, financial markets consolidate previous results for France, Germany, and the United Kingdom.

3.4.2. Results robustness: Fama-French plus momentum model

Applied in event studies, expected return models predict hypothetical returns that are established based on actual (and past) stock returns to deduct abnormal returns. In order to check the robustness of our results, we refer to Fama-French Plus Momentum Model (also known as Carhart's Four Factor Model) within our event analysis. While the CAPM uses one beta (systematic risk) to explain the stock return, Fama and French decided to integrate two additional betas (size and value) in order to improve estimation accuracy. Their model was extended by Carhart through integrating the momentum factor.

Applied to the US market, we notice that a cyberattack generates a loss of 1.196% and 0.434% of cumulative abnormal returns for Nasdaq and NYSE, respectively, during the event windows [−1,3]. Whereas, not attacked firms over-perform by 4,16% and 0.564% for NYSE and NASDAQ, respectively, during accident dates. These results are confirmed within the first notice date of cyberattack. In fact, the Nasdaq overreact to a cyberattack detection by generating a CAR of almost 1.88% while the counterfactual sample is reflecting a negative return of −0.89%. However, we notice an opposite reaction of the NYSE on information release related to first notice date. In fact, involved companies suffer from a decrease of their returns out of 0.766% while non-affected ones generate a cumulative abnormal return of 0.372% which confirm our previous results.

4. Discussion and concluding remarks

It is expected that the market provides a negative return after a data breach Campbell et al. (2003); Cavusoglu et al. (2004); Yayla and Hu (2011); Pirounias et al. (2014). However, this study shows different abnormal returns for various event dates related to data breaches for different markets. This research deepens our understanding of the market reaction to a data breach for a large, wide-ranging sample of markets.

The literature shows mixed results regarding market reactions after data breach. One of the comparison periods is before and after 9/11. Kannan et al. (2007) show that there is no significant negative impact of data breach on the long run (after 15 days). A negative bias is found after 9/11 event but this is interpreted as cofounding event. Moreover, authors argue that there are different reactions of investors and the dotcom era showed a higher negative abnormal returns. Gordon et al. (2011) show that security breaches occurring over the post-9/11 sub-period have an insignificant effect on the stock returns of firms and there are also other cases which show positive returns after a data breach. Gatzlaff and McCullough (2010) demonstrate that firms with higher market-to-book ratios experience greater negative abnormal returns. Firm size and subsidiary status mitigate the negative effect of a data breach on the firms' stock price. Authors provide a table which shows the number of firms having positive and negative CAR for different event windows. All tested event windows under 60 days show that firms experiencing negative returns outnumber the number of positive returns.

Acquisti et al. (2006) show that there is negative mean abnormal return the day of the breach announcement but decreases the following day and the abnormal return become positive on $t + 3$. Garg, Curtis, and Halper (2003) found that theft of customer data shows positive returns ranging from 0.2% to 1.2% at t, $t + 1$ and $t + 2$ periods unlike to the theft of credit card information, DoS and web-site defacement cases found in their sample. Hovav and D'Arcy (2004) show that there is not a negative abnormal return when firms indicate that they went through a virus attack. The same result is obtained when the analysis is carried out for different economic sectors.

There are two explanations that we can provide for the positive return which is observed in the literature. Hovav and D'Arcy (2004) argue that firms are not penalized when involved in events with negative information and a correct communication strategies that are adopted by firms may decrease the negative market reactions. The second argument is financial. It is argued that, the average cost for data breach has become less costly Gordon et al. (2011). According to Romanosky (2016), a typical cyber incident costs less than $200k which is a modest financial impact compared to the increasing rates of breach and legal actions that the public is mostly aware. The average $200k cost represents only 0.4% of

firm revenues which is also far less than other types of losses due to frauds, theft or corruption. Moreover, Romanosky (2016) is arguing that firms are adopting an optimal level of cybersecurity as they do with other types of security risk and they are investing limited amount of money on data protection.

Our results are consistent with the literature and the results obtained in this study can provide a guide for both retail and institutional investors, and the growing cyber-insurance industry. Investors should reconsider their asset allocation strategy as a function of the exposure of a firm to the risk of a cyber-threat, and the stock market it is listed on. Moreover, a diverse investment portfolio that includes cybersecurity stocks could be an attractive solution to decrease the risks of a cyber-attack and its negative outcomes. From the viewpoint of the cyber-insurance industry, understanding the impact of a cyber-event on a firm's value in different stock markets could help to refine the risk models used.

Although our results are obtained from a large sample, our work should be deepened to understand the source of the attack and the motivation of cyber-criminals. There is a need for an in-depth analysis of the exposure of firms to a cyber-attack, and the profiling of cybercriminals. We leave this for a future study.

Notes

1. Please refer to Table A1 for a definition of variables used in output tables of our event study analysis.

Acknowledgements
This research is the result of the HERMENEUT project, which is funded under the H2020 Grant agreement n° 740322.

Funding
This work was supported by the Horizon 2020 Framework Programme [740322].

Author details
Niaz Kammoun[1]
E-mail: niazkammoun@gmail.com
Ahmed Bounfour[1]
E-mail: ahmed.bounfour@u-psud.fr
ORCID ID: http://orcid.org/0000-0002-3158-3582
Altay Özaygen[1]
E-mail: altay.ozaygen@u-psud.fr
ORCID ID: http://orcid.org/0000-0001-5594-5245
Rokhaya Dieye[1]
E-mail: rokhaya.dieye@gmail.com
[1] Laboratoire RITM, Université Paris Sud, Université Paris-Saclay, Faculté Jean Monnet 54, Sceaux, France.

Citation information
Cite this article as: Financial market reaction to cyberattacks, Niaz Kammoun, Ahmed Bounfour, Altay Özaygen & Rokhaya Dieye, *Cogent Economics & Finance* (2019), 7: 1645584.

Correction
This article has been republished with minor changes. These changes do not impact the academic content of the article.

Cover image
Source: Author.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*,Milwaukee, Wisconsin, USA 94. http://aisel.aisnet.org/icis2006/94

Ahern, K. R. (2009). Sample selection and event study estimation. *Journal of Empirical Finance*, *16*(3), 466–482. doi:10.1016/j.jempfin.2009.01.003

Andrade, G., Mitchell, M., & Stafford, E. (2001). New evidence and perspectives on mergers. *Journal of Economic Perspectives*, *15*(2), 103–120. doi:10.1257/jep.15.2.103

Ball, R., & Brown, P. (1968). An empirical evaluation of accounting income numbers. *Journal of Accounting Research*, *6*(2), 159–178. doi:10.2307/2490232

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991–1010. doi:10.1108/09596111211258883

Bhushan, R. (1994). An informational efficiency perspective on the post-earnings announcement drift. *Journal of Accounting and Economics*, *18*(1), 45–65. doi:10.1016/0165-4101(94)90018-3

Bianchi, D., & Tosun, O. (2019). *Cyber attacks and stock market activity*. SSRN: https://ssrn.com/abstract=3190454 or http://dx.doi.org/10.2139/ssrn.3190454

Binder, J. (1998). The event study methodology since 1969. *Review of Quantitative Finance and Accounting*, *11*(2), 111–137. doi:10.1023/A:1008295500105

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. doi: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. doi:10.1080/10864415.2004.11044320

Chen, A. H., & Siems, T. F. (2004). The effects of terrorism on global capital markets. *European Journal of Political Economy*, *20*(2), 349–366. doi:10.1016/j.ejpoleco.2003.12.005

Cheng, J. M.-S., Tsao, S.-M., Tsai, W.-H., & Tu, H. H.-J. (2007). Will eChannel additions increase the financial performance of the firm?—The evidence from Taiwan. *Industrial Marketing Management*, *36*(1), 50–57. doi:10.1016/j.indmarman.2006.06.011

Commission, Federal Trade (2006). Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief https://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069stip.pdf

Culnan, M. J. (1999). *Georgetown internet privacy policy survey: Report to the federal trade commission*. Washington, DC: Georgetown University, The McDonough School of Business.

Dehejia, R. H., & Wahba, S. (2002). Propensity score-matching methods for nonexperimental causal studies. *Review of Economics and Statistics*, *84*(1), 151–161. doi:10.1162/003465302317331982

Dolley, J. C. (1933). Characteristics and procedure of common stock split-ups. *Harvard Business Review*, *11*(3), 316–326.

Fama, E., Richardroll, J., Jensen, M. B., & Roll, R. (1969). The adjustment of stcok prices to new information. *International Economic Review*, *10*(1), 26. doi:10.2307/2525569

Gajewski, J.-F., & Ginglinger, E. (2002). Seasoned equity issues in a closely held market: Evidence from France. *Review of Finance*, *6*(3), 291–319. doi:10.1023/A:1022024925877

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74–83. doi: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. doi:10.1111/rmir.2010.13.issue-1

Gewald, H., & Gellrich, T. (2007). The impact of perceived risk on the capital market's reaction to outsourcing announcements. *Information Technology and Management*, *8*(4), 279–296. doi:10.1007/s10799-006-0008-0

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. doi:10.3233/JCS-2009-0398

Hachette, I. (1991). *Op´erations Financi`eres, Valeur de La Firme et Richesse Des Actionnaires: Le Cas Fran¸cais 1980-1990* (PhD Thesis), Paris 9.

Hasan, R., & Yurcik, W. (2006). A statistical analysis of disclosed storage security breaches. Proceedings of the Second ACM Workshop on Storage Security and Survivability, Alexandria, Virginia, USA. https://doi.org/10/dvnk6w

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. doi:10.1201/1086/44530.13.3.20040701/83067.5

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91. doi:10.2753/JEC1086-4415120103

King, Michael Robert, The Contagion and Competition Effects of Bank Bailouts Announced in October 2008 (2013). SSRN: https://ssrn.com/abstract=2019113 or http://dx.doi.org/10.2139/ssrn.2019113

Lambertides, N. (2009). Sudden CEO vacancy and the long-run economic consequences. *Managerial Finance*, *35*(7), 645–661. doi:10.1108/03074350910960364

Lintner, J. (1965). Security prices, risk, and maximal gains from diversification. *The Journal of Finance*, *20*(4), 587–615.

Lintner, J. (1975). The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets. In W.T. Ziemba and R.G. Vickson (Ed.), *Stochastic optimization models in finance,* (pp. 131–155). Elsevier.

Luftman, J., Kempaiah, R., & Nash, E. (2008). Key Issues for IT Executives 2005. *MIS Quarterly Executive*, *5*(2), 5.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, *35*(1), 13–39.

Mase, B. (2009). The impact of name changes on company value. *Managerial Finance*, *35*(4), 316–324. doi:10.1108/03074350910935812

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 206–215. doi:10.1177/074391569101200206

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, 27–32. doi:10.1145/270858.270866

Mossin, J. (1966). Equilibrium in a capital asset market. *Econometrica: Journal of the Econometric Society*, 768–783. doi:10.2307/1910098

Peterson, P. (1989). Event Studies: A Review of Issues and Methodology. Quarterly Journal of Business and Economics, 28(3), 36–66. Retrieved from http://www.jstor.org/stable/40472954http://www.jstor.org/stable/40472954.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, *19*(4), 257–271. doi:10.1016/j.jisa.2014.07.001

Ponemon. (2018). *2018 cost of a data breach study: Global overview, Ponemon Institute, Traverse City, Michigan, USA*. Technical report..

Rhee, M., & Haunschild, P. R. (2006). The liability of good reputation: A study of product recalls in the US automobile industry. *Organization Science*, *17*(1), 101–117. doi:10.1287/orsc.1050.0175

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer Security Institute*, *1*, 1–30.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135.

Rosenbaum, P. R., & Rubin, D. B. (1983). The central role of the propensity score in observational studies for causal effects. *Biometrika*, *70*(1), 41–55. doi:10.1093/biomet/70.1.41

Roztocki, N., & Weistroffer, H. R. (2009). Information technology investments: Does activity based costing matter? *Journal of Computer Information Systems*, *50*(2), 31–41.

Sharpe, W. F. (1964). Capital asset prices: A theory of market equilibrium under conditions of risk. *The Journal of Finance*, *19*(3), 425–442.

Sinanaj, G., Muntermann, J., & Cziesla, T. (2015). How Data Breaches Ruin Firm Reputation on Social Media!-Insights from a Sentiment-based Event Study. 902–916. Retrieved from https://pdfs.semanticscholar.org/7ae6/c10058ecf4967f678f3bd08b3aa0d37c6327.pdf

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196. doi:10.2307/249477

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. doi:10.1287/isre.13.1.36.97

Treynor, J. L. (2012). Toward a theory of market value of risky assets. In Wiley Finance. Treynor on Institutional Investing (pp. 49–59). John Wiley & Sons.

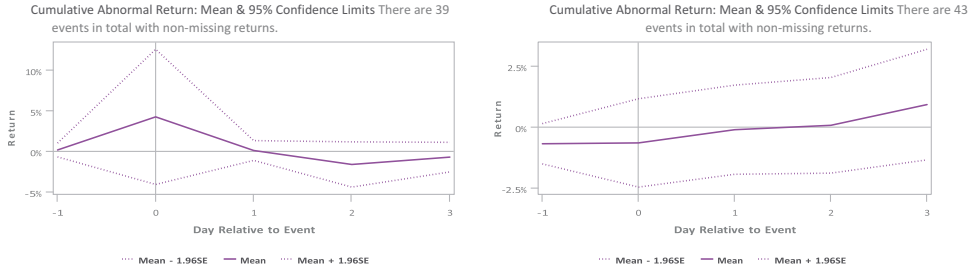
Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77. doi:10.1057/jit.2010.4

cogent economics & finance

A. Appendix

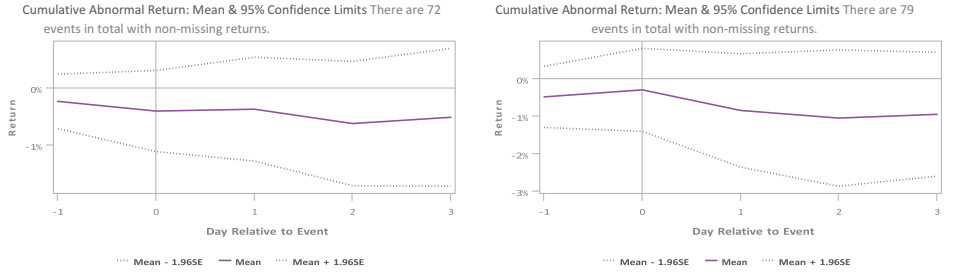
A.1 Accident date (counterfactual analysis)

Figure A1. Attacked and non-attacked firms listed on NASDAQ.



(a) Attacked (b) Not-attacked

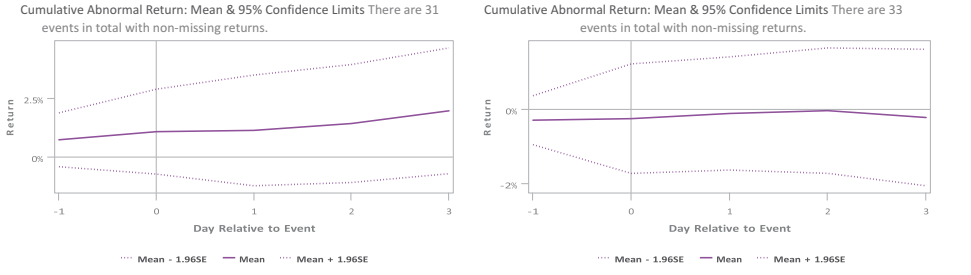
Figure A2. Attacked and non-attacked firms listed on NYSE.



(a) Attacked (b) Not-attacked

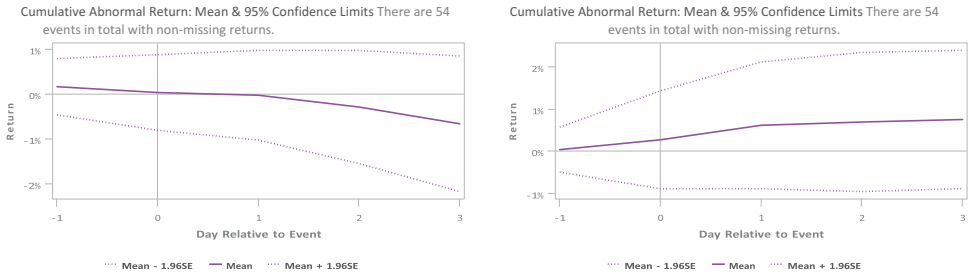
A.2 First notice date (counterfactual analysis)

Figure A3. Attacked and non-attacked firms listed on NASDAQ.



(a) Attacked (b) Not-attacked

Figure A4. Attacked and non-attacked firms listed on NYSE.

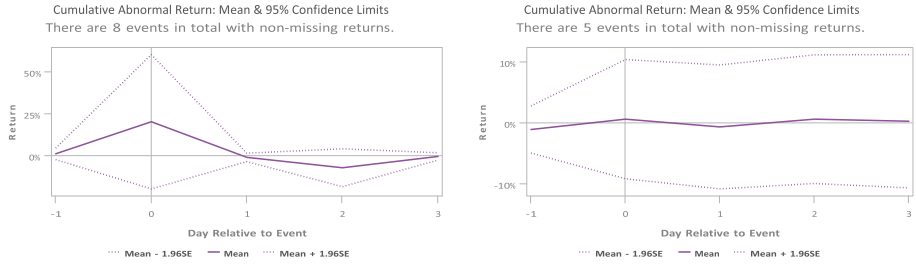


(a) Attacked (b) Not-attacked

A.3 Original loss start date (counterfactual analysis)

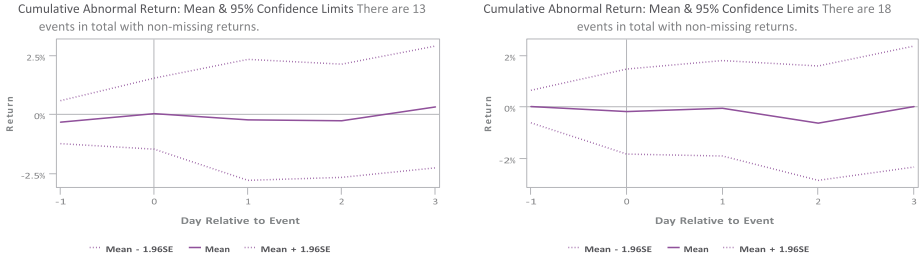
NASDAQ National Market YES.pdf NASDAQ National Market Not.pdf

Figure A5. Attacked and non-attacked firms listed on NASDAQ.



(a) Attacked (b) Not-attacked

Figure A6. Attacked and non-attacked firms listed on NYSE.



(a) Attacked (b) Not-attacked

cogent economics & finance

A.4 Extract of event study output[*]

Table A1. Definition of variables used in event study analysis output tables

variable name	variable label
evttime	Day Relative to Event Date
ret m	Mean Total Return
abret m	Mean Abnormal Return
cret m	Mean Cumulative Total Return
car m	Mean Cumulative Abnormal Return
bhar m	Mean Buy-and-Hold Abnormal Return
cret me	Mean Cumulative Total Return(At the End of Event Window)
car me	Mean Cumulative Abnormal Return(At the End of Event Window)
bhar me	Mean Buy-and-Hold Abnormal Return(At the End of Event Window)
lower bound	Mean CAR—1.96SE
upper bound	Mean CAR + 1.96SE
pat ar	Patell Z for ARs
pat car	Patell Z for CARs
abret t	cross-sectional test
scar	standarized cumulative abnormal return

[*]Further output are available under request.

Table A2. Attacked firms listed on NASDAQ, the event refers to accident date. Model used is Fama-French Plus Momentum (final dataset)

evttime	ret m	abret m	car m	abret t	sar t	pat ar
−1	0.002202493	−.000385758	−.000385758	−0.23396	−0.64414	−0.78603
0	0.001757244	0.003301640	0.002915882	0.79800	−0.32289	−0.32230
1	0.001054893	−.004752904	−.001837022	−1.07414	0.11468	0.16207
2	0.000702185	−.001495263	−.003332285	−0.80797	−0.76703	−0.83148
3	−.001287509	0.001462276	−.001870009	0.67304	0.11872	0.15711
evttime	**cret me**	**car me**	**patcar me**	**car te**	**scar te**	**bhar me**
−1	.004914457	−.001870009	−0.72477	−0.48458	−0.51981	.003143217
0	.004914457	−.001870009	−0.72477	−0.48458	−0.51981	.003143217
1	.004914457	−.001870009	−0.72477	−0.48458	−0.51981	.003143217
2	.004914457	−.001870009	−0.72477	−0.48458	−0.51981	.003143217
3	.004914457	−.001870009	−0.72477	−0.48458	−0.51981	.003143217

Table A3. Attacked firms listed on NYSE, the event refers to accident date. Model used is Fama-French Plus Momentum (final dataset)

evttime	ret m	abret m	car m	abret t	sar t	pat ar
−1	.000962865	0.001385793	0.001385793	1.33814	0.61968	0.62756
0	.000125404	−.001504651	−.000118858	−1.21411	−1.67158	−2.01811
1	.002543990	0.001922464	0.001803606	1.14785	0.20619	0.28813
2	.001451767	0.001212512	0.003016118	1.05580	1.15056	1.45262
3	.002221470	0.002660262	0.005676380	2.02323	2.56052	2.94883
evttime	**cret me**	**car me**	**patcar me**	**car te**	**scar te**	**bhar me**
−1	.007158677	.005676380	1.47537	1.98022	1.17974	.005513948
0	.007158677	.005676380	1.47537	1.98022	1.17974	.005513948
1	.007158677	.005676380	1.47537	1.98022	1.17974	.005513948
2	.007158677	.005676380	1.47537	1.98022	1.17974	.005513948
3	.007158677	.005676380	1.47537	1.98022	1.17974	.005513948

Table A4. Attacked firms listed on NASDAQ, the event refers to accident date. Model used is Fama-French Plus Momentum (counterfactual dataset)

evttime	ret m	abret m	car m	abret t	sar t	pat ar
−1	0.001495139	−0.002892	−0.002892	−0.64729	−1.54721	−1.36063
0	0.005326725	0.040037	0.037145	1.02387	0.17201	0.15229
1	−.000246444	−0.041091	−0.003946	−0.99346	0.14612	0.11156
2	−.004959142	−0.018066	−0.022011	−1.38789	−1.98680	−1.42489
3	−.002197185	0.010045	−0.011966	0.70287	−0.79493	−1.08263
evttime	**cret me**	**car me**	**patcar me**	**car te**	**scar te**	**bhar me**
−1	−.000318096	−0.011966	−1.61189	−1.29149	−1.51090	0.035219
0	−.000318096	−0.011966	−1.61189	−1.29149	−1.51090	0.035219
1	−.000318096	−0.011966	−1.61189	−1.29149	−1.51090	0.035219
2	−.000318096	−0.011966	−1.61189	−1.29149	−1.51090	0.035219
3	−.000318096	−0.011966	−1.61189	−1.29149	−1.51090	0.035219

Table A5. Attacked firms listed on NYSE, the event refers to accident date. Model used is Fama-French Plus Momentum (counterfactual dataset)

evttime	ret m	abret m	car m	abret t	sar t	pat ar
−1	−.002020508	−.001755464	−.001755464	−0.71332	−0.79725	−1.19685
0	−.004019107	−.001253760	−.003009224	−0.55752	−0.03984	−0.04609
1	0.001415861	−.000282875	−.003292100	−0.14574	−0.29999	−0.34390
2	−.005555463	−.002409014	−.005701113	−0.87363	0.11972	0.16494
3	0.000342482	0.001361291	−.004339822	0.64134	1.13661	1.19809
evttime	**cret_me**	**car_me**	**patcar_me**	**car_te**	**scar_te**	**bhar_me**
−1	−.009406003	−.004339822	−0.10009	−0.73508	−0.080877	−.003888127
0	−.009406003	−.004339822	−0.10009	−0.73508	−0.080877	−.003888127
1	−.009406003	−.004339822	−0.10009	−0.73508	−0.080877	−.003888127
2	−.009406003	−.004339822	−0.10009	−0.73508	−0.080877	−.003888127
3	−.009406003	−.004339822	−0.10009	−0.73508	−0.080877	−.003888127

Table A6. Not attacked firms listed on NASDAQ, the event refers to accident date. Model used is Fama-French Plus Momentum (counterfactual dataset)

evttime	ret m	abret m	car m	abret t	sar t	pat ar
−1	−.007015075	−.008598629	−.008598629	−1.94706	−1.89497	−1.99761
0	0.001093382	0.001064902	−.007533728	0.15213	0.67423	1.40994
1	0.005627817	0.005009357	−.002524371	1.19084	1.02426	0.97078
2	−.000159794	0.001157183	−.001367188	0.43974	0.40960	0.32236
3	0.008943261	0.007006896	0.005639709	1.29302	1.35185	2.34046
evttime	**cret_me**	**car_me**	**patcar_me**	**car_te**	**scar_te**	**bhar_me**
−1	.008326113	.005639709	1.36219	0.48030	0.85466	.005044933
0	.008326113	.005639709	1.36219	0.48030	0.85466	.005044933
1	.008326113	.005639709	1.36219	0.48030	0.85466	.005044933
2	.008326113	.005639709	1.36219	0.48030	0.85466	.005044933
3	.008326113	.005639709	1.36219	0.48030	0.85466	.005044933

Table A7. Not attacked firms listed on NYSE, the event refers to accident date. Model used is Fama-French Plus Momentum (counterfactual dataset)

evttime	ret m	abret m	car m	abret t	sar t	pat ar
−1	−.003828827	−.002820132	−.002820132	−0.75995	−0.77436	−0.85676
0	−.000940209	0.005925576	0.003105444	2.12455	2.53041	3.29490
1	−.005157067	−.005450440	−.002344995	−1.70176	−1.38232	−1.90137
2	−.007548999	−.002166972	−.004511967	−0.62110	−0.20235	−0.25365
3	−.002510038	−.000488546	−.005000514	−0.17120	−0.19428	−0.19003
evttime	**cret me**	**car me patcar me**	**car te**	**scar te**	**bhar me**	
−1	−0.019295	−.005000514	0.041628	−0.62898	0.036422	−.004466918
0	−0.019295	−.005000514	0.041628	−0.62898	0.036422	−.004466918
1	−0.019295	−.005000514	0.041628	−0.62898	0.036422	−.004466918
2	−0.019295	−.005000514	0.041628	−0.62898	0.036422	−.004466918
3	−0.019295	−.005000514	0.041628	−0.62898	0.036422	−.004466918

***Cogent Economics & Finance* (ISSN: 2332-2039) is published by Cogent OA, part of Taylor & Francis Group.**