International Review of Financial Analysis 76 (2021) 101795

Contents lists available at ScienceDirect

International Review of Financial Analysis

journal homepage: www.elsevier.com/locate/irfa

Cyber-attacks and stock market activity

Onur Kemal Tosun

Cardiff University, Aberconway Building, Cardiff CF10 3EU, United Kingdom

ARTICLE INFO

JEL codes:
G11
G14
G32

Keywords:
Security breaches
Cyber-attacks
Market activity
Long-term impact
Investors' attention

ABSTRACT

I study how financial markets react to unexpected corporate security breaches in the short and the long-term. The main results show that daily excess returns drop, trading volume increases due to selling pressure, and liquidity improves upon the public disclosure of first-time corporate hacking events. The evidence from the search frequency in Google suggests that such short-lived market reaction is due to increasing investors' attention. Cyber-attacks affect firms' policies in the long run, up to five years after the security breach announcement. These results are consistent with the hypothesis that security breaches represent unexpected negative shocks to firms' reputations.

1. Introduction and related literature

The cost of security breaches and hacking for businesses is staggering. Although detailed data are difficult to collate, the 2020 annual Cost of Data Breach Study run by the Ponemon Institute for IBM estimates that the average per-record-compromised cost of data breaches reached the all-time high of $392 million for breaches of more than 50 million records.[1] This is as much of a concern for businesses as it is for regulators; since late 2011, the Securities and Exchange Commission (SEC) has urged companies to spell out the operational and financial risks posed by cyber-attacks and to converse with investors regarding any effects on operating results, liquidity or financial position. Similarly, under the Global Data Protection Regulation (GDPR), which has become enforceable in the European Union since 25 May 2018, all organizations must report any form of data breach to supervisory authorities within 72 h, in an attempt to protect investors and citizens.

The substantial influence that security breaches have on businesses and regulators raises questions regarding the economics of information security and, ultimately, on the actual impact of hacking on targeted firms, which could be detrimental to their financial performance. As a matter of fact, the knock-on effect of a data breach can be devastating for a company's reputation, resulting in abnormal customer turnover and loss of goodwill, which in turn affect cash flows and profits. Moreover, incidents of security breaches that reveal sensitive and confidential information can not only lead to litigation and government sanctions, but also to a loss of competitive edge against same-industry competitors through a reduction of resources dedicated to R&D, dividend payments, or investments more generally. For instance, on August 27, 2014, the Federal Bureau of Investigation (FBI) contacted several media channels including Bloomberg, CNBC, the Economist, the Guardian, USA Today and CNN about a cyber-attack to JPMorgan Chase. The hackers infiltrated the network of the bank and downloaded data containing checking and savings account information. The news states that this attack is considered as one of the biggest ever.

Considering the gravity of cyber-attacks, I analyze both the short-term and the long-term market reaction to security breaches at large publicly traded US firms during the period from March 2004 to December 2019. Data is hand-collected on officially confirmed and publicly disclosed security breaches across eight different industrial sectors, along with reports and news articles corresponding to them. These 58 confirmed first announcements of security breaches are mandatory data disclosures that include stolen hardware, malware attacks, poor security or hacking, but exclude events that can be categorized as accidental release of private information or accidentally lost information.

This study adds on to the work of Akey, Lewellen, and Liskovich (2018) and Lending, Minnick, and Schorno (2018). Akey et al. (2018) exploit unexpected corporate data breaches as negative reputational shocks and show that corporate social responsibility (CSR) can provide insurance-like benefits. I examine the severity of those negative reputational shocks deeper. Particularly, I investigate the magnitude of excess returns as market reaction. Further, I analyze how strongly the

E-mail address: TosunO@cardiff.ac.uk.

[1] The full report can be found at https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

https://doi.org/10.1016/j.irfa.2021.101795
Received 8 February 2021; Received in revised form 30 April 2021; Accepted 5 May 2021
Available online 11 May 2021

investors incorporate such news on security breaches into their trading in terms of volume and direction of trading. Lending et al. (2018) study corporate governance and social responsibility as potential reasons for data breaches, and they show that socially responsible companies with smaller boards and greater financial expertise are less likely to be breached. While Lending et al. (2018) analyze firm attributes and policies potentially leading to cyber-attacks, I examine the aftermath of such attacks and how they influence firms' future policies on investments, innovation, payout, CEO remuneration, as well as, firm performance.

This paper is also related to Corbet and Gurdgiev (2019) and Kamiya, Kang, Kim, Milidonis, and Stulz (2020). Corbet and Gurdgiev (2019) examine the impact of cybercrime on equity market volatility across publicly traded corporations, and they show that target corporations are punished significantly in the form of stock market volatility. Although my study is based on cyber-attacks, it focuses on other forms of market reaction than volatility. Kamiya et al. (2020) show that cyber-attacks are more likely to occur at larger and more visible and more highly valued firms, firms with more intangible assets, and with less board attention to risk management. In this respect, they provide direct evidence that firm characteristics matter to incentivize and/or facilitate fraudulent hacking activity. Different from theirs, this paper focuses more on the pure market reaction of security breaches rather than on the reverse causality between firms' characteristics and security breaches. In other words, the goal here is not to establish what drives hacking activity and the underlying economic incentives, but rather to investigate both the short and the long-term impact on market activity and firms' fundamentals.

Although rapidly growing, the literature on the financial costs of security breaches is rather thin. Earlier papers focus on the technical aspects of security breaches, such as e-commerce (see, e.g. Kim, Tao, Shin, & Kim, 2010; Zhang, Deng, Wei, & Deng, 2012), the design of optimal security systems for software vulnerabilities (see, e.g. Liu & Zhang, 2011; Liu, Zhang, Kong, & Wu, 2012), and information security management (see, e.g. Suh & Han, 2003; Kotulic & Clark, 2004; Yeh & Chang, 2007). The vast majority of existing studies in economics related to hacking events investigate the implications in terms of information risks and optimal incentives for the design of security systems (see, e.g. Gordon & Loeb, 2002; Gordon, Loeb, & Lucyshyn, 2003; Anderson & Moore, 2006; Gordon, Loeb, & Zhou, 2011). Few papers in computer science and information management (see, e.g. Acquisti, Friedman, & Telang, 2006; Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Goel & Shawky, 2009; Spanos & Angelis, 2016) document significant negative short-term stock price reactions to corporate data breaches. In particular, Campbell et al. (2003) show that firms that experience a leak of confidential information suffer a significant drop in subsequent returns compared to firms where no confidential information is released. Similarly, Cavusoglu et al. (2004) find that announcements of security breaches are negatively associated with stock price changes within two days of the announcement date. Along the same lines, Goel and Shawky (2009) show that, on average, the announcement of a corporate security breach has a negative impact of about 1% of the firm's market value in the days after the event. Makridis and Dean (2017) study whether corporate investments change following data breaches.

In this paper, I implement both an event study and a set of difference-in-difference (DID) analyses, whereby I compare the market reaction upon security breach announcements of target firms to a group of control firms. Target firms are matched via a propensity score matching procedure at a four-digit Standard Industrial Classification (SIC) level.

The main empirical results provide strong evidence of a significant market reaction to cyber-attacks, especially in the short term. Those firms affected by security breaches exhibit significantly worse performances with respect to control firms, conditional on several fundamental variables, such as firm size, leverage, cash holdings and measures of profitability and investments. In addition, the results suggest that both traded volume and liquidity (through bid-ask spreads) tend to be significantly higher for target vs control firms at the event dates. That is, higher trading activity is matched by higher liquidity. This is confirmed by the evidence on the reaction of signed traded volume, which shows a significant sell pressure for target firms compared to non-target peers at the event date. The market reaction in terms of trading volume, liquidity, and sell pressure anticipates negative changes in stock prices which turn out to be significant and negative only the day after security breaches are publicly announced.

Delving further into the heterogeneity of the market reaction across firms, a triple DID analysis shows that larger firms with higher leverage, higher Tobin's Q, and higher operating profits tend to experience larger return drops, experience more trading, sell orders in particular, and are more liquid when they are targeted compared to smaller and less risky firms.

The underlying assumption is that data breaches increase investors' attention as they constitute an exogenous negative shock to a firm's reputation and thus future growth prospects. Indeed, the vast majority of data breaches do not directly affect products or services. Instead, they influence the firm's reputation by drawing negative attention from investors, consumers, and, more generally, stakeholders. I report the Google Search Volume Index (SVI) averaged across firms and rescaled. While the investor attention to target firms around the event date is quite evident, control firms do not show any sensible increasing investors' interest at the event date.

Firms are often reluctant to disclose security breaches because they fear that consequences of cyber-attacks may reveal sensitive and confidential information that can be damaging for those firms. I proxy private information incorporated into prices through measures of non-synchronicity (see, e.g. Chen, Goldstein, & Jiang, 2007; Ferreira, Ferreira, & Raposo, 2011; Tosun & El Kalak, 2021). Estimates from a regression analysis indicate that prices include sensitive private information at the week of the event for target firms compared to control firms. There is no evidence of transfer of private information neither before nor after the week of cyber-attack announcement for target companies. These findings validate the fear of attacked firms regarding the transmission of confidential information due to security breaches and subsequent trading that can cause further damage to those companies.

The reputational costs of a security breach likely result in persistent changes in firms' policies and operations that can only be captured by looking at the longer-term market reaction. To address this issue, I examine firms' policies, i.e. R&D expenses, dividend payments, investments, CEO compensation, CEO turnover, and firm performance. I compare the changes in these measures for target and control firms from one to five years after a hacking event.

Interestingly, the empirical results show that the impact of security breaches is weaker in the longer term. In particular, none of the performance measures experience a statistically significant change following security breaches. On the contrary, CEO compensation, R&D expenses and dividend policies significantly react to hacking events for target firms. These results are built on a set of theoretical models (see, e.g. Kreps, 1996; Tadelis, 1999) and extend a variety of existing empirical evidences (see, e.g. Armour, Mayer, & Polo, 2017; Karpoff, Lee, & Martin, 2008; Murphy, Shrieves, & Tibbs, 2009; Akey et al., 2018; Kamiya et al., 2020), which suggest that security breaches represent a costly negative shock to the reputation of publicly traded US firms, and therefore negatively affect investors' expectations on future cash-flows of targeted firms.

This paper contributes to the literature along two key dimensions. First, it provides a deeper empirical analysis on the daily market reaction following security breaches by investigating the changes in aggregate trading activity and liquidity, conditional on firms' characteristics. More specifically, it provides further insights, through a triple DID, on the heterogeneity of the market reaction across firms following security breaches by clustering firms according to their main risk profiles. This study shows that, indeed, the market reaction strongly depends on

leverage, size, and operating profits. Second, it provides direct evidence about the mapping between cyber-attacks, increasing investors' attention and market activity by showing that, on average, investors' attention indeed significantly increases for targeted firms around event dates.

The rest of the paper proceeds as follows. Sections 2 and 3 provide a detailed description of the data and the empirical strategy. Section 4 presents the core of the paper and discusses the main empirical results on the market reaction to first-time security breach announcements. Section 5 reports a set of further analyses. Section 6 concludes.

2. Data

2.1. Security breaches

Information on corporate data breaches from 2004 to 2019 is collected from the Privacy Rights Clearinghouse (PRC) website.[2] The PRC data includes information about firms targeted by a data breach, a short description of the type of the event and, if available, the number of records that were affected. I obtain the list of breaches concerning only publicly listed companies in the US. I manually cross-reference these events with alternative private data sources available on the internet, such as the Breach Level Index (BLI) provided by Gemalto. Additionally, I search for major hacking news in Factiva and also verify the identification with alternative non-conventional sources including blogs and social media.[3]

I focus exclusively on officially confirmed and publicly disclosed security breaches along with related reports and news articles. There are 267 cyber-attacks with "intended and known reasons" between 2004 and 2019. I keep only security breaches that include stolen hardware, malware attacks, poor security and hacking. This strict criterion shrinks the sample to 132 cyber-attack cases.[4] Among these incidents, cases that can be categorized further as accidental release of private information, fraud, or lost information are excluded. After I consider only the events that are intentional violation or infraction of a security and/or privacy policy, the number of cases drops to 65. This particularly rigid elimination process is necessary to examine the "true" cyber-attacks and their consequences on target firms without any doubts.

I identify the date of the hacking event as the date indicated in the official press release by the affected firm or in major financial newspapers and media. I cross-check the identified dates with alternative sources, such as blogs and social media.[5] Excepting a few nuances, unofficial information tends to be consistent with the official public releases. I focus uniquely on the first press appearance of a security breach incident and disregard follow-up news. That is, I aim to investigate the pure effect of first-time hacking events and disregard the follow-up news, which largely depends on consumers' and regulators' reactions and the existing law across states e.g., if a class action by consumers and/or officials is pursued. In this respect, the specific consequences of hacking events include legal litigations and features that are beyond the scope of this paper. After this last filtering, the final sample has 58 confirmed major incidents concerning publicly listed firms.

One comment is in order. Although follow-up news after security breaches are discarded, I indirectly investigate the firms' trajectories years after the event by looking at the long-term changes in fundamentals of target vs control firms. In this respect, one can plausibly consider that the effect of follow-up news is incorporated in the firm's fundamentals through time. Nevertheless, it is worth pointing out that this rationale relates to the long-term effects of follow-up news, rather than the short-term market reaction. For the latter, I only focus on first-time press releases to fully capture the effect of unexpected news on market activity.

The left panel of Fig. 1 presents the breakdown of events by four-digit SIC industries. The majority of cyber-attacked firms operate in the Electronics sector (40%). Wholesale & Retail (19%) and Banking & Finance (14%) are the next major groups of industries for target firms. While 10% of target firms are in Restaurants & Hotels, 9% operate in the Business Services sector. Communication (3%), Healthcare (3%), and Transportation (2%) are the remaining industries.

The right panel of Fig. 1 reports the frequency of data breaches over time in the sample. Consistent with existing empirical evidence and media commentaries, the number of cyber-attacks and threats has increased substantially over the last few years. In fact, some of the hacking events in the later years of the sample are particularly significant. For instance, on March 24, 2016, the news released in media including USA Today, CBS News, CNBC and Fortune was about the hacking of the Verizon customer database and the stolen contact information of more than 1.5 million customers. The news also claimed that customers' contact information appeared in an underground cybercrime forum. All Fortune 500 companies use Verizon for its cybersecurity prowess and the company also releases annual reports on avoiding cyber threats; however, this did not prevent Verizon being a victim of a massive cyber-attack.

Table 1 provides the summary statistics for key variables of targeted firms. Consistent with existing evidence (see, e.g. Kamiya et al., 2020), firms affected by data breaches are relatively large, with an average size of $66.7 billion, and highly leveraged: on average, 66%. While average cash holdings are 19% of their total assets, their average operating profits are 10%. Target firms have an average Tobin's Q of 0.57 and 55% of them pay dividends. Finally, about 45% of those firms in the sample invest in R&D, whereas the average excess stock return on the event date is slightly negative and equal to minus 90 basis points.

2.2. Firm and market data

I obtain daily data on firm stock prices, traded volume (in US dollars), and bid-ask spreads for publicly traded US firms from CRSP and yearly firm fundamentals from COMPUSTAT. Excess returns are defined as the daily log-returns in excess of the risk-free rate that is proxied by the 1 month T-Bill rate. Market activity is measured by using two different variables: the daily average traded volume in US dollars and a signed version of traded volume calculated as the product of the realized daily returns and the daily average traded volume. While the former represents a proxy for the aggregate fund flows that come into the marketplace, the latter gives a sense of the direction of trading activity. The signed traded volume takes a negative (positive) value if there is sell (buy) pressure in the market (see, e.g. Campbell, Grossman, & Wang, 1993; Llorente, Michaely, Saar, & Wang, 2002; Tosun, Eshraghi, & Muradoglu, 2021). Market liquidity is proxied by the bid-ask spreads for each trading day. Bid and ask prices are calculated as the average bid and ask within a given day rescaled by the end-of-day stock price.

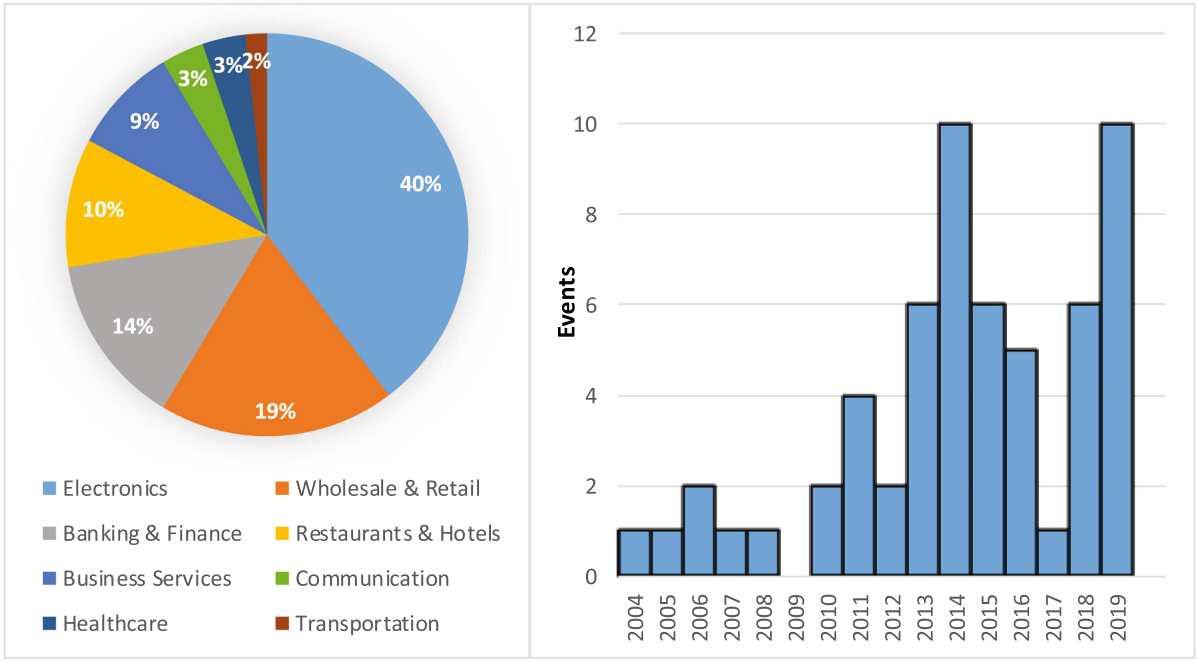
I use several aggregate risk factors, such as market risk, size, value, momentum, investment opportunities and profitability (see, e.g. Carhart, 1997; Fama & French, 2015), while investigating the effect of security breaches on excess daily returns. I obtain factor mimicking

[2] The PRC is a non-profit foundation that advocates the education of consumers on privacy protection (see https://www.privacyrights.org/ for details).

[3] Gemalto is a private organization that provides security solutions (see https://breachlevelindex.com/data-breach-database). Search words in Factiva are "data breach", "hacking", "fraud", "poor security", "security violation", "security infraction", "hacked", "stolen hardware", among others. Note that these alternative sources are primarily used for cross-referencing and auditing purposes. As an example of an alternative web source, I use information from the blog https://krebsonsecurity.com, a widely followed blog providing information on security breaches for major corporations.

[4] These numbers are consistent with previous studies, e.g. Lending et al. (2018).

[5] See, e.g., https://krebsonsecurity.com, which provides timely information on major security breaches for both private and public US corporations.



(a) Industry Distribution (b) Events

Fig. 1. Industry distribution.
This figure shows the distribution of the target firms according to their industry classification. Industry aggregation is based on the four-digit SIC codes of the existing firm at each time *t*. The 48 industry classification codes are used to construct the industries, they are obtained from Kenneth French's website. The overall sample is from March 2004 to December 2019. A detailed description of the collection of security breaches events is provided in the main paper.

Table 1
Descriptive statistics.

	Mean	St Dev.	25th	Median	75th
Firm size	10.063	1.793	8.765	10.300	11.801
Total assets (in $billion)	66.702	72.501	6.407	30.829	133.376
Leverage	0.657	0.270	0.489	0.637	0.874
Cash holdings	0.193	0.185	0.044	0.133	0.253
R&D dummy	0.446	0.502	0.000	0.000	1.000
Dividend dummy	0.554	0.502	0.000	1.000	1.000
Operating profit	0.096	0.081	0.039	0.085	0.142
Tobin's Q	0.565	0.223	0.401	0.645	0.749
Excess return at the event date	−0.009	0.028	−0.018	−0.004	0.004

This table reports descriptive statistics for the characteristics of target firms used in the main empirical analysis. The cross-sectional mean, standard deviation, and quartiles are reported for the year in which the hacking event takes place. The overall sample is from March 2004 to December 2019. *Firm Size* is the natural logarithm of total assets. *Leverage* is total liabilities over total assets. *Cash Holdings* is cash and short-term investments over total assets. *R&D* is a dummy variable that equals one if the firm invests in research and development, and zero otherwise. *Dividend* is a dummy variable that equals one if the firm pays dividends, and zero otherwise. *Operating Profit* is net cash flow over total assets. *Tobin's Q* is the market value (year-end stock price multiplied by common shares outstanding) of the firm over total assets.

portfolios that proxy for these risk factors on a daily basis from the Kenneth R. French online library.[6] I control for the aggregate market behavior by using both the value-weighted daily market returns and the total market value expressed in trillions of US dollars. To capture firms' fundamentals, I construct a set of variables: *Firm Size*, calculated as the natural logarithm of total assets; *Tobin's Q*, calculated as the market value (year-end stock price multiplied by common shares outstanding) of the firm over total assets; *Operating Profit*, calculated as net cash flow over total assets; *Leverage*, which is defined as total liabilities over total assets; *Cash Holdings*, calculated as cash and short-term investments over total assets; *R&D*, defined as a dummy variable that equals one if the firm invests in research and development, and zero otherwise, and *Dividend*, defined as a dummy variable that equals one if the firm pays dividends, and zero otherwise. These proxies are used for firms' fundamentals to construct clusters of firms for the triple DID analysis.

The long-term effect of security breaches on firms' policies is measured by using a variety of observables: *R&D Ratio*, measured as R&D expenses over total assets; *Investment*, measured as capital expenditures over total assets; *CEO Pay*, measured as CEO total compensation (in million USD) including salary, bonus, options, stocks, pensions, deferred pay and other long-term incentives; *Incentive Pay*, as the proportion of CEO pay (in million USD) including deferred pay, unearned unvested stock awards, options and stock grants. The effect on firm performance is measured by using net earnings from operating activities over total assets, i.e. *ROA*, stock price over earnings per share, i.e. *PE ratio*, and *Sales growth* measures as the annual growth rate of net sales.

3. Empirical strategy

I first test whether the disclosure of data breaches constitutes a negative shock to share prices. To do this, I analyze directly short-term stock market reactions around the public announcement of a security breach. Abnormal returns are measured using three different estimation windows, e.g., 3-, 4- and 5-month, which end 30 days before a breach is publicly disclosed. I estimate abnormal returns using a variety of different event windows: [−1, +1], [−2, +2], [−3, +3], [−3, +1], [−2, +1], [−1, +2], and [−1, +3], where the numbers refer to trading days relative to the date on which the data breach is disclosed. Expected returns are estimated using a three-factor Fama-French model, a four-factor extension including momentum and the recent five-factor specification outlined in Fama and French (2015). As is common in event study analyses, the identifying assumption is that the disclosure of a

[6] http://mba.tuck.dartmouth.edu/pages/faculty/Ken.French/data_library.html

security breach is not correlated with a firm's expected return after controlling for the tradable risk factors.

Firms subject to security breaches may inherently differ from unaffected firms in an unobservable way. Such unobserved differences can explain the market reaction upon disclosure of a security breach. For example, small firms that are likely to underinvest in data security may be more likely to be targeted by hackers and fraudulent behaviors. Although such interpretation is contradicted by the facts – large internet firms that invest hundreds of millions USD in IT security are regularly targeted by hackers – it is something that must be considered in the empirical analysis. To address this issue and provide a benchmark comparison in the analyses, I match target firms with a set of control peers by using propensity score matching for the random assignment of firms. In particular, I match firms subject to security breaches (target) with at least one (at most two) nearest neighbor firms in the sample using firm characteristics, such as firm size, Tobin's Q, and operating profits. Both target and control firms are sampled from the same four-digit SIC industry code to make sure that both firms operate in the same industry. This results in a total sample of 169 firms, 58 target and 111 control firms.

First, I use the target and control firms to examine the relationship between security breaches and the cumulative abnormal returns conditional on firms' characteristics. More specifically, I run the following regression analyses:

$$CAR_i = a + \beta_0 \,\text{Target}_i + \beta' \mathbf{z}_i + \varepsilon_i \tag{1}$$

where CAR_i represents the cumulative abnormal returns for that data breach for firm i over a given event window, $\mathbf{z}_i$ represents a vector of firm characteristics calculated over the year prior to the event, and Target_i is a dummy variable that takes value one for target firms and zero otherwise.

To better understand the causal effect of security breaches on daily excess returns, market activity and liquidity, I run a DID analysis by estimating a set of panel regressions of the form:

$$\begin{aligned} &y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t} \\ &t = \tau\text{–}180, \ldots, \tau + 180 \end{aligned} \tag{2}$$

where τ identifies the event date; $y_{i,t}$ represents the variable of interest, i.e. excess return, raw trading volume, signed trading volume, and bid-ask spread, for firm i at time t; Target_i is a dummy variable that takes value one for target firms, and zero otherwise; $\mathbf{D}_{i,\tau}$ is a $(k + 1)$-dimensional vector of daily dummy variables that takes a value of one in the interval $[\tau - k, \tau + k]$ and zero otherwise; $\mathbf{z}_{i,t}$ is a set of control variables, e.g. mimicking risk factor portfolios; and μ_i is the firm-fixed effect. k takes values between −3 and + 3. Firms need to disclose in 72 h to SEC, so τ – *3* captures if there is any leak during this period. The null hypothesis that hacking events affect the quantity of interest $y_{i,t}$ is tested based on the regression coefficients $\gamma' = (\gamma_{\tau-k}, \ldots, \gamma_{\tau}, \ldots, \gamma_{\tau+k})$, which represent the reaction of $y_{i,t}$ to a security breach for target firms vs control firms over the event window. Notice that the indicator target vs control enters only as interaction with $\mathbf{D}_{i,\tau}$ as it is subsumed by the firm-fixed effect.

The necessary identifying assumption is that there are no omitted time-varying characteristics that covary with the probability of being affected by a security breach. Yet, some firms may be more vulnerable to data breaches than others. However, I would not expect structural vulnerabilities to significantly vary over time in a predictable way over short time periods. This assumption is plausible, particularly given that information technology infrastructures are rather difficult to change and typically require long-term investments, especially for large publicly listed firms such as those in the sample.

To test the effects of data breaches on longer-term firm value, I construct an annual panel of all target and control firms from 2004 to 2019. In order to study firms in the wake of data breaches, I create an indicator variable, $Post_{i,t}$, which identifies the firm-year observations following the official disclosure of security breaches. The main specification is the following:

$$p_{i,t} = \alpha + \gamma \,\text{Post}_{i,t} + \beta' \mathbf{x}_{i,t} + \mu_i + \delta_{t+}\, \varepsilon_{i,t} \tag{3}$$

where the variable $p_{i,t}$ captures annual firm policies and operating performance such as R&D, dividend payments, investments, CEO total pay, CEO incentive pay, CEO turnover, sales growth, ROA, and PE ratio. Time-varying firm characteristics are captured by $x_{i,t}$, which controls for ln(*Assets*), Tobin's Q, cash holdings, annual stock return, and market leverage. I use three different definitions of $Post_{i,t}$ to capture responses over various time horizons. The first definition includes 1 year following a security breach. That is an indicator variable for the year the data breach occurred and the following year. The second and third definitions include three and five years following the security breach. Finally, μ_i and δ_t represent firm- and year-fixed effects, respectively. The inclusion of firm fixed effects ensures that the identification controls for any time-invariant characteristics that differ across target and control firms. The year-fixed effects ensure that the comparisons are within a given year, between target and control firms.

Delving further into the heterogeneity of the market reaction across firms, I design a triple DID analysis by constructing a firm-level indicator, x_i, which takes a value of one if the sample average of a given firm's characteristic is above the cross-sectional median and zero otherwise, such that:

$$\begin{aligned} &y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i \times x_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t} \\ &t = \tau\text{–}180, \ldots, \tau + 180 \end{aligned} \tag{4}$$

Clusters are constructed based on size, leverage, Tobin's Q and operating profits. Similar to Eq. (2), $y_{i,t}$ represents the variable of interest, i.e. excess return, raw trading volume, signed trading volume, and bid-ask spread, for firm i at time t. Also, the target dummy is considered only as interaction with the other indicators as it is subsumed by the firm-fixed effect. In addition, double interaction terms as in Eq. (2) are excluded due to high collinearity with the triple interaction term.

4. Empirical results

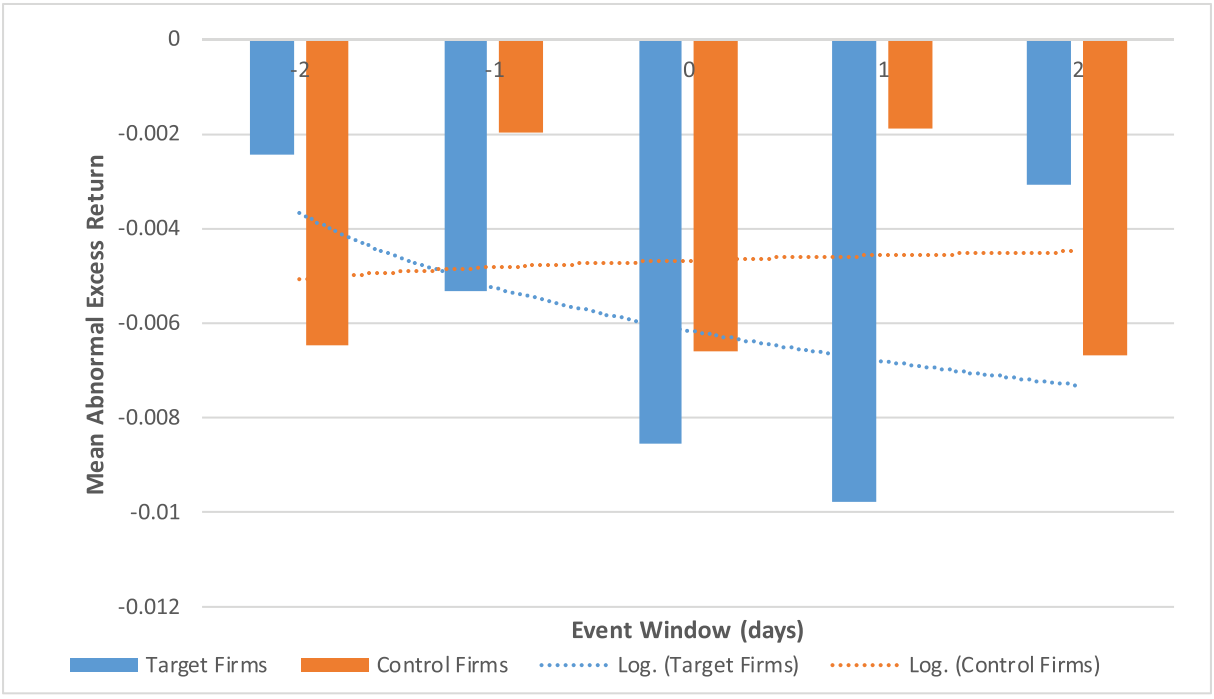
4.1. Security breaches and stock returns

Fig. 2 gives preliminary insight into the relation between abnormal excess returns and cyber-attacks. Abnormal excess returns are estimated by using both Carhart four-factor model (Panel A) and Fama-French five-factor model (Panel B). Fig. 2 presents daily abnormal excess returns for target and control firms over a five-day event window. There is a clear downward trend in the returns of target firms throughout the event window compared to control firms that have mildly upward trending abnormal excess returns. Particularly, the abnormal excess return drops to almost −100 basis points at the event date and the day after the security breach disclosure. This suggests a strong impact on firms' stock return from a cyber-attack. On the other hand, abnormal excess returns of control firms fluctuate around −60 basis points around the disclosure of hacking events.

Although instructive, the preliminary results provided in Fig. 2 are not conclusive. Table 2 shows the results of a more formal analysis in which I test the null hypothesis that daily cumulative abnormal excess returns are significantly different from zero for different lengths of the event window as well as for different specifications of conditioning risk factors.

Panel A of Table 2 shows the results for the firms affected by security breaches. Regardless of the factor model specification and the length of the event window, the cumulative abnormal returns are significant and negative, with a magnitude of −1.9% on average on a daily basis. Although they remain negative across factor model specifications, Panel B shows that the cumulative abnormal returns over the same event window are not statistically significant for control firms. This is consistent with the intuition provided by Fig. 2.

Panel A: Carhart Four-Factor



Panel B: Fama French Five-Factor

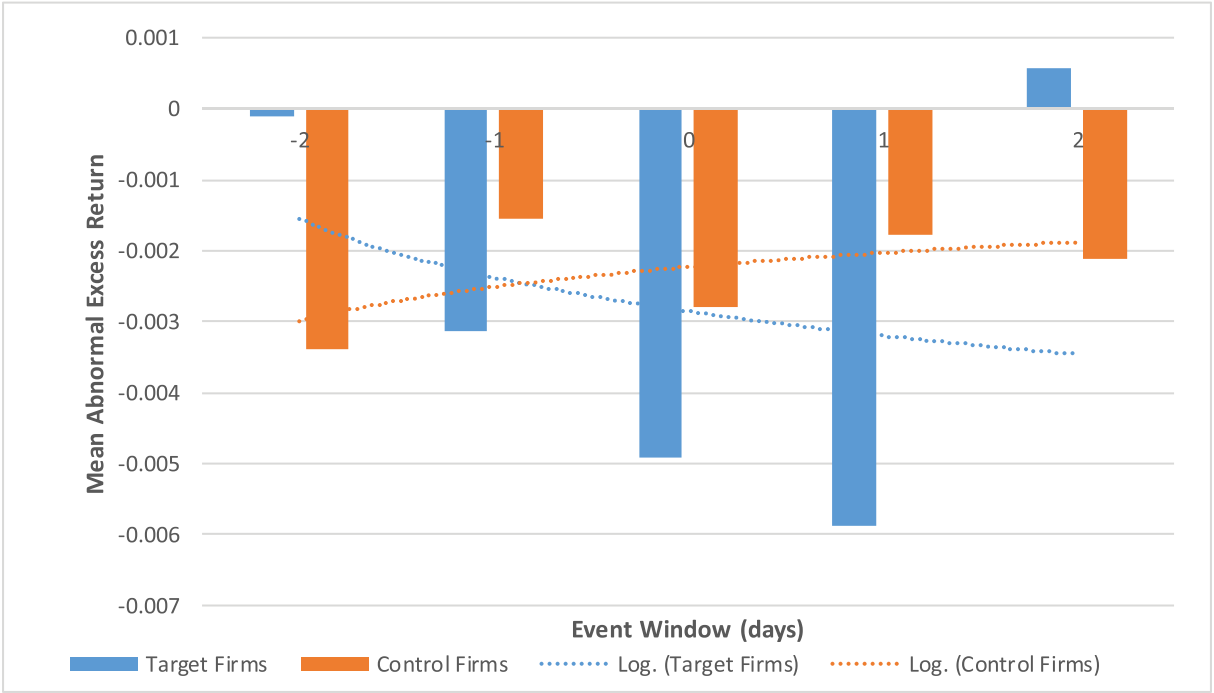


Fig. 2. Abnormal excess returns.
This figure shows the abnormal excess returns throughout the event window [−2, +2] for both firms subject to security breaches (blue bar) and peers which are matched in terms of economic fundamentals but are not subject to hacking events (orange bar). Panel A shows the results where abnormal excess returns are calculated conditional on market risk, size, value and momentum. Panel B shows the results where abnormal returns are calculated conditional on market risk, size, value, as well as mimicking portfolios for profitability and investment.
Panel A: Carhart four-factor.
Panel B: Fama French five-factor. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Table 2
Significance of the cumulative abnormal returns during the event window.

Event window	Fama French three-factor			Carhart four-factor			Fama French five-factor		
	3 months	4 months	5 months	3 months	4 months	5 months	3 months	4 months	5 months
Panel A: Target firms									
−1 to +1	−0.0204***	−0.0195***	−0.0200***	−0.0212***	−0.0202***	−0.0197***	−0.0199***	−0.0190***	−0.0190***
	(0.00544)	(0.00542)	(0.00536)	(0.00527)	(0.00514)	(0.00514)	(0.00532)	(0.00533)	(0.00529)
−2 to +2	−0.0180***	−0.0176***	−0.0168***	−0.0194***	−0.0177***	−0.0173***	−0.0163**	−0.0170**	−0.0165**
	(0.00698)	(0.00682)	(0.00690)	(0.00685)	(0.00659)	(0.00653)	(0.00696)	(0.00672)	(0.00670)
−3 to +3	−0.0172***	−0.0166***	−0.0167***	−0.0192***	−0.0179***	−0.0172***	−0.0164**	−0.0160**	−0.0151**
	(0.00641)	(0.00632)	(0.00642)	(0.00635)	(0.00621)	(0.00631)	(0.00635)	(0.00632)	(0.00637)
−3 to +1	−0.0185**	−0.0184**	−0.0181***	−0.0201***	−0.0185***	−0.0189***	−0.0183***	−0.0176***	−0.0178***
	(0.00594)	(0.00577)	(0.00580)	(0.00559)	(0.00548)	(0.00544)	(0.00580)	(0.00568)	(0.00566)
−2 to +1	−0.0200***	−0.0196***	−0.0198***	−0.0214***	−0.0204***	−0.0205***	−0.0197***	−0.0195***	−0.0195***
	(0.00549)	(0.00541)	(0.00544)	(0.00526)	(0.00515)	(0.00515)	(0.00533)	(0.00525)	(0.00525)
−1 to +2	−0.0181***	−0.0179***	−0.0172***	−0.0189***	−0.0175***	−0.0175***	−0.0165**	−0.0158**	−0.0164**
	(0.00674)	(0.00665)	(0.00668)	(0.00665)	(0.00655)	(0.00649)	(0.00669)	(0.00671)	(0.00661)
−1 to +3	−0.0191***	−0.0183***	−0.0178***	−0.0207***	−0.0187***	−0.0180***	−0.0171***	−0.0170***	−0.0166***
	(0.00602)	(0.00601)	(0.00603)	(0.00603)	(0.00593)	(0.00594)	(0.00601)	(0.00604)	(0.00601)
Panel B: Control firms									
−1 to +1	−0.00440	−0.00483	−0.00455	−0.00136	−0.00117	−0.000925	−0.00487	−0.00553	−0.00533
	(0.00286)	(0.00381)	(0.00360)	(0.00386)	(0.00383)	(0.00373)	(0.00301)	(0.00395)	(0.00382)
−2 to +2	−0.00767	−0.00840	−0.00794	−0.00511	−0.00545	−0.00504	−0.00795	−0.00870	−0.00863
	(0.00486)	(0.00589)	(0.00566)	(0.00373)	(0.00382)	(0.00358)	(0.00576)	(0.00575)	(0.00562)
−3 to +3	−0.00474	−0.00593	−0.00557	0.00266	−0.000228	0.000234	−0.00545	−0.00671	−0.00687
	(0.00504)	(0.00505)	(0.00490)	(0.00571)	(0.00575)	(0.00561)	(0.00558)	(0.05611)	(0.00546)
−3 to +1	−0.00217	−0.00340	−0.00306	0.000261	0.00202	0.00238	−0.00264	−0.00409	−0.00387
	(0.00370)	(0.00370)	(0.00359)	(0.00531)	(0.00539)	(0.00530)	(0.00362)	(0.00367)	(0.00357)
−2 to +1	−0.00672	−0.00764	−0.00723	−0.00477	−0.00510	−0.00474	−0.00727	−0.00818	−0.00788
	(0.00456)	(0.00503)	(0.00486)	(0.00314)	(0.00317)	(0.00306)	(0.00536)	(0.00531)	(0.00522)
−1 to +2	−0.00538	−0.00564	−0.00528	−0.00174	−0.00145	−0.00123	−0.00557	−0.00606	−0.00614
	(0.00374)	(0.00372)	(0.00347)	(0.00414)	(0.00414)	(0.00393)	(0.00437)	(0.00437)	(0.00420)
−1 to +3	−0.00696	−0.00739	−0.00707	−0.00372	−0.00339	−0.00310	−0.00768	−0.00814	−0.00833
	(0.00447)	(0.00538)	(0.00517)	(0.00465)	(0.00449)	(0.00435)	(0.00510)	(0.00502)	(0.00587)

Next, I explore cross-sectional determinants of the market reactions reported in Table 3. The null hypothesis is that the cumulative abnormal returns can be explained by firms' characteristics rather than by security breaches, i.e., $b = 0$ in Eq. (1). Table 3 reports regressions where the dependent variable is a firm's $CAR_{i,t}$ from 1 day before to 3 days after the public disclosure of a security breach.

In Columns (1) to (3), I test whether the stock market reaction is related to firms' attributes conditional on market risk, size and value. Consistent with the findings above, I find that a negative market reaction is associated with the disclosure of a data breach by a target firm regardless of its economic fundamentals. Columns (4) to (6) show the results by including momentum in the set of risk factors used to calculate abnormal returns. Finally, Columns (7) and (9) confirm that the negative effect of data breaches cannot be explained by firms' characteristics

Table 3
Determinants of cumulative abnormal returns.

	Fama French three-factor			Carhart four-factor			Fama French five-factor		
	−1 to +1	−1 to +2	−1 to +3	−1 to +1	−1 to +2	−1 to +3	−1 to +1	−1 to +2	−1 to +3
Target	−0.0208**	−0.0168*	−0.0175*	−0.0235***	−0.0200**	−0.0207**	−0.0209**	−0.0157*	−0.0161*
	(0.00842)	(0.00948)	(0.00921)	(0.00849)	(0.00926)	(0.00912)	(0.00830)	(0.00927)	(0.00950)
Firm size	0.000675	0.000273	0.000842	−0.000368	−0.000733	−0.000723	0.000839	−0.00146	0.00129
	(0.00224)	(0.00302)	(0.00329)	(0.00197)	(0.00286)	(0.00318)	(0.00212)	(0.00299)	(0.00330)
Leverage	−0.0349	−0.0351	−0.0333	−0.0457*	−0.0528	−0.0480*	−0.0270	−0.0261	−0.0231
	(0.0263)	(0.0277)	(0.0282)	(0.0268)	(0.0362)	(0.0273)	(0.0263)	(0.0294)	(0.0303)
Cash holdings	−0.00988	−0.0311	−0.0356	−0.00824	−0.0260	−0.0327	−0.0105	−0.0254	−0.0319
	(0.0314)	(0.0354)	(0.0372)	(0.0294)	(0.0339)	(0.0372)	(0.0307)	(0.0351)	(0.0384)
R&D	−0.00314	−0.0104	0.0140	−0.000720	−0.0102	0.0133	0.00344	−0.00444	0.0218
	(0.0137)	(0.0151)	(0.0255)	(0.0123)	(0.0135)	(0.0250)	(0.0137)	(0.0151)	(0.0258)
Dividend	−0.00613	−0.00958	−0.00504	−0.000143	−0.001346	0.00121	−0.00915	−0.0129	−0.00969
	(0.00663)	(0.0116)	(0.0122)	(0.0843)	(0.0121)	(0.0126)	(0.00687)	(0.0123)	(0.0132)
Operating profit	0.0505*	0.0869	0.106	0.0395	0.0586*	0.0806	0.0548*	0.0881	0.0100
	(0.0302)	(0.0569)	(0.0657)	(0.0276)	(0.0325)	(0.0596)	(0.0320)	(0.0565)	(0.0696)
Tobin's Q	−0.0691	−0.0847	−0.0515	−0.0733*	−0.0971	−0.0651	−0.0629	−0.0792	−0.0455
	(0.0428)	(0.0519)	(0.0450)	(0.0376)	(0.068)	(0.0438)	(0.0397)	(0.0515)	0.0455)
Observations	169	169	169	169	169	169	169	169	169
Adj. R^2	0.266	0.282	0.260	0.294	0.301	0.267	0.280	0.299	0.277

This table reports the results of the following OLS regression
$CAR_i = a + \beta_0 \cdot \text{Target}_i + \beta' \mathbf{z}_i + \in_i$
where CAR_i represents the cumulative abnormal returns over the event window for firm i, $\mathbf{z}_i$ represents a vector of firm characteristics calculated over the year prior the event, Target_i is a dummy variable that takes value one if firm i is a target and zero otherwise. Year and industry fixed effects are included. The table reports the results for cumulative abnormal returns calculated over different event windows and conditional on different risk factors. Robust standard errors are reported in parenthesis. $^*p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.

when abnormal returns are calculated conditional on Fama-French five-factor specification. Overall, the results indicate that CAR of target firms drops by about 2% compared to their peers due to the cyber-attack when other risk factors are considered. This considerable loss is also statistically significant. Interestingly, the cross-sectional regression estimates show that the negative effect has the most significance for 1 day after the public disclosure of data breaches. Although it is still negative, the coefficient on the dummy Target_i is less significant for longer periods, i.e. $[-1, +2]$ and $[-1, +3]$. Similarly, the economic impact diminishes slightly to about 1.6% for such longer periods.

I finally implement a DID analysis to disentangle the causal effect of security breaches on daily excess returns. In particular, I estimate Eq. (2) by conditioning on a set of risk factors $\mathbf{z}_{i,t}$. Table 4 reports the estimates of the regression coefficients γ', which represent the reaction of $y_{i,t}$ to a security breach for target vs control firms over the event window.

The panel regression estimates confirm a significant and negative effect of hacking events on daily excess returns. In particular, target firms lose about 88 basis points compared to control firms the day after the announcement a cyber-attack. This negative effect is stronger the day after the public disclosure of a security breach, while it is only marginally significant at the event day τ. In addition, the weak significance of $\gamma_{\tau-1}$ is encouraging regarding the identification of the event dates.

Table 4 clearly shows that the results are robust to the inclusion of firms-fixed effects and to different specifications of conditioning risk factors. As a matter of fact, the negative slope parameter $\gamma_{\tau+1}$ is strongly significant for Fama-French three-factor model, as well as, extensions that include either a momentum factor or mimicking portfolios that capture both a profitability and an investment risk factor.

4.2. Security breaches, market activity, and liquidity

I analyze how markets react to the public disclosure of first-time hacking events. More precisely, I try to establish both the magnitude and the direction, i.e. buy vs sell, of trading at the aggregate level. Table 5 shows the reaction of percentage changes (on a daily basis) of aggregate traded volume in US dollars in a seven-day window around the security breaches. As shown earlier, I report the results by conditioning on different explanatory variables that possibly affect trading volume, such as the daily returns on the market portfolio, the risk premium on the market portfolio, and the de-trended total value of the market portfolio.

Interestingly, the results show that, for targeted firms, traded volume is positively and significantly affected by security breaches only at the announcement date, while there is no relationship before and after the disclosure date. Although the adjusted R^2 remains quite low, the results hold by including firm-fixed effects. As a whole, Table 5 provides evidence that market activity significantly increases at the announcement date for firms affected by a security breach compared to firms that are not affected by hacking events. However, changes in traded volume do not give an indication of the direction of trading; that is, an increase in trading volume does not necessarily reflect buy or sell pressure on the market.

Table 6 reports the results of a DID analysis where the quantity of interest is no longer the daily changes in traded volume but a "signed" version of market activity calculated as the product between the daily average traded volume in US dollars and the daily realized returns. Such measure takes a negative (positive) value if there is sell (buy) pressure in the market (see, e.g. Campbell et al., 1993; Llorente et al., 2002; Tosun et al., 2021).

Consistent with the results in Table 5, the public announcement of security breaches affected signed traded volume only at the hacking announcement date.[7] As expected, the effect of security breaches is negative, meaning that the announcement of a security breach at time t generates a significant sell pressure at the day of announcement, consistent with the assumption that hacking events represent an exogenous negative shock to a firm's future growth prospects. Interestingly, there is neither any leakage effect nor any reaction one or 2 days ahead of the public disclosure. Recall that these results are for target vs control firms; that is, they represent the change in trading behavior of target vs control firms around the event window. As above, the estimates are robust to conditioning on different explanatory variables that possibly affect trading volume, such as the daily returns on the market portfolio, both gross and in excess of the returns on a risk-less asset, as well as, the de-trended total value of the market portfolio.

I further explore how data breaches affect the daily average bid-ask spread normalized by the daily closing price. Table 7 shows the results of a DID analysis as in Eq. (2) where the dependent variable is the normalized bid-ask spread.

The results show that liquidity through bid-ask spread increases at the announcement date for target firms, meaning that the coefficient γ_τ is negative and significant. Such an effect is limited to the date of public disclosure while there is no evidence of both subsequent market reactions or leakage effects. The results hold by controlling for different market variables as above and by including firm-fixed effects.

Table 8 extends the DID analysis by explicitly introducing a further layer of heterogeneity. In particular, I construct an indicator that separates firms into two clusters according to their economic fundamentals. This allows two kinds of potentially confounding effects to be controlled for – namely, firms' characteristics and non-random selection of firms affected. In addition, a triple DID allows a further exploration of the heterogeneous effect of security breaches conditional on firms' fundamentals. Table 8 shows the results by conditioning of firms through size, leverage, Tobin's Q and operating profits.

A few interesting aspects emerge. Panel A shows the results for the excess returns and the bid-ask spread. The negative reaction of returns and bid-ask spread is largely confirmed around the event dates. In addition, Column (1) suggests that larger firms tend to experience larger negative drops in returns than smaller firms. Indeed, the coefficient on the triple interaction term is negative and significant for the day after the announcement of a security breach. Similarly, firms with higher leverage, higher Tobin's Q, and higher operating profits all experience more negative returns upon hacking events. Columns (5) to (8) show that the rescaled bid-ask spread is negative consistent with the original findings. Columns (1) to (4) in Panel B show that the trading activity on larger and risky firms tends to be significantly higher than smaller and less risky firms. That is, market participants react more to security breaches that affect larger and highly leveraged firms compared to smaller and less leveraged ones. Columns (5) to (8) provide evidence that such increasing market activity tends to coincide with selling pressure.

To summarize, Tables 5–7 imply that there is a significant market reaction at the event date; in particular, there is significant selling pressure, which leads to increasing transaction volumes and liquidity through narrowing of the re-scaled bid-ask spread.[8] The trading activity of investors seems to be condensed to the day of cyber-attack announcement. This implies that market might anticipate negative changes in stock prices and investors react accordingly. As shown in Table 4, such market reaction at the announcement date leads to decreasing returns at the date following the announcement. Further, these findings indicate that market reaction to such considerable events

[7] Notice that in order to make the numbers more readable, the signed volume has been rescaled by its sample standard deviation.

[8] About one third of the cases (20 out of 58) in the sample are in 2014 and 2019. To test that the findings are not driven particularly by these cases, I exclude them and repeat the main analyses. Results stay robust.

Table 4
Security breaches and excess returns.

	Fama French three-factor			Carhart four-factor			Fama French five-factor		
$D\tau + 3 \times$ Target*i*			−0.000605			−0.00577			−0.000637
			(0.00260)			(0.00260)			(0.00258)
$D\tau + 2 \times$ Target*i*		−0.00104	−0.00104		0.00102	0.00102		0.00102	0.00102
		(0.00409)	(0.00409)		(0.00409)	(0.00409)		(0.00411)	(0.00411)
$D\tau + 1 \times$ Target*i*	−0.0088***	−0.0088***	−0.0087***	−0.0087***	−0.0087***	−0.0087***	−0.0089***	−0.0089***	−0.0089***
	(0.00325)	(0.00326)	(0.00326)	(0.00325)	(0.00325)	(0.00325)	(0.00326)	(0.00326)	(0.00326)
$D_\tau \times$ Target$_i$	−0.00642*	−0.00641*	−0.00641*	−0.00642*	−0.00641*	−0.00641*	−0.00638*	−0.00637*	−0.00637*
	(0.00352)	(0.00352)	(0.00352)	(0.00352)	(0.00352)	(0.00351)	(0.00353)	(0.00353)	(0.00353)
$D\tau - 1 \times$ Target*i*	−0.00386*	−0.00385*	−0.00385*	−0.00385*	−0.00384*	−0.00384*	−0.00381*	−0.00380*	−0.00380*
	(0.00199)	(0.00199)	(0.00199)	(0.00201)	(0.00201)	(0.00200)	(0.00199)	(0.00199)	(0.00199)
$D\tau - 2 \times$ Target*i*		0.00159	0.00159		0.00158	0.00158		0.00155	0.00155
		(0.00185)	(0.00185)		(0.00184)	(0.00184)		(0.00186)	(0.00186)
$D\tau - 3 \times$ Target*i*			0.00119			0.00118			0.000987
			(0.00211)			(0.00211)			(0.00211)
Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Control Variables	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369
Adj. R^2	0.061	0.061	0.061	0.061	0.061	0.061	0.060	0.060	0.060

This table reports the estimates of the following regression analysis:
$y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t}\ t = \tau - 180, \ldots, \tau + 180$
where τ identifies the event date, $y_{i,t}$ represents the daily returns in excess of the risk-free rate, Target$_{i,t}$ is a dummy variable that takes value one if firm *i* is a target firm and zero otherwise, $\mathbf{D}_{i,\tau}$ is a $(k+1)$-dimensional vector of dummy variables that takes value one in the interval $[\tau - k, \tau + k]$, $\mathbf{z}_{i,t}$ is a set of risk factor mimicking portfolios, and μ_i is a firm fixed effect. Control firms are matched to the target firms based on size, Tobin's Q, and operating profits via propensity score matching. Standard errors are clustered at the firm level and reported in parenthesis. $^*p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.

Table 5
Security breaches and raw trading volume.

Control variable:	Excess market return			Market return			Total market value		
$D\tau + 3 \times$ Target*i*			0.0500			0.0499			0.0495
			(0.0610)			(0.0610)			(0.0616)
$D\tau + 2 \times$ Target*i*		−0.106	−0.106		−0.106	−0.106		−0.103	−0.103
		(0.0647)	(0.0648)		(0.0647)	(0.0647)		(0.0632)	(0.0632)
$D\tau + 1 \times$ Target*i*	0.0636	0.0630	0.0632	0.0635	0.0630	0.0632	0.0608	0.0603	0.0605
	(0.0106)	(0.0106)	(0.0106)	(0.0106)	(0.0106)	(0.0106)	(0.0106)	(0.0106)	(0.0106)
$D_\tau \times$ Target$_i$	0.157**	0.156**	0.156**	0.157**	0.156**	0.156**	0.156**	0.155**	0.156**
	(0.0719)	(0.0719)	(0.0718)	(0.0719)	(0.0718)	(0.0718)	(0.0718)	(0.0717)	(0.0717)
$D\tau - 1 \times$ Target*i*	−0.0579	−0.0585	−0.0583	−0.0577	−0.0583	−0.0581	−0.0608	−0.0613	−0.0611
	(0.0372)	(0.0371)	(0.0371)	(0.0372)	(0.0371)	(0.0371)	(0.0378)	(0.0378)	(0.0378)
$D\tau - 2 \times$ Target*i*		−0.0423	−0.0421		−0.0425	−0.0423		−0.0387	−0.0385
		(0.0576)	(0.0575)		(0.0576)	(0.0575)		(0.0583)	(0.0583)
$D\tau - 3 \times$ Target*i*			0.00129			0.000951			0.00422
			(0.0638)			(0.0673)			(0.0642)
Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Control variables	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369
Adj. R^2	0.003	0.003	0.003	0.003	0.003	0.003	0.002	0.002	0.002

This table reports the estimates of the following regression analysis:
$y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t}\ t = \tau - 180, \ldots, \tau + 180$
where τ identifies the event date, $y_{i,t}$ represents the firm-specific daily (log) change in traded volume, Target$_{i,t}$ is a dummy variable that takes value one if firm *i* is a target firm and zero otherwise, $\mathbf{D}_{i,\tau}$ is a $(k+1)$-dimensional vector of dummy variables that takes value one in the interval $[\tau - k, \tau + k]$, $\mathbf{z}_{i,t}$ is a set of risk factor mimicking portfolios, and μ_i is a firm fixed effect. Control firms are matched to the target based on size, Tobin's Q, and operating profits via propensity score matching. Standard errors are clustered at the firm level and reported in parenthesis. $^*p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.

is significantly strong, yet short-lived. Finally, Table 8 provides evidence of an asymmetric reaction of market participants upon hacking disclosure depending on the size of a firm, its leverage and its growth prospects. Overall, these are interesting findings that earlier literature did not provide.

4.3. Long-term effects of security breaches

The results provided so far show that the market reaction following data breaches tends to vanish a few days after the announcement. The natural question is whether investors discount such cyber-attacks in their long-term trading with those target firms. To examine this further, I construct 1-, 3-, and 5-year CARs from the event date for the target and control firms. Abnormal returns are calculated with a three-factor Fama-French model, a four-factor extension including momentum, and the recent five-factor specification with an estimation window of 1-year prior the event. I regress these CAR measures on a binary target-firm indicator along with risk factor controls and fixed effects. Table 9 gives the results from these regressions along with the estimates of short-term excess returns from Table 4 for comparison.

As suspected, there is no evidence that cyber-attacks have a long-term impact on target firms' market value. The results suggest that in the long term investors re-evaluate their perception of target firms after their initial reaction to security breach announcements.

Although data breaches may not have a long-term impact on investors regarding target firms, that does not necessarily mean that a long-term effect on firms' policies should be ruled out. In fact, firms' fundamentals can change for a variety of reasons following a data

Table 6
Security breaches and signed trading volume.

Control variable:	Excess market return			Market return			Total market value		
$D\tau + 3 \times$ Target*i*			0.0114			0.0116			0.0112
			(0.0266)			(0.0266)			(0.0264)
$D\tau + 2 \times$ Target*i*		−0.00259	−0.00258		−0.00269	−0.00268		−0.00264	−0.00262
		(0.0271)	(0.0271)		(0.0271)	(0.0271)		(0.0272)	(0.0272)
$D\tau + 1 \times$ Target*i*	−0.0507	−0.0506	−0.0506	−0.0506	−0.0504	−0.0504	−0.0510	−0.0509	−0.0509
	(0.0321)	(0.0321)	(0.0321)	(0.0320)	(0.0320)	(0.0320)	(0.0323)	(0.0323)	(0.0323)
$D_\tau \times$ Target$_i$	−0.0622**	−0.0621**	−0.0620**	−0.0622**	−0.0621**	−0.0621**	−0.0617**	−0.0616**	−0.0616**
	(0.0293)	(0.0293)	(0.0293)	(0.0293)	(0.0293)	(0.0293)	(0.0292)	(0.0292)	(0.0292)
$D\tau - 1 \times$ Target*i*	−0.00510	−0.00500	−0.00498	−0.00504	−0.00493	−0.00492	−0.00492	−0.00481	−0.00480
	(0.0222)	(0.0222)	(0.0221)	(0.0222)	(0.0222)	(0.0222)	(0.0222)	(0.0222)	(0.0221)
$D\tau - 2 \times$ Target*i*		0.0320	0.0320		0.0320	0.0320		0.0318	0.0318
		(0.0226)	(0.0226)		(0.0227)	(0.0227)		(0.0226)	(0.0226)
$D\tau - 3 \times$ Target*i*			−0.00677			−0.00679			−0.00786
			(0.0195)			(0.0195)			(0.0194)
Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Control variables	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369
Adj. R^2	0.116	0.116	0.116	0.116	0.116	0.116	0.117	0.117	0.117

This table reports the estimates of the following regression analysis
$y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t}\ t = \tau - 180, \ldots, \tau + 180$
where τ identifies the event date, $y_{i,t}$ represents the firm-specific daily *signed* trading volume – calculated as the raw trading volume in US dollars multiplied by the contemporaneous realized returns, Target$_{i,t}$ is a dummy variable that takes value one if firm i is a target firm and zero otherwise, $\mathbf{D}_{i,\tau}$ is a $(k+1)$-dimensional vector of dummy variables that takes value one in the interval $[\tau - k, \tau + k]$, $\mathbf{z}_{i,t}$ is a set of risk factor mimicking portfolios, and μ_i is a firm fixed effect. Control firms are matched to the target based on size, Tobin's Q, and operating profits via propensity score matching. Standard errors are clustered at the firm level and reported in parenthesis. Notice signed volume is rescaled by its unconditional volatility for the ease of readability. $^*p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.

Table 7
Security breaches and the bid-ask spread.

Control variable:	Excess market return			Market return			Total market value		
$D\tau + 3 \times$ Target*i*			−0.00501			−0.00500			−0.00352
			(0.00501)			(0.00501)			(0.00507)
$D\tau + 2 \times$ Target*i*		−0.00297	−0.00301		−0.00300	−0.00305		−0.00505	−0.00509
		(0.00483)	(0.00486)		(0.00483)	(0.00483)		(0.00426)	(0.00427)
$D\tau + 1 \times$ Target*i*	−0.00513	−0.00513	−0.00518	−0.00511	−0.00511	−0.00515	−0.00510	−0.00509	−0.00513
	(0.00510)	(0.00510)	(0.00511)	(0.00508)	(0.00508)	(0.00510)	(0.00507)	(0.00507)	(0.00509)
$D_\tau \times$ Target$_i$	−0.00512*	−0.00512*	−0.00516*	−0.00511*	−0.00511*	−0.00516*	−0.00518*	−0.00517*	−0.00521*
	(0.00297)	(0.00297)	(0.00297)	(0.00297)	(0.00297)	(0.00298)	(0.00302)	(0.00302)	(0.00303)
$D\tau - 1 \times$ Target*i*	−0.000920	−0.000921	−0.000964	−0.000893	−0.000894	−0.000938	−0.00196	−0.00165	−0.00162
	(0.00604)	(0.00604)	(0.00605)	(0.00604)	(0.00604)	(0.00605)	(0.00598)	(0.00598)	(0.00599)
$D\tau - 2 \times$ Target*i*		0.00272	0.00267		0.00269	0.00264		0.00408	0.00405
		(0.00690)	(0.00690)		(0.00690)	(0.00690)		(0.00733)	(0.00732)
$D\tau - 3 \times$ Target*i*			−0.00769			−0.00771			−0.00722
			(0.00520)			(0.00521)			(0.00520)
Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Control Variables	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369	55,369
Adj. R^2	0.001	0.001	0.001	0.001	0.001	0.001	0.002	0.002	0.002

This table reports the estimates of the following regression analysis
$y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t}\ t = \tau - 180, \ldots, \tau + 180$
where τ identifies the event date, $y_{i,t}$ represents the daily bid-ask spread normalized by the closing price, Target$_{i,t}$ is a dummy variable that takes value one if firm i is a target firm and zero otherwise, $\mathbf{D}_{i,\tau}$ is a $(k+1)$-dimensional vector of dummy variables that takes value one in the interval $[\tau - k, \tau + k]$, $\mathbf{z}_{i,t}$ is a set of risk factor mimicking portfolios, and μ_i is a firm fixed effect. Control firms are matched to the target based on size, Tobin's Q, and operating profits via propensity score matching. Standard errors are clustered at the firm level and reported in parenthesis. $^*p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.

breach. The risk of being hacked effectively represents a reputational risk, with consequences that span from increasing operating, capital or regulatory costs, to a reduction in firms' profitability and revenues. In this respect, the reputational damage can be internalized in firms' policies, which will possibly have long-term consequences. As a result, it is worth comparing policies and operating performance of target firms to the ones of their peers. In particular, I examine the reaction to a security breach for target vs control firms' fundamentals over 1, 3 and 5 years following the public disclosure.

Firms' policies are approximated by using *R&D* ratio, measured as R&D expenses over total assets; *Dividend* payments, measured as a dummy variable that takes a value of one if a firm payed dividends over the last fiscal year and zero otherwise; *Investment*, measured as capital expenditures over total assets; *CEO Pay*, measured as CEO total compensation in million USD including salary, bonus, options, stocks, pensions, deferred pay and other long-term incentives; *Incentive Pay*, measured as the proportion of CEO pay in million USD including deferred pay, unearned unvested stock awards, options and stock grants; and *CEO Turnover*, measured as a dummy variable that is equal to one if the CEO is fired the year a security breach takes place, and zero otherwise. On the other hand, firm performance is captured by using *Sales Growth*, measured as the annual growth rate of net sales; *ROA*, measured as net earnings from operating activities over total assets; and *PE Ratio*, measured as stock price over earnings per share. I further control in the regression for firm size, leverage, Tobin's Q, cash holdings, and stock returns due to their potential effect on firms' policies. The regression

Table 8
Triple difference-in-difference analysis.

Panel A:	Excess returns				Bid-ask spread			
x_i:	Size	Leverage	Tobin's Q	Op. Profit	Size	Leverage	Tobin's Q	Op. profit
$D\tau + 3 \times$ Targeti $\times x_i$	−0.0000525	−0.00152	0.00121	−0.00865	−0.000556	−0.00922	−0.00691	−0.0237
	(0.000236)	(0.00341)	(0.00473)	(0.0241)	(0.000450)	(0.00645)	(0.00723)	(0.0303)
$D\tau + 2 \times$ Targeti $\times x_i$	0.0000641	0.00113	0.00170	0.0200	0.000328	−0.00347	−0.00537	−0.00571
	(0.000367)	(0.00459)	(0.00768)	(0.0397)	(0.000510)	(0.00771)	(0.00633)	(0.0291)
$D\tau + 1 \times$ Targeti $\times x_i$	−0.000854***	−0.00938**	−0.0143**	−0.0581***	−0.000432	−0.00705	−0.00690	0.00207
	(0.000313)	(0.00429)	(0.00654)	(0.0215)	(0.000535)	(0.00733)	(0.00740	(0.0354)
$D_\tau \times$ Target$_i \times x_i$	−0.000586*	−0.0117*	−0.0132*	−0.0220	−0.000598***	−0.00664*	−0.00407	−0.0232
	(0.000299)	(0.00606)	(0.00763)	(0.0164)	(0.000290)	(0.00383)	(0.00406)	(0.0192)
$D\tau - 1 \times$ Targeti $\times x_i$	−0.000354*	−0.00678*	−0.00513	−0.000575	−0.000232	−0.00111	0.000516	−0.0333
	(0.000191)	(0.00371)	(0.00364)	(0.0149)	(0.000558)	(0.00915)	(0.00995)	(0.0254)
$D\tau - 2 \times$ Targeti $\times x_i$	0.000148	0.00203	0.00499	0.0200	0.000231	0.00432	−0.000574	−0.0385
	(0.000196)	(0.00289)	(0.00305)	(0.0133)	(0.000705)	(0.0103)	(0.00768)	(0.0272)
$D\tau - 3 \times$ Targeti $\times x_i$	0.0000976	0.00176	−0.00081	−0.0147	−0.000771*	−0.0119	−0.0109	−0.00883
	(0.000189)	(0.00344)	(0.00335)	(0.0133)	(0.000433)	(0.00757)	(0.00752)	(0.0243)
FE and controls	YES	YES	YES	YES	YES	YES	YES	YES
Observation	54,728	54,728	54,728	54,728	50,944	50,944	50,944	50,944
Adj. R^2	0.061	0.061	0.061	0.061	0.001	0.001	0.001	0.001

Panel B:	Raw volume				Signed volume			
x_i:	Size	Leverage	Tobin's Q	Op. Profit	Size	Leverage	Tobin's Q	Op. profit
$D\tau + 3 \times$ Targeti $\times x_i$	0.00386	0.0686	0.0642	0.714	0.00181	0.0180	0.0290	0.0221
	(0.00603)	(0.0975)	(0.105)	(0.715)	(0.00270)	(0.0338)	(0.0450)	(0.254)
$D\tau + 2 \times$ Targeti $\times x_i$	−0.00732	−0.0931	−0.167	−0.0702	−0.000047	0.00495	−0.0161	−0.0213
	(0.00607)	(0.0821)	(0.112)	(0.435)	(0.000284)	(0.0292)	(0.0550)	(0.339)
$D\tau + 1 \times$ Targeti $\times x_i$	0.00391	−0.00910	0.0826	−0.0555	−0.00497	−0.0364	−0.0943	−0.379
	(0.00958)	(0.143)	(0.194)	(0.691)	(0.00357)	(0.0420)	(0.0572)	(0.257)
$D_\tau \times$ Target$_i \times x_i$	0.0148**	0.213*	0.289**	0.782	−0.00587**	−0.0983**	−0.117**	−0.343*
	(0.00728)	(0.114)	(0.128)	(0.596)	(0.00290)	(0.0468)	(0.0565)	(0.207)
$D\tau - 1 \times$ Targeti $\times x_i$	−0.00561	−0.105	−0.0743	−0.404	−0.000498	−0.0179	0.000321	0.138
	(0.00370)	(0.0752)	(0.0633)	(0.321)	(0.00253)	(0.0261)	(0.0432)	(0.212)
$D\tau - 2 \times$ Targeti $\times x_i$	−0.00297	−0.117	0.0129	0.129	0.00342	0.0211	0.0679*	0.404*
	(0.00596)	(0.0873)	(0.0871)	(0.501)	(0.00258)	(0.0297)	(0.0407)	(0.210)
$D\tau - 3 \times$ Targeti $\times x_i$	−0.000690	0.0601	−0.0565	0.366	−0.000613	−0.00206	−0.0306	−0.0625
	(0.00633)	(0.108)	(0.0937)	(0.483)	(0.00197)	(0.0219)	(0.0372)	(0.155)
FE and controls	YES	YES	YES	YES	YES	YES	YES	YES
Observation	50,837	50,837	50,837	50,837	54,199	54,199	54,199	54,199
Adj. R^2	0.002	0.002	0.002	0.002	0.118	0.118	0.118	0.118

This table reports the estimates of the following regression analysis:
$y_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i \times \mathrm{x}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t}\ t = \tau - 180, \ldots, \tau + 180$
where τ identifies the event date, $y_{i,t}$ represents the quantity of interest, Target$_{i,t}$ is a dummy variable that takes value one if firm i is a target firm and zero otherwise, $\mathbf{D}_{i,\tau}$ is a $(k+1)$-dimensional vector of dummy variables that takes value one in the interval $[\tau - k, \tau + k]$, x_i is a dummy variable that takes value one if the average value of the given characteristic for firm i is above the cross-sectional median, and $\mathbf{z}_{i,t}$ is a set of risk factor mimicking portfolios, and μ_i is a firm fixed effect. Panel A reports the results for the daily return in excess of the risk free rate and the normalized bid-ask spread. Panel B reports the results for the daily (log) change in raw trading volume and a signed version of trading volume calculated by multiplying raw volume to the contemporaneous realized returns. Standard errors are clustered at the firm level and reported in parenthesis. $^*p < 0.10$, $^{**}p < 0.05$, $^{***}p < 0.01$.

specification includes both year and firm-fixed effects as shown in Eq. (3).

Panel A of Table 10 shows the estimation results for the first set of firms' policy variables. Although positive, the long-term effects of security breaches on investment are not significant. On the other hand, the impact on cash-flow payments, i.e. dividends, and R&D expenses are negative and significant in the longer term, i.e. up to five years after the security breach. These findings confirm that the effect of a security breach can be deteriorating and persistent, consistent with the results in Kamiya et al. (2020). In particular, they show that, after a security breach, firms tend to experience a deterioration in credit ratings while they issue more debt and increase leverage after a cyber-attack. As a result of low credit ratings and high leverage, firm risk, i.e. the risk of financial distress and bankruptcy, could increase. To alleviate the increased risk, firms can decide to accumulate cash due to its cushion effect through keeping external funds, and cutting dividends and secondary investments such as R&D. That is supported by these results.

I find a decrease in R&D in the long run, while cyber-attacks do not significantly affect primary investments measured by capital expenditures. The negative link between R&D and increased risk through a negative shock is consistent with Nanda and Nicholas (2014). They show that R&D expenses in firms drop after a negative shock, such as the Great Depression or the 2008 Financial Crisis, which increases firm risk. Similar to the cuts in R&D, these findings indicate that firms reduce dividend pay-outs in the long term to manage increased risk. As far as the results for dividends are concerned, the evidence is consistent with Bliss, Cheng, and Denis (2015) which show how firms tend to pay lower dividends when operating in highly volatile environments, such as during the 2008 Financial Crisis.

Interestingly, Panel B shows that, for target firms, both CEO total pay and incentive pay tend to increase several years after a security breach compared to control firms.[9] This result is consistent with the idea that the average firm response to a data breach is investing more in the management to address possible structural issues and flaws, as well as, keeping the integrity of the firm in response to the reputational loss. As a matter of fact, Panel B shows there is no evidence of a higher propensity

[9] In untabulated analyses, I obtain similar and robust results when these CEO pay measures are constructed through natural logarithm.

Table 9
Short-term and long-term market reaction to security breaches.

	Carhart four-factor				Fama French five-factor			
	Excess Return	CAR (1-year)	CAR (3-year)	CAR (5-year)	Excess return	CAR (1-year)	CAR (3-year)	CAR (5-year)
$Target_i$		0.640	3.634	8.667		0.606	3.518	8.097
		(0.682)	(3.608)	(8.041)		(0.660)	(3.578)	(7.685)
$D_{\tau+3} \times Target_i$	−0.00577				−0.000637			
	(0.00260)				(0.00258)			
$D_{\tau+2} \times Target_i$	0.00102				0.00102			
	(0.00409)				(0.00411)			
$D_{\tau+1} \times Target_i$	−0.0087***				−0.0089***			
	(0.00325)				(0.00326)			
$D_{\tau} \times Target_i$	−0. 00641*				−0.00637*			
	(0.00351)				(0.00353)			
$D_{\tau-1} \times Target_i$	−0.00384*				−0.00380*			
	(0.00200)				(0.00199)			
$D_{\tau-2} \times Target_i$	0.00158				0.00155			
	(0.00184)				(0.00186)			
$D_{\tau-3} \times Target_i$	0.00118				0.000987			
	(0.00211)				(0.00211)			
Fixed effects	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES
Adj. R^2	0. 061	0.267	0.215	0.296	0.060	0.268	0.214	0.295

This table reports estimates of short-term excess returns from Table 4 and long-term CARs. Carhart Four-Factor and Fame French Five Factor models are used with an estimation window of 1-year. $Target_i$ is a dummy variable that takes value one if firm *i* is a target firm, and zero otherwise. Control firms are matched to the target firms based on size, Tobin's Q, and operating profits via propensity score matching. For short-term estimations, the interaction of day dummies and Target dummy are included. D_τ represents the event day. The models include risk factors as control variables along with fixed effects. Standard errors are clustered at the firm level and reported in parenthesis. *$p < 0.10$, **$p < 0.05$, ***$p < 0.01$. This table reports estimates of short-term excess returns from Table 4 and long-term CARs. Carhart Four-Factor and Fame French Five Factor models are used with an estimation window of 1-year. $Target_i$ is a dummy variable that takes value one if firm *i* is a target firm, and zero otherwise. Control firms are matched to the target firms based on size, Tobin's Q, and operating profits via propensity score matching. For short-term estimations, the interaction of day dummies and Target dummy are included. D_τ represents the event day. The models include risk factors as control variables along with fixed effects. Standard errors are clustered at the firm level and reported in parenthesis. *$p < 0.10$, **$p < 0.05$, ***$p < 0.01$.

of managers being fired in target firms as opposed to control firms (see Columns (7) to (9)). Panel C indicates that there is no significant effect of hacking on firm performance in the long term.

Considering the findings that the firm cuts R&D and dividends to deal with increased risk in the post-attack period, the results suggesting an increase in incentive-based CEO pay may seem puzzling initially. One may argue if hacked firms increase the CEO incentive pay, it would induce managers' risk-taking behavior. However, Ross (2004) explicitly shows that paying the CEO more incentive-based pay does not necessarily lead to increased risk taking. That is true in particular conditions. Hence, the results regarding R&D, payout policy and CEO incentive pay should not necessarily contradict with each other.

In addition, to address legitimate concerns about the correct interpretation, I further investigate the distribution of CEO total pay of target vs control firms in the pre- and post-announcement periods. Fig. 3 shows the average annual CEO total pay for target (blue line) vs control (red line) firms in the five years after the announcement of a data breach. The post-announcement period is chosen consistent with the regression analysis.

Interestingly, the CEO total pay for target firms fluctuates by around 11.5 million USD and remains almost constant throughout the post-announcement period. Contrary to target firms, there is a downward trend in CEO total pay for control firms. In particular, the CEO total pay for peer firms drops from 10 to 8 million USD. This figure implies that, while the peers' CEOs tend to be compensated less due to the downward trend in business overall, firms experiencing cyber-attacks do not change their CEO remuneration policy and keep paying their CEOs more than what their peers pay. Table 11 reports the results of *t*-tests for the differences in the CEO total pay for target vs control firms regarding the pre- and post-announcement periods. To provide a clearer comparison, the analysis considers 5-year periods before and after the cyber-attack disclosure, excluding +/− 3 years around the announcement, i.e. (−8; −4) vs. (4; 8). The differences in millions of USD and the *p*-values of the t-tests are provided.

Consistent with the narrative outlined in Fig. 3, while the change in CEO total pay for target firms in the period after the announcement is not statistically significant, the drop in total pay is statistically significant (about 2 million USD, on average) for control firms. This finding indicates that firms once targeted by hacking events do not substantially change their policy on CEO pay; that is, the marginal increase in CEOs' compensation of target vs control firms primarily comes from the fact that CEOs of target firms tend to be paid higher than their peers.

To summarize, I find that, across a variety of specifications, firms' policies change substantially in the years following a data breach. Affected firms tend to pay lower dividends and invest less in R&D. I also find that such a response does not involve firing the management but rather investing more in the existing CEO to address potential structural concerns. However, the results reveal that there is no long-term market reaction to cyber-attacks and subsequently, firm performance tends to move much less.

5. Further analyses

At the outset of the paper, I argue that the underlying assumption is that data breaches increase investors' attention as they constitute an exogenous negative shock to a firm's reputation and thus future growth prospects. I use Google Search Volume Index to analyze this further. Google Trends provides data on search term frequency dating back to January 2004. I collect the weekly SIV for individual stocks following Da, Engelberg, and Gao (2011). As a search query, together with the company ticker symbol or official name, I include any of the following phrases: "stolen hardware", "malware attacks", "poor security", "cyber-attack", "hacking". I aggregate the search frequency around the event date from both google search and google news for "all categories, business & industrial, law & government, news". The search frequency indexes are collected for six months around the event date and averaged and rescaled so that a value of 100 identifies the highest level within the sample. In Fig. O.A.1 in Online Appendix, the spike in SVI around the event date, i.e. date 0 in the event window, for the target firms is quite evident. On the other hand, control firms do not show any increasing

Table 10
Security breaches and long-term firm fundamentals.

Panel A: Firm policies – innovation, dividend, investments

	R&D	R&D	R&D	Dividend	Dividend	Dividend	Investment	Investment	Investment
*Post*1 year	−0.00160			−0.0204			0.00202		
	(0.00193)			(0.0330)			(0.00305)		
*Post*3 year		−0.00403*			−0.0583**			0.00424	
		(0.00234)			(0.0292)			(0.00260)	
*Post*5 year			−0.00294*			−0.0632**			0.00309
			(0.00173)			(0.0270)			(0.00286)
Year & Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	1102	1042	892	1736	1633	1402	1736	1633	1402
Adj. R^2	0.077	0.066	0.048	0.033	0.056	0.064	0.101	0.103	0.091

Panel B: Firm policies - CEO Pay and CEO turnover

	CEO pay	CEO pay	CEO pay	Incentive pay	Incentive pay	Incentive pay	CEO turnover	CEO turnover	CEO turnover
*Post*1 year	1.839			2.018			−0.0151		
	(2.151)			(2.144)			(0.0435)		
*Post*3 year		0.909			1.097*			−0.0285	
		(0.843)			(0.623)			(0.0260)	
*Post*5 year			2.194**			1.891**			−0.0132
			(1.064)			(0.928)			(0.0313)
Year & Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	1198	1150	998	1198	1150	998	1203	1153	1000
Adj. R^2	0.034	0.034	0.044	0.033	0.033	0.033	0.007	0.008	0.006

Panel C: Firm performance

	Sales growth	Sales growth	Sales growth	ROA	ROA	ROA	PE ratio	PE ratio	PE ratio
*Post*1 year	−0.0443			0.00565			1.008		
	(0.0327)			(0.00652)			(5.751)		
*Post*3 year		−0.0298			0.000424			−5.628	
		(0.0186)			(0.00582)			(5.507)	
*Post*5 year			−0.0143			0.00242			−9.509
			(0.0164)			(0.00670)			(6.331)
Year & Firm FE	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES
Observations	1736	1633	1402	1736	1633	1402	1736	1633	1402
Adj. R^2	0.068	0.064	0.039	0.055	0.053	0.072	0.019	0.017	0.025

This table reports the estimates of the long-term reaction of firms' fundamentals to the announcement of security breaches. The table summarizes the results for different proxies of firm policies and operating performance. It reports the regression coefficient on a dummy $Post_{i,k}$ that takes value one if the firm *i* has been targeted over the last *k* years and zero otherwise. Control firms are matched to the target based on size, Tobin's Q, and operating profits via propensity score matching. In addition, the model includes firm leverage, cash holdings, past realized stock returns as additional control variables. Standard errors are clustered at the firm level and reported in parenthesis. $*p < 0.10$, $**p < 0.05$, $***p < 0.01$.

investors' interest at the event date. Interestingly, investors seem to focus only on the day of such announcements after which their attention on target firms drops significantly. This finding provides further evidence that the interest in these events are short-lived.

I further test the assumption that security breaches increase investors' attention by estimating the following regression:

$$SVI_{i,t} = \alpha + \gamma' \mathbf{D}_{i,\tau} \times \text{Target}_i + \beta' \mathbf{z}_{i,t} + \mu_i + \varepsilon_{i,t} \quad t = \tau\text{–}26, \ldots, \tau + 26 \tag{5}$$

where τ identifies the event date, $SVI_{i,t}$ represents the standardized Google SVI index for a given firm, $\text{Target}_{i,t}$ is a dummy variable that takes value one if firm *i* is a target firm and zero otherwise, $\mathbf{D}_{i,\tau}$ is a $(k+1)$-dimensional vector of dummy variables that takes value 1 in the interval $[\tau - k, \tau + k]$, $\mathbf{z}_{i,t}$ is a set of risk factor mimicking portfolios, and μ_i is a firm fixed effect. Control firms are matched to the target based on size, Tobin's Q, and operating profits via propensity score matching. Notice the data and the dummies are weekly.

Table OA.1 in Online Appendix shows the estimation results. The results indicate that regardless of the conditioning variables the SVI significantly increases at the day of the event for target firms. This is consistent with the idea that the official disclosure of a security breach corresponds to increasing investors' attention as proxied by the search frequency on Google. It is important to note that investors' interest seems to drop the day after the announcement of cyber-attacks after which it completely disappears.

Firms are often reluctant to disclose security breaches because consequences of cyber-attacks may reveal sensitive and confidential information. Therefore, I examine further whether security breaches lead to transfer of private information as target firms fear. To measure private information incorporated into prices, I follow Chen et al. (2007), Ferreira et al. (2011), and Tosun and El Kalak (2021). First, I estimate firm-specific return variation by performing the following regression using daily data:

$$ret_{i,t} = \alpha + \beta_1 Market_{i,t} + \beta_2 Industry_{i,t} + \varepsilon_{i,t} \tag{6}$$

where *ret* is the daily return of company *i, Market* is the CRSP value weighted market index, and *Industry* is the equally weighted return of a portfolio of firms that belong in the same industry as firm *i* (3-digit SIC). For each firm-week including the week of cyber-attack announcement, firm-specific return variation is estimated by $1 - R^2$ from the regression. This is *Non-Synchronicity*. The second measure, i.e. *Ln(Non-Synchronicity Ratio)*, is defined as $\text{Ln}((1 - R^2)/R^2)$. Similar to Eq. (2), I regress these measures of private information on the interaction of target firm indicator and event week dummies, along with controls.

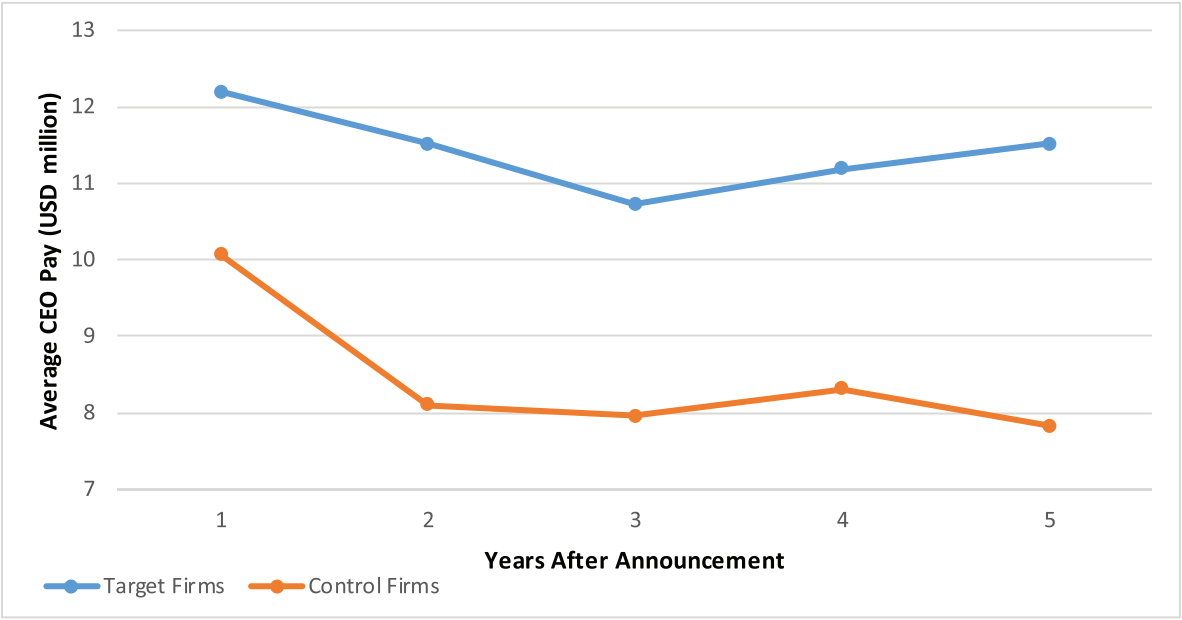


Fig. 3. Average annual CEO total pay.
This figure shows the average CEO Total Pay for target (orange line) vs control (blue line) firms after the announcement of a data breach. The post-announcement period is up to five years. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Table 11
Comparison of CEO total pay.

	Pre-announcement	Post-announcement	Difference (USD million)	*p*-Value
Target	13.968	12.219	*−1.749*	0.280
Control	10.535	8.524	*−2.010***	0.039

This table reports the T-test results for the differences in the CEO total pay between target and control firms regarding the pre- and post-announcement periods. To provide a clearer comparison, the analysis excludes +/− 3 years around the announcement. Pre-announcement period includes five years before the cyber-attack disclosure, i.e. (−8; −4), while post-announcement period has five years after such disclosure, i.e. (4; 8). The differences in million of USD and the *p*-values are provided. *$p < 0.10$, **$p < 0.05$, ***$p < 0.01$.

Table OA.2, Online Appendix shows statistically significant and positive estimates for *Non-Synchronicity* and *Ln(Non-Synchronicity Ratio)* indicating that prices include sensitive private information at the week of the event for target firms compared to control firms. It is interesting to note that there is no evidence of transfer of private information neither before nor after the week of cyber-attack announcement for target companies. These findings validate the fear of attacked firms regarding the transmission of confidential information due to security breaches and subsequent trading that can cause further damage to those companies.

As a robustness test, I exclude the repetitive cyber-attack cases of same firms because the follow-up security breaches may not generate the same market reaction as the first-time attack. Analyses on excess return, raw trading volume, signed trading volume, and bid-ask spread with this revised sample are given in Table OA.3 in Online Appendix. The results are robust and similar to the original findings.

Next, I verify that the results are not purely driven by a few industries. Panel A of Fig. 1 shows that hacking events are mostly concentrated in a couple of industrial sectors. As a result, data breaches in some industries might drive the aggregate results. To address this concern, I re-estimate Eq. (2) for top three industries regarding the changes in stock prices, market activity variables, and the normalized bid-ask spread. Tables OA.4 and OA.5 in Online Appendix confirm the negative reaction of daily excess returns across industries. The positive change in market activity, the sell pressure, and increased liquidity documented in Tables 5–7 are supported. As a whole, the findings suggest that the original results are not driven by a particular industry classification as the negative market reaction upon security breaches is largely confirmed at the industry level.

Next, I examine the robustness of the original findings to the presence of undisclosed features that affect market activity above and beyond security breaches. To address this concern I run a placebo test and re-estimate Eq. (2) at a different point in time by shifting the sample period by 30 days and re-testing for the significance of γ, ceteris paribus. That is, I keep the same exact model specifications of Section 4.1 with the only exception that I shift the event window backwards by 30 days.[10] Tables OA.6 and OA.7 in Online Appendix give the results. It is evident that for none of the days within the event window the market reaction is significantly different from zero for targeted firms compared to their peers across all analyses. This exercise provide evidence that the results of Sections 4.1 and 4.2 are not spurious; that is, the significant market reaction during the public disclosure of security breaches is most likely not contaminated by unobservable features of target firms selected that point in the same direction of hacking events.

6. Conclusion

I study how financial markets respond to unexpected fraudulent corporate security breaches both in the short term and in the long term. In particular, I investigate how daily excess returns, market activity and bid-ask spreads react in the days around the public disclosure of hacking events. In the short term, the results show that, while excess returns drop the day after the breach announcement, both the traded volume and liquidity significantly increase at the announcement date. In addition, a signed volume measure, calculated as the product of realized returns and raw traded volume suggest that short-term market activity is primarily driven by a sell off of shares. The findings show that such changes in market activity can be due to increasing investors' attention, proxied

[10] I anticipate the event window rather than postpone it in the placebo test, since it is certain that follow-up news and events will not fall within the newly defined window.

by search frequency on Google, at the public disclosure of the security breach. Further results indicate that security breaches and subsequent trading lead to transmission of confidential information about target firms into prices that can cause further damage to those companies.

In the longer term, the empirical analysis shows that, while firms' market value and performance are not significantly affected up to five years after the event, firms' policies, e.g. payout and R&D, incorporate security breaches. Target firms rely on the guidance by existing management in such troubled times, and subsequently, invest more on their CEO.

To summarize, the results are consistent with the idea that a data breach constitutes an exogenous negative shock to a firm's reputation and has considerable short-term impact on firm value and trading. The lack of long-term effect on target firms' performance can be due to firms following the lead of their CEO who they support fully, through which they address this issue properly with necessary policy change.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.irfa.2021.101795.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Akey, P., Lewellen, S., & Liskovich, I. (2018). *Hacking corporate reputations*. working paper.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*, 610–613.

Armour, J., Mayer, C., & Polo, A. (2017). Regulatory sanctions and reputational damage in financial markets. *Journal of Financial and Quantitative Analysis, 52*, 1429–1448.

Bliss, B. A., Cheng, Y., & Denis, D. J. (2015). Corporate payout, cash retention, and the supply of credit: Evidence from the 2008–2009 credit crisis. *Journal of Financial Economics, 115*, 521–540.

Campbell, J. Y., Grossman, S. J., & Wang, J. (1993). Trading volume and serial correlation in stock returns. *The Quarterly Journal of Economics, 108*, 905–939.

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*, 431–448.

Carhart, M. M. (1997). On persistence in mutual fund performance. *The Journal of Finance, 52*, 57–82.

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*, 70–104.

Chen, Q., Goldstein, I., & Jiang, W. (2007). Price informativeness and investment sensitivity to stock price. *The Review of Financial Studies, 20*, 619–650.

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis, 65*, 1–18.

Da, Z., Engelberg, J., & Gao, P. (2011). In search of attention. *The Journal of Finance, 66*, 1461–1499.

Fama, E., & French, K. (2015). A five-factor asset pricing model. *Journal of Financial Economics, 116*, 1–22.

Ferreira, D., Ferreira, M. A., & Raposo, C. C. (2011). Board structure and price informativeness. *Journal of Financial Economics, 99*, 523–545.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*, 404–410.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*, 438–457.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal, 19*, 1–16.

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*, 33–56.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. forthcoming.

Karpoff, J. M., Lee, D. S., & Martin, G. S. (2008). The cost to firms of cooking the books. *Journal of Financial and Quantitative Analysis, 43*, 581–611.

Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*, 84–95.

Kotulic, A. G., & Clark, J. G. (2004). Why there arent more information security research studies. *Information & Management, 41*, 597–607.

Kreps, D. M. (1996). Corporate culture and economic theory. In *Firms, Organizations and Contracts* (pp. 221–275). Oxford: Oxford University Press.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review, 53*, 413–455.

Liu, Q., & Zhang, Y. (2011). VRSS: A new system for rating and scoring vulnerabilities. *Computer Communications, 34*, 264–273.

Liu, Q., Zhang, Y., Kong, Y., & Wu, Q. (2012). Improving VRSS-based vulnerability prioritization using analytic hierarchy process. *Journal of Systems and Software, 85*, 1699–1708.

Llorente, G., Michaely, R., Saar, G., & Wang, J. (2002). Dynamic volume-return relation of individual stocks. *The Review of Financial Studies, 15*, 1005–1047.

Makridis, C. A., & Dean, B. (2017). *The economic effects of cyber security failures on firms: Evidence from publicly reported data breaches*. working paper.

Murphy, D. L., Shrieves, R. E., & Tibbs, S. L. (2009). Determinants of the stock price reaction to allegations of corporate misconduct: Earnings, risk, and firm size effects. *Journal of Financial and Quantitative Analysis, 43*, 581–612.

Nanda, R., & Nicholas, T. (2014). Did bank distress stifle innovation during the Great Depression? *Journal of Financial Economics, 114*, 273–292.

Ross, S. A. (2004). Compensation, incentives, and the duality of risk aversion and riskiness. *The Journal of Finance, 59*, 207–225.

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

Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. *Information & Management, 41*, 149–158.

Tadelis, S. (1999). What's in a name? Reputation as a tradeable asset. *American Economic Review, 89*, 548–563.

Tosun, O. K., & El Kalak, I. (2021). *ETFs ownership and corporate cash holdings*. Available at SSRN 3440350.

Tosun, O. K., Eshraghi, A., & Muradoglu, G. (2021). *The financial impact of corporate exposure to prior disasters*. Working Paper.

Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management, 44*, 480–491.

Zhang, Y., Deng, X., Wei, D., & Deng, Y. (2012). Assessment of E-commerce security using AHP and evidential reasoning. *Expert Systems with Applications, 39*, 3611–3623.