Should You Disclose a Data Breach via Social Media? Evidence from US Listed Companies

Pierangelo Rosati
IC4 - DCU Business School
pierangelo.rosati@dcu.ie

Peter Deeney
DCU Business School
peter.deeney@dcu.ie

Mark Cummins
DCU Business School
mark.cummins@dcu.ie

Lisa Van der Werff
DCU Business School
lisa.vanderwerff@dcu.ie

Theo Lynn
IC4 - DCU Business School
theo.lynn@dcu.ie

Abstract

Data breaches represent one of the main concerns for executives across all sectors. Data breaches open a period of crisis for the affected firm and require them to disclose complex information to a variety of stakeholders in a timely and proper manner. This paper investigates the relationship between social media disclosure of a data breach and its cost, as proxied by the response of the affected firm's stock price. Using an event study methodology on a sample of 32 data breaches from 29 US publicly-traded firms from 2011 to 2014, we find that social media disclosure exacerbates the negative stock price's response to the announcement. However, such a negative association is contingent on firm's visibility on traditional media with social media disclosure having a beneficial effect for low-visibility companies.

1. Introduction

The amount of data organizations collect, store and process for their daily activities has grown exponentially in the last few years [29]. This data usually contains valuable information that is attractive to cyber criminals. As such, firms are heavily investing in ways to protect their information systems (IS) from cyber attacks [45]. According to Privacy Rights Clearinghouse, 543 million records were lost between January 2005 and January 2012 as a consequence of 2,800 data breaches [37]. Data breaches are costly events for the affected firms and estimating such costs is challenging as they comprise largely implicit costs e.g. loss in customers' trust and brand reputation [18, 20]. Empirical researchers attempt to overcome this issue by adopting stock price reaction as a proxy [18, 20] and show that a breach may cause a loss in firm value of up to 5.5 percent [7]. Given this significant impact, it is not surprising that data breaches are a real concern for firms, investors and regulators. Regulators have tried to limit the harm of data breaches for affected individuals, investors and stakeholders by enforcing a mandatory and timely disclosure for such events. However, data breaches generate complex information and therefore how such information is disclosed, is important in this context [12, 47].

Historically, firms relied on traditional media (i.e. the press) to disseminate information [6]. But traditional media tends to focus on highly visible firms since they attract larger readership [5]. As a result, low visibility firms, which represent the largest part of the market, struggle in reaching a larger set of stakeholders through traditional media. In this context, the emergence of social media represented a structural change in corporate communication, and particularly for low visibility firms, since it offers firms the opportunity to communicate more effectively at relatively low cost.

Previous studies suggest a positive effect of social media adoption in improving customer engagement [37], constraining negative outcomes caused by product recalls [30], detecting customer complaints regarding product defects [2], increasing equity market value [42], and lowering information asymmetry [6]. Despite these advantages, some studies advise caution in how the value of social media is measured since social media per se cannot generate value without the implementation of an adequate communication strategy [25]. In addition to firms, policymakers and regulators have acknowledged the increasing importance of social media for corporate information disclosure, and have recognized it as an official communication channel [41].

Social media represents a useful communication channel in the context of a company crisis [30], which is defined as "*a specific, unexpected and non-routine event or series of events that create high levels of uncertainty and threaten, or are perceived to threaten,*

URI: http://hdl.handle.net/10125/50489
ISBN: 978-0-9981331-1-9

an organization's high priority goals" [40]. Given the unexpected nature and the extent of the potential damage, a data breach arguably fits into such a definition. Social media allows a breached firm to bypass information intermediaries and easily disseminate its intended message, potentially lowering the cost of the breach and exposure to litigation risk [36]. However, there is also a potential counter effect. Due to the virality typical of social media platforms, a company may lose control of the information flow, thereby in fact worsening an already serious situation [9, 30]. Understanding social media usage around data breaches is therefore critical for firms that suffer data breaches and this study aims to shed light on its potential contrasting impacts.

To our knowledge, this is the first study that investigates the impact of data breach disclosure via social media on stock market reaction. We therefore provide novel and important insights for management into communications strategy around data breaches. Our study also contributes to the literature on the impact of social media for crisis communication in two key ways. First, by investigating the role of social media in the context of data breach disclosure; and second, by providing unique evidence of a significant benefit to social media for low visibility firms in particular, which typically struggle in gaining attention in traditional media.

The rest of the paper is organized as follows. The next section provides a review of the essential literature while the following section presents our research hypotheses. We then describe the research design and the data collection. Finally, we present the results of the empirical analyses and the robustness tests, and conclude by discussing the implications of the study and directions for future research.

2. Background

2.1. Data breaches

A data breach is defined as an incident that involves unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data [22]. The number of IS breaches is growing every year and the increasing popularity of cloud computing, mobile devices and big data exacerbate this issue [1].

Data breaches impose both short and long term costs on the affected companies. Short-term costs are due to investigation and remediation activities, legal advisory, fines, and lost transactions. Long-term costs are related to loss of present and future revenues as well as the deterioration of customers' and partners' trust [20]. A prominent example of the cost of a data breach is ChoicePoint. In early 2006, the Federal Trade Commission (FTC) imposed a $10 million fine against ChoicePoint as a consequence of a massive data breach that involved 160,000 records; the company also agreed to pay another $5 million to compensate affected individuals [17]. Research into the economics of information security provides evidence on both determinants and deterrents, and consequences of security breaches. Investments in cyber-security [21], effective internal controls [9], adequate vendors policies [21] and external monitoring [39], users' behaviors [35], and domestic and international law enforcement [34] proved to constrain the number of security breaches. From a consequences perspective, most of the empirical research to date attempts to estimate the overall cost of breach events by adopting the change in stock price following the announcement (i.e. cumulative abnormal returns) as an appropriate proxy. This assumption is based on the semi-strong market efficiency hypothesis [15] according to which the stock price incorporates all public information and all future expected firm cash flows. However, even though empirical results, thus far, suggest a negative impact, evidence on the magnitude is mixed with price decline values ranging from 0.86 [18] to 5.5 percent [7]. Gordon et al. [22] argue that such conflicting results may be due to differences in the sample composition or in the period of analysis with more recent data breaches causing a lower negative market reaction.

A factor that significantly affects the overall costs of data breaches is the amount of time between the beginning of the breach activity and its detection as well as the time between the breach detection and its disclosure [36]. Furthermore, investigating a data breach is a complex process and often requires a significant amount of time and deep technical capabilities [8]. As a result, details about the incident may not become apparent or public for some time resulting in uncertainty during this period. Similarly, the explanation surrounding the data breach announcement may be complex. This uncertainty and complexity is likely to adversely affect the market reaction [26].

2.2. Social media

Social media represents one of the most transformative impacts of information technology and has fundamentally changed the way we communicate, collaborate, consume, and create content [13]. Social media research is still at an early stage of conceptualization and due to the rapid evolution of

social media platforms, a degree of definitional ambiguity exists. Lynn et al. [31] suggest that there are three definitional perspectives – the application view, the communication view and the integrative view. For the purposes of this paper, we use the integrative view. From this perspective, social media is defined as both the conduits and the content disseminated through interactions between individuals and organizations [28]. As such, it includes a set of web-based and mobile tools and applications that allow users to create (consume) content that can be consumed (created) by others and which enables and facilitates connections [24].

Social media allows firms to overcome one of the main limitations of traditional media (e.g. newspapers): limited coverage [10]. Media coverage is often related to size, with larger firms having higher visibility and greater access both to media outlets and their audiences [9]. Network (and audience) accessibility combined with the ability for users to generate and share content distinguishes social media and traditional media [30]. Social media allows both large and small firms to directly engage with end-consumers in an efficient way [27]. However, social media represents a challenge from a firm perspective since messages can be propagated, attenuated, and amplified by users themselves [3]. This requires a shift in a firms' communication strategy as well as adequate resources invested in managing social media [19].

Academic research on the impact of corporate disclosures via social media on the stock market has grown in recent years. Many studies focus on Twitter since it is the most commonly adopted for social investor communication and company event disclosure [6, 25]. Compared to other widely adopted social media platform (e.g. Facebook), Twitter has the peculiarity of being a largely open network and it also has the unique feature of 'retweeting', which makes it a powerful mechanism for information sharing [28].

Empirical studies on the impact of Twitter on stock market suggest that the emotionality [49] and sentiment [43] of tweets affect stock market returns, and that additional dissemination of firm-initiated news via Twitter is associated with lower information asymmetry [6].

More recently, studies have begun to investigate the impact of social media around specific scheduled events such as earnings announcements [25, 44, 47], while Lee et al. [30] investigate the economic impact of social media in the context of a company crisis. The authors adopt product recalls as an example of company crisis and their findings suggest that the disclosure of the recall through Twitter mitigates the negative price reaction when the recalling firm can control the information flow. Like product recalls, data breaches represent firm crises, which expose affected firms to a number of potential negative consequences. As such, they contrast with many corporate events where there are varying degrees of expectations and provide an ideal setting to examine the role of social media usage as a firm communication channel. Despite these similarities, product recalls and data breaches differ in terms of number of occurrences and number of people affected, with data breaches typically affecting a larger number of organizations and individuals than product recalls[1]. Furthermore, the increasing complexity and pervasiveness of data breaches, as well as the lack of a clear guidance for their disclosure[2], make managers consider data breaches more concerning than product recalls because of the combination of higher likelihood and potential damages [36].

3. Hypotheses development

Disseminating information around a breach event quickly is a requirement under compliance with the Security Breach Notification Laws (SBNLs). Although the disclosure of a data breach is mandatory, the communication of the event on social media is voluntary. Firms are likely to use voluntary disclosure to share positive news while they are more reluctant to voluntarily disclose bad news both on traditional [32] and social media [14]. Since a data breach is bad news, and with this bad news being broadcast to a wide audience using social media, we expect the negative price reaction to the announcement to be larger if a firm discloses the event through its social media account. Our first hypothesis is therefore stated as follows:

H1: The disclosure of data breaches on social media increases the negative stock price reaction to data breach announcements.

As discussed in the previous section, traditional media accommodates high visibility firms, while low visibility firms struggle in reaching a large audience with their company specific news [5]. This may be particularly detrimental when information has to be disclosed quickly, as in the case for data breach events.

[1] Privacy Rights Clearinghouse reports 2,197 data breaches from 2011 to 2014 while the Consumer Product Safety Commission

[2] While product recalls in the US have been regulated nation-wide since 1972 (Consumer Product Safety Act), a unique regulation for data breach disclosure is still missing. Since 2002, when the first SBNL was enacted California, 47 states Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted their own SNBLs [33]. However, SBNLs still significantly differ from each other creating uncertainty in terms of disclosure requirements [46].

The risk is that low visibility firms, though they detect the breach quickly, cannot disseminate the event information effectively because they do not command enough attention in traditional media and, therefore, face larger relative damage. Social media levels the playing field somewhat by providing low visibility firms direct access to a potentially wider audience and a greater prospect of market attention than would otherwise be possible [30]. As such, it provides the affected firm with an opportunity to disclose data breach event information in a more effective manner. Given this important innovation provided by social media, we test whether there is a difference in market reaction between high and low visibility firms. Our contention is that, in contrast to high visibility firms, low visibility firms benefit from having the level of market attention afforded by its social media presence, over and above the case of either no traditional media or very limited traditional media news coverage. For high visibility firms, a social media presence simply adds to an already established level of market attention. We therefore state our second hypothesis as follows:

H2: The disclosure of data breaches on social media by low visibility firms decreases negative stock price reaction to data breach announcements.

4. Research methodology

In this study we adopt an event study methodology based on the efficient market theory which states that new information in the market will fully reflect in a firm's stock price [15]. Because the market should not be capable of anticipating when firms will make a data breach announcement, it is appropriate to use the event methodology to catch unexpected business events in the stock market [11].

The following regression model is used to test our research hypotheses:

$$CAR_{i,j} = \alpha_0 + \alpha_1 TweetEvent_{i,j} + \alpha_2 Low_{i,j} + \alpha_3 TweetEvent_{i,j} \times Low_{i,j} + \alpha' Controls_{i,j} + \varepsilon_{i,j} \quad (1)$$

The dependent variable in Eq. (1) is the cumulative abnormal return (*CAR*) over a two- (0;+1) or three-day (0;+2) period starting on the announcement day (hereafter, the event period) [18]. We adopt the market model [14] to estimate daily abnormal returns (ARs) and then sum up the daily ARs over the event period to obtain the cumulative abnormal returns (CARs), which is proxy for price reaction to the announcement [7, 18]. The market model equation is as follows:

$$R_{i,t} - RF_t = \alpha_i + \beta_i (RM_t - RF_t) + \varepsilon_{i,t} \quad (2)$$

where $R_{i,t}$ is the stock return for firm i on day t; RF_t is the risk-free interest rate on day t; RM_t is the stock return of market on day t; α_i is Jensen's alpha for firm i; β_i is the Capital Asset Pricing Model's slope parameter for firm i (i.e., the systematic risk of the return of firm i, relative to the return of the entire market, and often denoted as the beta of the stock); and ε_{it} is the model's error term.

To capture the effect of a data breach disclosure on social media on price reaction, we adopt two indicator variables (i.e. *TweetEvent* and *Low*) and the interaction variable between them. *TweetEvent* is a dummy variable equal to 1 if a firm disclosed a data breach through its active Twitter account and 0 otherwise. We classify the firms in our sample as low visibility (*Low*) if the average daily number of newspaper articles during the estimation period was below the first tercile threshold. The interaction variable (*Twitter x Low*) allows us to explore if there is a difference in the communication use of Twitter in data breach disclosure for low visibility firms relative to high visibility firms. The regression coefficient of *TweetEvent* tests H1, while the regression coefficient of the interaction variable tests H2.

Our models include four categories of control variables: (a) controls for breach characteristics; (b) controls for traditional media activity; (c) controls for social media activity; and (d) controls for firm characteristics.

The cost of a data breach, and, therefore, the market reaction to the announcement, depends on the breach type, the number of records breached, and the occurrence of previous breaches [5, 6]. Thus, our model includes seven dummy variables identifying six different breach types as reported by the Privacy Rights Clearinghouse[3]: (a) a payment card fraud (*Card*), (b) an unintended information disclosure (*Disc*), (c) an attack by a hacker (*Hack*), (d) an insider misbehavior (*Insd*), (e) a lost, discarded or stolen portable device (*Port*), and (f) an unknown reason (*Unkn*)[4]; and two dummy variables, *RecordsKnown* and *PriorBreach*, indicating whether a firm disclosed the exact number of breached records or whether it had suffered previous breach(es) before respectively.

A control variable for traditional media activity (*ATMedia)* was constructed as suggested by Lee et al. [11].

$$ATMedia_{i,j} = \frac{TMedia_{i,j} - NTMedia_{i,j}}{NTMedia_{i,j}} \quad (3)$$

[3] https://www.privacyrights.org/node/1398.

[4] The Privacy Right Clearinghouse classification includes two more breach categories i.e. physical loss (Phys) and stationary device (Stat). Since none of the events in our sample fall into these categories, we do not create any indicator variable for them.

Where *TMedia* is the average daily number of newspaper articles during the event period (0;+1) while *NTMedia* is the average daily number of newspaper articles during a 120-day estimation period ending five days before the event (-125;-6). This variable provides a measure of the abnormal attention a firm attracts around a data breach announcement.

Control variables for social media activity include a variable to control for a firm Twitter activity around the announcement (*ATweet*) and a proxy for a firm's social media audience (*Followers*). While *Followers* is log-transformed to reduce the variance of the distribution, *ATweet* is defined as follows:

$$ATweet_{i,j} = \frac{Tweet_{i,j} - NTweet_{i,j}}{NTweet_{i,j}} \quad (4)$$

Where *Tweet* (*NTweet*) is the average daily number of tweets generated by the Twitter account of firm *i* during the event period (estimation period) for event *j*.

Finally, include control variables for firms' characteristics such as (i) size, as proxied by total assets (*Size*), the cost of a data breach might be different for small and large firms [5]; (ii) growth expectations, as proxied by the market-to-book ratio (*Growth*), since firms with higher growth opportunities might suffer larger negative market reaction [5]; and (iii) industry-related security expectation (*HighExp*) since firms operating in financial services and data processing are expected to meet high security standards [18].

5. Sample and data

We build our sample starting from the list of breaches that occurred from January 2011 to December 2014 as compiled by Privacy Rights Clearinghouse[5]. While the number of Twitter users has increased since 2010 [30], the actual number of tweets, which denotes the real activity, only increased dramatically in 2011[6]. For this reason we adopt 2011 as the starting year of our sample.

The initial event list included 2,257 breaches. Being interested in analyzing the stock price reaction to the announcement, we deleted all events that affected non-publicly traded companies (2,034). We then searched on Lexis-Nexis to determine if any newspaper reported an event in our sample before the official announcement date and, if this was the case, we adjusted the event date to the date of this first newspaper article. This occurred for 14 events. We also used Lexis-Nexis to check whether any confounding event or information leakage [7] occurred in a seven-day period before the announcement of a given breach. 57 events were excluded on this basis. In case of multiple events for the same firm, we required the events to be at least 130 days apart from each other. This was necessary to avoid any biases in the defined estimation periods; we excluded 47 events that did not meet this condition. In order to ensure a sample of comparable events, we excluded 9 events that were announced during weekends or public holidays.

We searched for the main Twitter accounts or for customer services Twitter accounts on the firms' websites and then used Twitter advanced search to check whether the firms tweeted about the data breach[8]. When a firm had both active main and customer service Twitter accounts, we considered only the customer service accounts as this would more likely be targeted by customers' complaints. Finally, given that SBNLs were enacted in different years across different states, we checked that all firms in our final sample were subject to mandatory disclosure when the breach occurred. Finally, we excluded 23 events because of missing values. Our final sample includes 32 events corresponding to 29 firms[9]. Table 1 summarizes the sampling process. Table 2 provides relative frequencies of events over time, while Table 3 reports the number of events per breach type.

For this study we retrieved data from three other sources. Daily stock price and market index data was sourced from Thomson Reuters Datastream. To collect the number of newspaper articles we searched for company name or ticker symbol in the headlines or the lead paragraph of newspaper articles using Lexis-Nexis PowerSearch [30]. The Twitter data came from TwitterCounter, which provides daily statistics on active Twitter accounts. TwitterCounter statistics include the daily number of tweets generated from a specific account as well as the daily number of followers and followings.

[5] http://www.privacyrights.org/data-breach. This dataset has been adopted in other recently published studies (e.g. [38]).

[6] According to Twitter statistics, the number of tweets per day was 35 million in 2010, and 200 million in 2011. See https://blog.twitter.com/2010/measuring-tweets for further details.

[7] We consider confounding events all earnings announcements, merger and acquisitions news or rumors, CEO and/or top executive turnover. We checked for information leakage in both newspaper articles and in the tweets generated from or mentioning the company account.

[8] We searched whether any tweet was generated from the official Twitter account containing the following keywords in the event period 'breach OR breached OR breaches OR hacker OR hacked OR attack'. All the tweets retrieved were manually inspected to ensure that they were related to the announcement of the data breach that affected the company that generated the message.

[9] The limited sample size reflects the data availability and the need to apply adequate filters in order to reduce possible noise. Both the sampling criteria and the size of our sample are in line with previous studies on the same topic e.g. [7, 18, 22, 38].

Table 1. Sample definition

Filters	No. of Events
Events reported by Privacy Rights Clearinghouse (2011-2014)	2,257
Non-publicly traded firms	(2,034)
Events with possible confounding announcements	(57)
Events overlapping	(47)
Announcement during weekends or public holidays	(9)
Missing data	(23)
Without Active Twitter account	(55)
Final Sample	32
Number of firms	29

Table 2. Events distribution by year

Year	No. of Events	%
2011	8	25.00%
2012	9	28.14%
2013	8	25.00%
2014	7	21.86%
Total	32	100.00%

Table 3. Events distribution by breach type

Type of Breach	No. of events	%
Payment card Fraud	2	6.25%
Disclosure	2	6.25%
Hacker	15	46.88%
Insider	7	21.88%
Portable device	3	9.38%
Unknown	3	9.38%
Total	32	100.00%

6. Findings

Table 4 shows the descriptive statistics of the variables included in our regression models. We Winsorized all continuous variables at 1 and 99 percent to avoid outliers that could alter the results. The average price drop during the event period (CARs) is 1.4 percent. The average value of *ATMedia* reveals that traditional media pays significant attention to data breaches since the number of newspaper articles concerning the events in our sample increases, on average, by 36 percent in the event period. Looking at social media activity, results show that breached firms increase their social media communication (i.e. tweets), on average, by 10 percent, but only 9 percent of firms with an active Twitter account decide to disclose the event through their account suggesting opportunistic behavior in social media communication [25]. Given the limited number of characters allowed in a tweet (140) and the complexity of the information to be disclosed, these tweets tend to not provide details regarding the incident occurred and to link back to a more comprehensive text on the firm's website. An exemplar case is the tweet posted by The Home Depot (@HomeDepot) when its payment card system was breached in 2014 which reports the following: "*To keep customers updated, we've posted a message about news reports of a possible payment data breach thd.co/update*". Our regression analysis aims to clarify whether those firms which do not disclose a data breach on social media choose the right option or not. Table 4 also reveals that the number of records breached is disclosed for just 35 percent of the events in our sample, while almost 44 percent of the events are preceded by other breaches.

Table 4. Descriptive statistics

Variable	Mean
CAR(0,1)	-0.018
Size	9.978
Growth	-0.860
ATMedia	0.362
Low	0.333
ATweet	0.101
Followers	11.703
TweetEvent	0.094
RecordsKnown	0.375
PriorBreach	0.438
HighExp	0.188
N	32

Table 5 reports the CARs over different time windows for the full sample (FS), for the subsample of firms that disclosed a data breach through their social media account (TD) and the subsample of firms that did not (NTD). It also reports the p-values of t-test on the differences between TD and NTD. Although the focus of this study is on the most immediate impact of the announcement over the days (0;+1), looking at different time windows is useful to investigate whether the announcement generates longer-term effects.

The results in Table 5 show that a data breach has a negative and significant impact over a three-day period starting at the announcement day (0;+2), but the largest

Table 5. CARs Analysis

CAR	FS		P-Value
(0,1)	-0.016		0.001***
(0,2)	-0.010		0.046**
(0,3)	0.007		0.283
(0,4)	-0.002		0.819
(0,5)	0.015		0.081*
	TD	NTD	P-Value
(0,1)	-0.037	-0.014	0.048**
(0,2)	-0.028	-0.008	0.090*
(0,3)	0.001	0.008	0.736
(0,4)	-0.022	0.000	0.472
(0,5)	-0.009	0.018	0.329

price drop occurs over the first two days (0;+1). Firms disclosing a data breach on Twitter face larger negative returns over the first three days from the announcement (0;+2) while there is no significant difference thereafter[10]. Overall, the results of our univariate analysis suggest that a data breach announcement triggers a short-term negative stock price reaction, which is larger when the event the firms discloses the event on Twitter. However, the market seems to absorb the shock relatively quickly with stock price reaching a new equilibrium after for days from the announcement (0;+3).

A correlation analysis was also performed in order to verify whether some of the variables included in our regression model have a strong correlation. None of the coefficients denote a strong correlation excluding potential bias in the regression results due to multicollinearity [23].

Table 6 presents the results of our regression analysis. The regression coefficients show that the disclosure of a data breach on social media (*TweetEvent*) exacerbates the negative price response to the announcement. In particular, the price drops by 5.2 and 3.4 percent more compared to other companies that have an active Twitter account but do not disclose the event directly from their account over a two- and three-day period respectively. This leads us to accept H1 and suggests that spreading bad news to a larger audience does not represent a convenient communications strategy. However, it seems to be an effective strategy for low visibility firms. The coefficient of the interaction variable (*TweetEvent x Low*), indeed, shows that the event disclosure through the Twitter account of a low-visibility firm mitigates the negative price response by 4.4 percent. This result leads us to accept H2. However, this effect is significant only when the dependent variable is CAR(0,1) suggesting that Twitter disclosure of a data breach accelerates the movement towards a new price equilibrium for low visibility firms.

Four other factors have a significant effect on the most immediate price response to the announcement for firms included in this subsample. Firstly, the abnormal Twitter communication of a breached firm (*ATweet*) increases the negative price reaction, on average, by 10 percent. This result is a clear signal that firms tend not to adopt effective communication strategies in their social media usage and/or that they cannot keep (enough) control of the information flow. In other words, the virality of social media overwhelms firms' communication skills. Secondly, the larger the audience (i.e. followers), the more negative the price response to announcement, as evidenced by the negative coefficient of *Followers*. In particular, the result indicates that stock prices decrease, on average, by 0.53 percent for every 100 followers. Thirdly, breaches caused by payment card frauds (*Card*) have a more negative price response. The coefficient shows that this type of breach leads, on average, to a 5 percent more negative response compared to the case in which the cause of the breach is unknown. This result is coherent with previous studies showing that data breaches involving confidential data trigger a more negative price reaction. Fourthly, abnormal traditional media activity (*ATMedia*) slightly mitigates (0.02 percent) the negative price reaction to the announcement. A possible interpretation of this result is that newspaper articles help firms to provide more details about the event and potentially soften stakeholder negative perceptions. Among the control varibales, only *ATweet*, *ATMedia*, and *Growth* have a significant impact on the three-day CARs (0;+2).

7. Robustness test

The dependent variable of our regression model is the cumulative abnormal returns (*CAR*). As shown above, we estimate CARs based on the Market Model [14]. Fama and French [16] propose an alternative model to estimate CARs. Their model, known as the *Three-factor Model*, takes into account two factors other than the market index return which are the difference of returns between (a) firms with small and large market capitalization and (b) firms with high and

Table 6. Regression results

Variable	CAR(0;+1)	CAR(0;+2)
Intercept	0.068*	-0.030
TweetEvent	-0.052***	-0.034**
TweetEvent x Low	0.044***	0.011
ATweet	-0.132**	-0.131*
Followers	-0.006***	-0.004
Card	-0.042***	-0.006
Disc	0.022*	0.030
Hack	0.015*	0.008
Insd	0.018*	0.019
Port	-0.013	-0.030
RecordsKnown	0.006	0.013
PriorBreach	-0.007	-0.016
ATMedia	0.000***	0.000***
Size	0.001	0.001
Growth	0.000**	0.001***
HighExp	0.025	0.023
Year Fixed-Effects	Yes	Yes
R-squared	0.82	0.81
F-Stat	26.41	23.07
p-Value	0.000	0.000
N	32	32

[10] We compared the CARs up to ten days after the announcement date with similar results.

low book-to-market ratio.

In order to ensure that the results of our analysis do not depend on the estimation model adopted, we estimate CARs using the Three-factor Model and run the regression using the new CARs as dependent variable. The results of our test (untabulated) show that, except for some minor changes in the value of the OLS coefficients, all our main findings are confirmed; therefore we can conclude that the results of this study are robust to the CAR estimation model specification.

Finally, to ensure that our findings on low visibility firms are not driven by the threshold adopted, we repeat the analysis adopting a quartile-based classification. In this case, low visibility firms are the ones with an average daily number of newspaper articles during the estimation period below the first quartile threshold. Our results (untabulated) are unaltered; therefore we can conclude that the results of this study are robust to different visibility classification criteria.

7. Conclusion

This paper investigates whether communication via social media affects the price reaction to a data breach announcement. Using a sample of 32 data breaches that occurred between January 2011 and December 2014 to U.S. publicly-traded firms with an active Twitter account, the study demonstrates that disclosing a data breach on social media tends to exacerbate the negative impact of the announcement on stock price, causing an average additional decrease of 5.2 and 3.4 percent over a two- (0;+1) and three-day (0;+2) event period respectively. Further analyses suggest that the negative effect of social media is even more pronounced when firms disclose the event through their Twitter account (-5.2 percent), when they increase the communication via social media (i.e. number of tweets) in the event period, and have a larger audience on social media (i.e. followers). However, our results also suggest that the impact of social media impact is positive for low-visibility firms. Specifically, social media disclosure of a data breach by a low-visibility firm mitigates the negative price response by 4.4 percent, and it accelerates the movement towards a new price equilibrium.

The contribution of this study is threefold. Firstly, the study provides new insights into the cost of data breaches by adding the disclosure via social media as a new significant factor affecting the price reaction to a data breach announcement. In doing so, we provide additional evidence on the effectiveness of the use of social media for crisis communication. In addition, we contribute to the ongoing debate on the net effect that social media generates in crisis communication by providing evidence of a differential impact based on firms' visibility on traditional media. This represents an important contribution to and extension of both the literature on crisis communication and that on the impact of firm level social media usage. Social media usage in firm communication is now commonplace, however as yet the academic literature provides little guidance on the impact of this communication strategy in the context of a company crisis. Our study provides evidence and important practical information for firms making communication decisions in crises such as these. Although there is a generalized positive view on the adoption of social media in firm communications, managers should also be aware of the challenges that it generates, and of the peculiarity of the crisis they are dealing with. This is particularly true when dealing with negative and complex information that might damage the reputation of the company. Managers need to carefully assess the risk of losing control of the information flow due to the virality of social media and to design appropriate communication strategies.

Secondly, our paper provides further evidence of a negative price reaction to data breach announcements contributing to the debate about the magnitude of the economic impact of data breaches and showing additional potential outcomes related to the way the information is delivered to the stakeholders. We also provide further evidence of investors including the possibility of recurring breaches in their expectations and penalizing firms affected by breaches involving confidential data (i.e. credit cards).

Thirdly, our study contributes to the research on the impact of company disclosure through social media on stock market by confirming that it significantly affects the stock price and providing evidence of a positive impact on low visibility firms in regard of data breach announcements. By showing that social media usage is likely to either help or hinder a firm in the context of a crisis, these results are likely to be useful for industry as they highlight the need for a contingent crisis communication strategy based on firm visibility and on the type of crisis a firm is facing.

7. Limitations and future research

This study is also subject to some limitations that might represent avenues for future research. Firstly, our analysis considers only Twitter as a social media platform. Although Twitter is the most accepted platform in the financial community, alternative social media platforms (e.g. Facebook) are available to firms or indeed firms may decide to disclose events through a number of platforms at the same time to reach different stakeholders. The use of alternative platforms,

potential interconnections between them, and stakeholders' preferences are not considered in this study, therefore further research on this would be informative. Secondly, our analysis is based on daily statistics about the use of social media. It does not allow us to investigate the content of the messages which might convey more information about the firms' communication strategies. Breached firms might provide updates on the incidents or just reply to customers' or investors' enquiries, but they might also attempt to divert followers' attention away from the bad news by issuing other positive announcements. Further research in this field would shed additional light on firms' communication strategy around data breach announcements and bad news disclosure in general.

Finally, we do not consider whether breached firms issue press releases on the announcement day or in the following day. Press releases arguably provide more information than a Tweet, which is limited to 140 characters. As such, press releases might reduce uncertainty and therefore affect the overall cost of the incident. Given the current lack of specific disclosure requirements for data breach disclosure, investigate the information included in disclosure statements to investigate how breached firms communicate the incident and whether providing specific type of information affect the market response to the announcements.

Acknowledgment

The research work described in this paper was supported by the Irish Centre for Cloud Computing and Commerce, an Irish National Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority.

References

[1] A. Abbasi, S. Sarker, and R.H., Chiang, "Big Data Research in Information Systems: Toward an Inclusive Research Agenda", Journal of the Association for Information Systems, 2016, 17, (2), pp. 1-32.

[2] A.S. Abrahams, J. Jiao, G.A. Wang, and W. Fan, "Vehicle defect discovery from social media" Decision Support Systems, 2012, 54, (1), pp. 87-97.

[3] S. Aral, C. Dellarocas, and D. Godes, "Introduction to the special issue-social media and business transformation: A framework for research", Information Systems Research, 2013, 24, (1), pp. 3-13.

[4] R.J. Arend, "The Definition of Strategic Liabilities, and their Impact on Firm Performance", Journal of Management Studies, 2004, 41, (6), pp. 1003-1027.

[5] B.M. Barber, and T. Odean, "All that glitters: The effect of attention and news on the buying behavior of individual and institutional investors", Review of Financial Studies, 2008, 21, (2), pp. 785-818.

[6] E. Blankespoor, S.G. Miller, and H.D. White, "The role of dissemination in market liquidity: Evidence from firms' use of Twitter™", The Accounting Review, 2014, 89, (1), pp. 79-112.

[7] K. Campbell, L.A. Gordon, M.P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", Journal of Computer Security, 2003, 11, (3), pp. 431-448.

[8] E. Casey, "Investigating sophisticated security breaches", Communications of the ACM, 2006, , (2), pp. 48-55.

[9] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture", Information Systems Research, 2005, 16, (1), pp. 28–46.

[10] R. N. Charette, K.M. Adams, and M.B. White, "Managing risk in software maintenance", IEEE Software, 1997, 14, (3), pp. 43-50.

[11] S. Chai, M. Kim, and H.R. Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior", Decision Support Systems, 2011, 50, (4), pp. 651-661.

[12] W.T. Coombs, "Protecting organization reputations during a crisis: The development and application of situational crisis communication theory", Corporate reputation review, 2007, 10, (3), pp. 163-176.

[13] J.C. Cortizo, F.M. Carrero, and J.M. Gómez, "Introduction to the special issue: mining social media", International Journal of Electronic Commerce, 2011, 15, (3), pp. 5-8.

[14] E.F. Fama, L. Fisher, M.C. Jensen, and R. Roll, "The adjustment of stock prices to new information", International economic review, 1969, 10, (1), pp. 1-21.

[15] E.F. Fama, "Efficient capital markets: A review of theory and empirical work", The Journal of Finance, 1970, 25, (2), pp. 383-417.

[16] E.F. Fama, and K.R. French, "Common risk factors in the returns on stocks and bonds", Journal of financial economics, 1993, 33, (1), pp. 3-56.

[17] Federal Trade Commission (FTC), "Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months", FTC, 2009, Available at: https://www.ftc.gov/news-events/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers.

[18] K.M. Gatzlaff, and K.A. McCullough, "The effect of data breaches on shareholder wealth", Risk Management and Insurance Review, 2010, 13, (1), pp. 61-83.

[19] D. Godes, D. Mayzlin, Y. Chen, S. Das, C. Dellarocas, B. Pfeiffer, B. Libai, S. Sen, M. Shi, and P.W.J. Verlegh, "The firm's management of social interactions", Marketing Letters, 2005, 16, (3), pp. 415–428.

[20] S. Goel, and H.A. Shawky, "Estimating the market impact of security breach announcements on firm values", Information & Management, 2009, 46, (7), pp. 404-410.

[21] L.A. Gordon, and M.P. Loeb, "The economics of information security investment", ACM Transactions on Information and System Security, 2002, 5, (4), pp. 438–457.
[22] L.A. Gordon, M.P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?", Journal of Computer Security, 2011, 19, (1), pp. 33-56.
[23] D. Gujarati, and D. Porter, "Multicollinearity: What happens if the regressors are correlated", Basic econometrics 4th Edition, McGraw Hill 2003.
[24] D.L. Hoffman, and T.P. Novak, "Why do people use social media? Empirical Findings and a New Theoretical Framework for Social Media Goal Pursuit", Working Paper, George Washington University School of Business, 2012.
[25] M.J. Jung, J.P. Naughton, A. Tahoun, and C. Wang, "Corporate use of social media", Working Paper, New York University, Northwestern University, 2015.
[26] P.S. Kalev, W.M. Liu, P.K. Pham, and E. Jarnecic, "Public information arrival and volatility of intraday stock returns", Journal of Banking & Finance, 2004, 28, (6), pp. 1441-1467.
[27] A.M. Kaplan, and M. Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media" Business Horizons, 2010, 53, (1), pp. 59-68.
[28] J.H. Kietzmann, K. Hermkens, I.P. McCarthy, and B.S. Silvestre, "Social media? Get serious! Understanding the functional building blocks of social media", Business Horizons, 2011, 54, (3), pp. 241-251.
[29] S. LaValle, E. Lesser, R. Shockley, M.S. Hopkins, and N. Kruschwitz, "Big data, analytics and the path from insights to value", MIT Sloan Management Review, 2011, 52, (2), pp. 21-32.
[30] L.F. Lee, A.P. Hutton, and S. Shu, "The Role of Social Media in the Capital Market: Evidence from Consumer Product Recalls", Journal of Accounting Research, 2015, 53, (2), pp. 367-404.
[31] T. Lynn, S. Kilroy, L. van der Werff, P. Healy, G. Hunt, S. Venkatagiri, and J. Morrison, "Towards a general research framework for social media research using big data", Professional Communication Conference (IPCC): IEEE International, 2015, pp. 1-8.
[32] W.J. Mayew, "Evidence of management discrimination among analysts during earnings conference calls", Journal of Accounting Research, 2008, 46, (3), pp. 627-659.
[33] National Conference of State Legislature (NCSL), "Security Breach Notification Laws", NCSL, 2017, Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[34] I.P.L Png, C.Y. Wang, and Q.H. Wang, "The deterrent and displacement effects of information security enforcement: International evidence", Journal of Management Information Systems, 2008, 25, (2), pp. 125-144.
[35] I.P.L Png, and Q.H. Wang, "Information security: Facilitating user precautions vis-à-vis enforcement against attackers", Journal of Management Information Systems, 2009, 26, (2), pp. 97-121.
[36] Ponemon Institute, "Cost of Data Breach Study: Global Analysis", Ponemon Institute, 2016. Available at: https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov542.
[37] M. Risius, and R. Beck, "Effectiveness of corporate social media activities in increasing relational outcomes", Information & Management, 2015, 52, (7), pp. 824-839.
[38] P. Rosati, P. Deeney, F. Gogolin, M. Cummins, L. van der Werff, and T. Lynn, "The effect of data breach announcements beyond the stock price: Empirical evidence on market activity", International Review of Financial Analysis, 2017, pp. 146-154.
[39] P. Rosati, F. Gogolin, and T. Lynn, "Cyber-security Incidents and the Probability of Financial Restatements", European Accounting Association Annual Meeting, 2017.
[40] F. Schultz, S. Utz, and A. Göritz, "Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media", Public relations review, 2011, 37, (1), pp. 20-27.
[41] Securities and Exchanges Commission (SEC), "SEC Says Social Media OK for Company Announcements if Investors Are Alerted", 2013. Available at: https://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171513574.
[42] M.W. Seeger, "Best practices in crisis communication: An expert panel process", Journal of Applied Communication Research, 2006, 34, (3), pp. 232-244.
[43] T. O. Sprenger, A. Tumasjan, P.G. Sandner, and I.M. Welpe, "Tweets and trades: The information content of stock microblogs", European Financial Management, 2014, 20, (5), pp. 926-957.
[44] T.O. Sprenger, P.G. Sandner, A. Tumasjan, and I.M. Welpe, "News or Noise? Using Twitter to Identify and Understand Company‐specific News Flow", Journal of Business Finance & Accounting, 2014, 41, (7), pp. 791-830.
[45] B. Srinidhi, J. Yan, and G.K. Tayi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors", Decision Support Systems, 2015, 75, pp. -62.
[46] G. Stevens, "Data Security Breach Notification Laws", Congressional Research Service, 2012, Available at: https://pdfs.semanticscholar.org/8f37/2875c6cdc54a0c40b65180a6b117bc228d61.pdf.
[47] B.S. Trinkle, R.E. Crossler, and F. Bélanger, "Voluntary Disclosures via Social Media and the Role of Comments", Journal of Information Systems, 2015, 29 (3), pp. 101-121.
[48] S. Utz, F. Schultz, and S. Glocka, "Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster", Public Relations Review, 2013, 39, (1), pp. 40-46.
[49] X. Zhang, H. Fuehres, and P.A. Gloor, "Predicting stock market indicators through twitter "I hope it is not as bad as I fear", Procedia-Social and Behavioral Sciences, 2011, 26, pp. 55-62.