Universiteit Leiden
The Netherlands

Opleiding Informatica & Economie

The Impact of Social Media Discourse on Market Reactions to Data Breach Announcements: An Empirical Analysis

Simeon Klumperbeek

Supervisors:
Dr. A.H. Zohrehvand & Dr. O. Gadyatskaya

BACHELOR THESIS

Leiden Institute of Advanced Computer Science (LIACS)
www.liacs.leidenuniv.nl

10/7/2023

Abstract

This study investigates the role of social media engagement preceding data breach announcements and its impact on market reactions. We posits two hypotheses: (1) social media discourse about a firm increases before a data breach announcement, suggesting potential impression management efforts; (2) such increased discourse tempers the negative effect of the announcement on cumulative abnormal returns and thus the market reaction. An empirical of data breach announcements and corresponding Twitter activity confirms both hypotheses. It shows a significant surge in daily tweets about the firms 11 to 2 days prior to the announcements compared to a baseline of daily tweets, indicating the potential use of strategic impression management by the firms. Moreover, a rise in pre-announcement social media discourse is associated with less negative market reactions, unveiling a crucial link between social media engagement and financial implications of data breaches. This research underlines the importance of proactive social media strategies for firms managing data breaches and provides valuable insights

1. Introduction

This paper seeks to explore the role of social media engagement and impression management strategies in shaping market reactions to data breach announcements. With the increasing prevalence of data breaches and the corresponding reputational and financial consequences, understanding the dynamics of market reactions and potential mitigating factors has gained significant importance. Specifically, the study investigates whether an increased level of social media discourse about a firm prior to a data breach announcement which might come from the use of impression management strategies by firms, could influence the market's reaction to such announcements.

Previous research has unveiled the complex nature of market reactions to data breach announcements with conflicting findings. Some studies have indicated negative market reactions following data breach announcements (e.g. Cavusoglu et al., 2004; Garg et al., 2003; Goel & Shawky, 2009; Yayla & Hu, 2011), while others have found no negative market reaction (Hilary et al., 2016; Kannan et al., 2007) These discrepancies can potentially partly be attributed to the absence of influential factors that may confound the market reaction. Bischoff's (2019) report demonstrated that factors such as industry type and breach severity have an impact on the market response. Additionally, Foerderer & Schuetz (2022) highlighted the influence of news pressure on the day of the announcement, while Rosati et al. (2019) showed the impact on the market reaction of when a firm announces her data breach through its Twitter account.

Despite these insights, some gaps remain unaddressed. The potential role of social media discourse about a firm preceding a data breach announcement in shaping market reactions has not yet been researched. Considering the extensive influence of social media on the public perception of a firm (Dijkmans et al., 2015) and its capacity to serve as a platform for impression management (Aral et al., 2013; Benthaus et al., 2016; Schniederjans et al., 2013), it becomes crucial to comprehend its role in shaping market reactions to data breach announcements. By examining this factor, we can gain insights into an additional confounding element and enhance our understanding of the overall dynamics at play.

To address this gap, this paper sets out to examine two key hypotheses. Firstly, the study will assess whether there is an increase in social media discourse on twitter about a firm in the days before a data breach announcement, indicating potential impression management efforts by the firm. Secondly, the study will investigate the potential impact of this heightened level of social media discourse on the market reaction to the data breach announcement. Through this study we hope to provide a better understanding of market

reactions to data breach announcements, particularly focusing on the role of social media discourse prior to the data breach announcement.

2. Theoretical Background

2.1 Data Breaches

In 2022 there were 1,774 publicly announced data breaches in the US according to the ITRC, which is a non-profit organisation that keeps track of data breach announcements of companies in the US (ITRC., 2022 p6) As of 2021, all states in the United States had implemented legislation mandating companies to disclose incidents of data breaches. These laws exhibit variations across states, primarily in two aspects. Firstly, the notification thresholds for the number of breached records differ, ranging from as low as 1 to as high as 1000 breached records. Secondly, the time frame within which companies are required to announce the breach varies among states. (*State Data Breach Notification Laws | Foley & Lardner LLP*) Some states merely encourage companies to announce it as soon as practically feasible (e.g. *General Law - Part I, Title XV, Chapter 93H, Section 3*), while others enforce a specific deadline between 30 to 60 days (e.g. *Texas Business and commerce code chapter 521. Unauthorised use of identifying information*, 2009).

A common definition of a data breach used by Foerderer & Schuetz (2022) is "An unauthorised and unlawful access of confidential and sensitive information.". Data breaches have numerous effects on firms and victims. But the most researched consequence of a data breach is the effect of the data breach announcement on the market reaction. (Schlackl et al., 2022).

2.1.1 Market reaction on data breaches

The primary approach for analysing market reactions to data breaches in academic research is through the utilisation of event studies (MacKinlay, 1997). These studies employ a statistical method to examine how a specific event, such as a data breach, affects a company's stock price. Event studies in this context are grounded in the efficient market hypothesis (EMH) (Fama, 1970), which asserts that the market incorporates all available information into the price of a security. Consequently, according to the EMH, a company's stock price promptly and accurately adjusts to any new information. Therefore, it is expected that the firm's stock price will fully reflect the impact of the data breach after it is announced.

The academic literature on this subject has generated conflicting outcomes. Some studies (Cavusoglu et al., 2004; Garg et al., 2003; Goel & Shawky, 2009; Rosati et al., 2019; Yayla & Hu, 2011) have identified a significant negative impact, whereas others have observed significant negative effects only in specific scenarios. For instance, negative effects were found when confidential records were compromised (Campbell

et al., 2003) or when the breach was announced through prominent news outlets (Bolster et al., 2010). On the other hand, some studies (Hilary et al., 2016; Kannan et al., 2007) have failed to find any significant negative influence.

One potential explanation for these contradictory results could be the absence of certain confounding factors, For example strategic timing of the data breach announcement. Foerderer and Schuetz (2022) conducted research that unveiled a correlation between data breach disclosures and high news pressure. Their findings suggest that companies might intentionally select days with anticipated high news pressure to announce data breaches so that the data breach announcement gets crowded out. Furthermore, their research indicates that when a data breach disclosure aligns with a day of heightened news pressure, the negative cumulative abnormal returns are less severe.

Other factors, including the scale of the data breach (e.g., number of affected records or type of breached data), the company's size, and its industry, have been investigated and shown to influence the market reaction (Bischoff, 2019). Another factor influencing the market response is the utilisation of social media by the firm (Rosati et al., 2019).

The study conducted by Rosati et al. (2019) exclusively focused on investigating the impact of data breach disclosure through a firm's Twitter account. The investigation regarding the potential impact of social media discourse prior to a data breach announcement on the market response remains unexplored.

2.2 Social media

It is crucial to understand that data breaches not only carry financial consequences but also significantly impact the public impression and perception of the affected firm (Syed & Dhillon, 2015) . In today's era of social media platforms, individuals possess a powerful avenue to express their opinions, concerns, and outrage regarding data breaches, consequently reshaping the overall impression and perception of the implicated company.

Social media are online platforms and tools used to create, share, and exchange information, ideas, and content among individuals. User-generated content is typically involved in these platforms, which promote user interaction and engagement such as commenting, sharing, and liking. Social media platforms examples are Facebook, Twitter, Instagram, LinkedIn, Youtube and TikTok. Social media has become an increasingly important tool for communication, networking, and information dissemination in both personal and professional contexts.

2.2.1 Social media and firms

Social media platforms introduce a new way besides traditional media for firms to engage with

customers, employees, investors, and the community at large and to build relationships and brand awareness. (Hanna et al., 2011; Kietzmann et al., 2011). Social media also provides an opportunity for firms to gather customer feedback and insights (Zohrehvand et al., 2023), which can help them improve their products and services (Kaplan & Haenlein, 2010) or influence firms strategic decisions (Zohrehvand, 2021). It is also widely used for corporate communication and is considered as an official communication channel by the Securities and Exchange Commission (*SEC says social media OK for company announcements if investors are alerted*, 2013). Social media engagement by a firm also has a positive influence on the perception of a firm's reputation. (Dijkmans et al., 2015) This can be explained by the use of social media to perform impression management, that is to manage the impression that customers and other stakeholders have of the firm. Some impression management strategies on social media can also improve financial performance. (Schniederjans et al., 2013)

2.2.2 Social media and market reaction

Social media discourse has the potential to influence market reactions. According to Ranco et al. (2015), the dominant sentiment on social media before and during an event can indicate the direction of cumulative abnormal returns and thus shape the market reaction. Additionally, social media activism can have a negative impact on a company's stock price (Gomez-Carrasco & Michelon, 2017). This means that discussions, movements, and campaigns initiated and amplified through social media platforms can significantly affect a company's financial performance and market value.

The interconnected nature of social media networks allows information to spread rapidly and reach a wide audience, giving individuals the power to express their opinions and concerns about corporate behaviour and practices. Moreover, social media platforms offer speed and accessibility, enabling both individuals and organisations to disseminate information quickly, sometimes even before traditional news outlets report on events. As a result, social media discourse can amplify the impact of events such as data breaches, controversies, scandals, or product failures, accelerating their diffusion across markets. These online discussions can shape public opinion, create investor uncertainty, and ultimately influence the stock price of the implicated company.

Lee et al. (2015) demonstrated that the impact of a product recall on stock price is influenced by the frequency of tweets from the firm and other users. They found that when the firm increases its own tweets during a product recall, the negative price reaction is lessened. However, when there is a high frequency of tweets

from other users, the negative price reaction is intensified. This highlights the significance for firms to consider their social media strategy when dealing with such events.

2.4 Social media and Data Breach announcements.

When a data breach is publicly disclosed, social media platforms become a place for discourse, where users and other shareholders can express their opinions, concerns, and outrage regarding the breach. These discussions can spread rapidly, reaching a large audience and potentially impacting investor sentiment and market perceptions of the affected firm. Negative sentiment expressed on social media may lead to increased uncertainty among investors, eroding confidence in the company's ability to protect customer data and maintain cybersecurity.

The utilisation of social media by a firm plays a significant role in shaping the market reaction to a data breach. When a firm chooses to communicate about a data breach through Twitter, it leads to a negative impact on the market reaction, specifically on the firm's stock price. However, this effect is reversed for firms with low visibility who have little traditional news coverage . (Rosati et al., 2019)

The reason for the negative impact can be that companies have limited control over how information spreads on social media after the announcement. Therefore, it can be wise for companies to take measures to control the spread of information on social media before announcing a data breach. So Rosati et al. (2019) looked at during and after the announcement where we will look at social media discourse prior to a data breach announcement.

3. Theory and Hypothesis

3.1 Impression management theory

Impression Management was conceptualised by Goffman in the 1950's, IM refers to the conscious or unconscious strategies individuals employ to control or shape the perceptions others have of them. It involves the deliberate presentation of oneself in a favourable light to create specific impressions and manage how others perceive and evaluate them. These strategies can include carefully selecting and manipulating verbal and nonverbal cues, such as appearance, speech, gestures, and online presence, in order to create a desired impression. The ultimate goal of impression management is to influence others' opinions, gain social acceptance, enhance personal or professional reputation, and achieve desired outcomes in various social and organisational contexts.

Furthermore, is it important to note that IM extends beyond individual behaviours and also encompasses organisational practices. Where with organisational impression management (OIM),

organisations employ various IM strategies with the aim of improving, maintaining, and safeguarding a positive image among diverse stakeholders both within and outside the organisation.(Bolino et al., 2008; Elsbach et al., 1998) Prior studies have identified distinct categories of IM/OIM tactics. They recognize four principal strategies, namely direct assertive/ proactive, indirect assertive/proactive, direct defensive/protective, and indirect defensive/ protective approaches (Mohamed et al., 1999). Social media has provided companies with the opportunity to utilise organisational impression management strategies by actively engaging on these platforms. This serves as a complementary channel through which companies can influence and control the public perception of their organisation (Aral et al., 2013; Benthaus et al., 2016; Schniederjans et al., 2013).

3.2 Hypothesis development:

Impression management theory posits that firms strategically influence stakeholders' perceptions through different communication channels, such as social media. Expanding on this theory and taking into account the notification laws allowing a window of time before official disclosure, companies have the opportunity to engage in impression management on social media platforms prior to announcing a data breach. Through a deliberate and proactive online strategy, firms can purposefully shape their online presence to cultivate a positive impression and mitigate potential negative reactions from stakeholders. The efforts of impression management may influence the level of social media discourse about the firm. Based on this premise, our study formulates the following hypothesis:

Hypothesis 1: *The level of social media discourse about a firm significantly increases in the days leading up to the announcement of a data breach.*

Our second hypothesis revolves around the implementation of direct proactive impression management strategies as a preemptive measure prior to publicly disclosing a data breach incident. We propose that by employing these strategies, the level of social media discourse about a firm will increase, resulting in a prevailing positive sentiment on social media leading up to the data breach announcement. As suggested by Ranco et al. (2015), the dominant sentiment on social media prior to an event can serve as an indicator of the market reaction's direction. The objective is to effectively limit public outrage and the spread of negative discussions surrounding the data breach announcement by fostering a prevailing positive sentiment, thereby reducing the impact on stock market returns.

To assess the effectiveness of this approach, we propose utilising the level of social media discourse about a firm as an indicator or

proxy to measure the extent of direct proactive impression management strategies. This methodology enables us to analyse and evaluate the potential influence of such strategies on subsequent market reactions. Based on this rationale, we present our second hypothesis:

Hypothesis 2: *A higher level of social media discourse about a firm in the days before a data breach announcement decreases the negative effect of a data breach announcement on the stock price.*

4. Methodology

To test our hypotheses, we retrieved data from the PRC Data Breach Chronology database (Privacy Rights Clearinghouse, 2023). According to PRC the PRC Data Breach Chronology database reflects breaches reported in the United States that are made publicly available by government entities from 2005 till February 2022. Each announcement in the PRC Data Breach Chronology database is labelled based on the type of breach and organisation involved. The type of breach indicates how the information was exposed, such as "HACK" for being hacked by an outside party or infected by malware, or "PORT" for the loss, disposal, or theft of portable devices like laptops,

Table 1: Sample construction

Filter	No. of Announcements
PRC announcements	20161
Filter on organisation type	(3060)
Non S&P-1500 firms	(16406)
Announcements before 2017-01-01	(54)
Firms with no tweets	(115)
Overlapping event windows	(79)
Hypothesis 1 sample	447
Missing stock data	(126)
Hypothesis 2 sample	321
Number of firms	148

Table 2: Announcements by year

Year	Total Breaches
2008	1 (0%)
2009	2 (1%)
2011	16 (5%)
2012	15 (5%)
2013	5 (2%)
2014	23 (7%)
2015	12 (4%)
2016	2 (1%)
2017	14 (4%)
2018	11 (3%)
2019	151 (47%)
2020	41 (13%)
2021	27 (8%)
2022	1 (0%)
Total	321 (100%)

Table 3: Announcements by type

Type of Breach	No. of Announcements
CARD	27 (8%)
DISC	52 (16%)
HACK	99 (31%)
INSD	23 (7%)
PHYS	35 (11%)
PORT	11 (3%)
STAT	5 (2%)
UNKN	69 (21%)
Total	321 (100%)

PDAs, smartphones, memory sticks, CDs, hard drives, or data tapes. A detailed explanation of each breach type can be found in Appendix A. Similarly, the organisation type denotes the nature of the entity, such as a business, government, or educational organisation. An explanation for each organisation type can also be found in Appendix A.

For our sample we selected all breaches with the labels BSF, BSO, and BSR for all businesses, as well as MED for all medical organisations. To prevent overlooking any organisations that might have been incorrectly labelled by the PRC, we included the UNKN label. To ensure access to stock price data, our sample was limited to S&P 1500 firms. We achieved this by matching the organisation names from the PRC database with an S&P 1500 database using the NameMatching Python library (Nijhuis, 2022). We manually checked the matches and performed some robustness checks to ensure the quality of the data. At this point we also removed any duplicate entries of the same announcement. Due to no availability of tweets prior to 2006-03-02, we have chosen to retain only announcements from 2007-01-01 onwards.

In order to look at the level of social media discourse about a firm we looked social media platform twitter following prior research (Rosati et al., 2019) Consequently to gather all relevant tweets, we began the process by conducting a Google search using the firm's name and "twitter" to locate official company Twitter handles. By utilising the Twitter API, we extracted tweets using the query pattern "(@TwitterHandle has:mentions)," enabling us to retrieve tweets where the company's Twitter handle was mentioned. The data collection period covered a span of 60 days prior to the announcement and 20 days after it. As a result, we obtained a comprehensive collection of tweets related to the firm's Twitter account. We filtered announcements from firms that had multiple announcements within 11 days of each other, retaining only the first announcement, this resulted in 447 announcements. Therefore the sample for the first hypothesis consisted of 447 announcements.

Subsequently, we collected daily stock market data from the Compustat database. For 368 announcements, we found sufficient daily stock market data. The final sample for hypothesis 2 of announcements where there was sufficient tweet data and stock market data and no overlapping events consisted of 321 announcements, see Table 1 for a breakdown of the sample construction (See figure 1 in Appendix A for the sample construction process). In table 2 you can find the distribution of the final sample by year and in table 3 the distribution by type of breach.

Hypothesis 1

To evaluate our first hypothesis, we measure the change in daily tweets from the 11 to 2 days interval preceding an announcement. In order to

explore this change, we analyse tweet data from the events in our first sample. The data is aggregated on a daily basis, forming a panel dataset that consists of 59 days daily tweets mentioning the firm for each announcement. The dataset covered a time span of 60 to 2 days prior to the announcement, resulting in a total of 447 samples multiplied by 59 days, equating to 26,373 days of data. To handle any outliers in the dataset, we applied a logarithmic transformation to the count of daily tweets. Specifically, we took the logarithm of the daily tweets, adding 1 to the count to ensure that days without any tweets would not result in undefined logarithms. This transformation helps mitigate the impact of extreme values and improves the distribution of the data.

Next, our objective is to investigate whether there is a change in the daily tweet count in the period from 11 to 2 days prior to the announcement compared to not being in that period. To achieve this, we create a binary variable that is assigned a value of 1 if the day falls within the 11 to 2 days before the announcement, and 0 otherwise. Next we estimate the following fixed effects model:

$$log(dailyTweets + 1)_{it} = \beta_0 + \beta_1 dummy_{it} + \alpha_i + \lambda_t + \mu_{it}$$

where the **dependent variable** is the logged daily tweet count + 1 for firm *i* at day *t* and the **independent variable** is the dummy representing the days 11 to 2 days before the announcement for firm *i* at day *t*. To mitigate potential biases from omitted variables, we incorporated firm fixed effects for firm *i* in α_i and yearly time fixed effects in λ_t for day *t*. The inclusion of firm fixed effects accounts for unobserved factors, such as firm size, that may impact the number of daily tweets. Additionally, the yearly time fixed effects control for unobserved factors over time that could influence the volume of daily tweets, such as the overall increase in tweets across the years.

Hypothesis 2

To explore our second hypothesis, we employ an event study methodology, building upon prior research conducted on market reactions to data breach announcements (Goel & Shawky, 2009). We chose to use an event study (MacKinlay, 1997) because of its alignment with the Efficient Market Hypothesis (Fama, 1970), which posits that the effects of an event can be discerned through changes in a firm's stock price. These effects are captured by abnormal returns, showing the differences between a firm's predicted returns without the announcement taking place and its actual realised returns with the announcement taking place, when we add the abnormal returns over a certain time period we get the cumulative abnormal returns which serve as an approximation for the price reaction to the announcement. (Campbell et al., 2003) By employing this approach, we aim to evaluate the impact of social

media discourse surrounding data breach announcements on market reactions.

Dependent variable

To compute the Cumulative Abnormal Returns (CAR), our initial step involves predicting the expected returns and calculating the Abnormal Returns (AR). The AR is determined by subtracting the expected returns $\hat{r}_{i,t}$ from the actual returns $r_{i,t}$. Mathematically, $AR_{i,t} = r_{i,t} - \hat{r}_{i,t}$.

To forecast the expected returns, we utilise a three-factor model, the market factor (mkt), the size factor (smb), and the value factor (hml). The three-factor model is used to estimate the expected returns based on the equation $\hat{r}_{i,t} = mktrf + smb + hml$ (Fama & French, 1993).

With the obtained AR values, we construct our dependent variable, the CAR, over a specific time window of one day before the data breach announcement till one day after the data breach announcement [-1,1]. This is achieved by summing the AR values within this time window, which provides a cumulative measure of abnormal returns over the given period.

Independent variable

The independent variable, referred to as "ΔTWEETS," measures the difference in average daily logged tweets between two specific time periods: 60 to 20 days prior to the announcement (serving as the baseline) and 11 to 2 days before the announcement. To calculate this, we begin by summing up the total logged daily tweets for each time window and dividing them by the respective number of days in each window. Subsequently, we subtract the average baseline value from the average during the 11 to 2 days period to get the variable ΔTWEETS.

Firm specific controls firm-specific factors

Past research has documented various firm-specific confounders. We include four control variables obtained from the Compustat Capital IQ database. These variables provide additional insights into the characteristics of the firms under study.

1. **Firm Size:**

   To consider the scale of the firms in our analysis, we incorporate firm size as a control variable. We utilise the logged amount of assets plus one as a proxy for firm size. This variable helps us understand the impact of company size on the market reaction to data breaches. Interestingly, previous studies have presented conflicting findings on the influence of firm size. Cavusoglu et al. (2004) reported a higher negative reaction for small firms, while Gatzlaff & McCullough (2010) found a higher negative reaction for large firms. As a result, the direction of the influence of firm size remains a subject of debate.

2. **Earnings:**

To account for the firm's earnings performance, we include the earnings before interest and taxes for the preceding year (EBIT) as a control variable. Notably, we do not log this variable since negative values are present, which would result in undefined logarithms. By considering the firm's earnings, we aim to control how profitability or financial performance may influence the market reaction to data breaches following Foerderer & Schuetz, (2022).

3. **Investments:**

   Incorporating the firm's investments, we utilise the logged capital expenditures (CAPEX) as a control variable. Higher levels of investment may indicate expectations of increased future returns or investments in IT infrastructure (Foerderer & Schuetz, 2022). By including this variable, we aim to control for the firm's investment decisions and strategic choices regarding technology infrastructure .

4. **Operating Expenses:**

   We also include the firm's logged operating expenses (OPEX) as a control variable. This variable helps us account for general business costs incurred by the firm, including various operational expenditures. Foerderer & Schuetz (2022) highlight the importance of this control variable in considering different types of business models within the firms and the use of third-party services in delivering IT infrastructure.

By incorporating these firm-specific control variables, we aim to address potential confounding factors and gain a more comprehensive understanding of the relationship between the studied variables.

Breach specific controls

To consider the influence of breach-specific factors, we introduce seven dummy variables corresponding to each breach label depicted in Table 1 in Appendix A. These dummy variables are employed to account for the specific type of breach encountered. Prior research has demonstrated the impact of these breach types. For instance, Morse et al. (2011) found a higher negative impact when the breach source involved a stolen laptop or fraudulent access and hacking. Additionally, Johnson et al. (2017) reported a higher negative impact when the breach type was payment card fraud. By incorporating these dummy variables, we can effectively capture and control for these variations, ensuring a more accurate assessment of the influence of breach type on our analysis and follow prior research (Rosati et al., 2019).

Time fixed controls

To capture the potential impact of macroeconomic factors on our analysis, we recognized the significance of temporal variations. As a result, we introduced control variables in the form of dummy variables for each year, month, and day of the week.

By including dummy variables for each year, we can control for any year-specific effects that may influence the variables under study. Economic conditions and trends can vary significantly from year to year, and these dummy variables enable us to isolate and account for such temporal fluctuations. Incorporating dummy variables for each year additionally assists in mitigating the breach fatigue phenomenon, wherein the increased frequency of breaches diminishes the impact on investors(Bischoff, 2019)

Similarly, incorporating dummy variables for each month enables us to control for any monthly patterns or seasonality in the data. For example the influence of the January effect (Lakonishok & Smidt, 1988).

Furthermore, introducing dummy variables for each day of the week allows us to control for any day-specific dynamics that may exist. Certain days of the week, such as Friday versus monday, may exhibit different returns due to the weekend effect (Lakonishok & Smidt, 1988). By including these dummy variables, we can adjust for such effects and obtain a more accurate understanding of the relationships within our analysis.

Analytical approach

To test the second hypothesis we estimate the following regression model:

$$CAR_{i,t} = \alpha_0 + a_1 \Delta TWEETS + a_2 X_t + a_3 V_{i,t} + a_4 B_{i,t} + \varepsilon_{i,t}$$

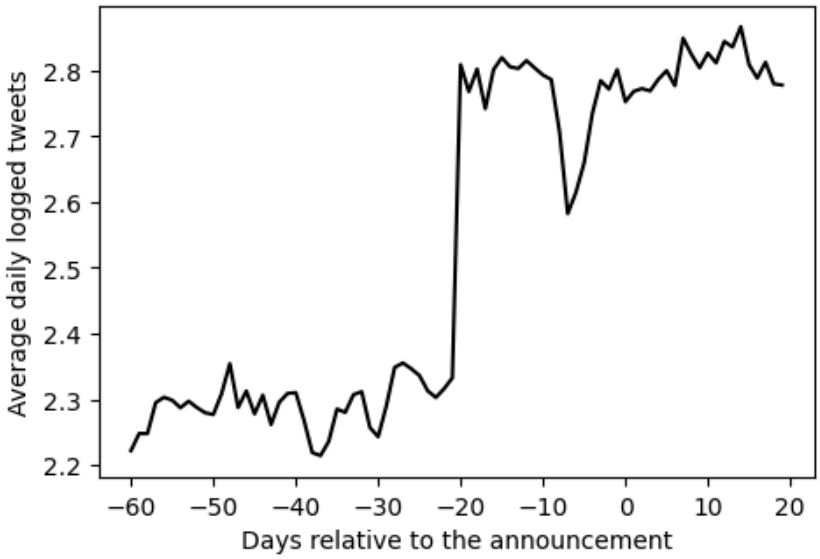
where *CAR* is the [-1,1] cumulative abnormal returns for firm *i* at announcement day *t*, and ΔTWEETS represents the difference in the average daily number of tweets mentioning the firm *i* during the period from 11 to 2 days before announcement day *t*, compared to the average daily number of tweets during the baseline window, which spans from 60 to 20 days before announcement day *t*. For the controls we have *X* which are the time fixed effects for the day *t*, *V* contains the firm-specific controls for the year preceding day *t*, lastly in *B* we control for breach specific effects. With these controls we follow previous research. (Foerderer & Schuetz, 2022; Rosati et al., 2019)

5. Results

Hypothesis 1

Figure 1 plots the average daily logged tweets over the time period of 60 days before to 20 days after a data breach announcement. This figure provides non-parametric evidence for hypothesis 1 as it shows that there is an increase of tweets 11 to 2 in the days before the announcement compared the days 60 to 20 days before the announcement.

Figure 1: Average logged tweets by day.



Notes: This plot shows the course of the average daily logged tweets surrounding the data breach. The x-axis represents the number of days relative to the announcement, while the y-axis represents the average count of logged tweets on that date.

In table 4 we have the regression results for the model for our first hypothesis, we see that both the constant and the parameter of the independent dummy variable are significant at the 0.1% level. Hypothesis 1 predicts that there is an increase in social media discourse about a firm prior to an data breach announcement, this is supported by the coefficient β_1 for the dummy variable which represents the expected change in the logged daily tweet count associated with a one-unit increase in the dummy variable. Since the dummy variable takes a binary value (0 or 1), it indicates whether the day falls within the 11 to 2 days before the announcement.

The overall R^2 value of the model indicates that only a portion of the variation in the dependent variable is explained by the independent variable. Looking at the between and within R^2 values, we observe that the dummy variable does not account for any variation between the firms. However, it does explain a portion of the variation within each individual firm. This is in line with our expectations.

To examine the actual change in the daily tweet count, we compare the exponentiated count when the dummy variable is zero to the exponentiated count when the dummy variable is one. Transforming the data back to its original scale provides a clearer understanding of the count in its natural form. Based on the estimated coefficients, we find that when the dummy

Table 4. PanelOLS Results

Parameter	Estimates
Constant β_0	2.384*** (0.006)
-11 to -2 day dummy β_1	0.347*** (0.018)
N	36207
R^2 (Between)	-0.123
R^2 (Within)	0.011
R^2 (Overall)	0.003
Entity fixed-effects	YES
Time fixed-effects	YES

Notes: OLS estimates, Standard errors are in parentheses.
+,*,** and *** indicate significance at the 10%,5%,1% and 0.1% levels, respectively.

variable equals zero, we expect an average daily count of approximately $e^{2.384} = 10.831$ tweets. This represents the expected count on days outside the 11 to 2 day range before the announcement.

Conversely, when the dummy variable equals one, indicating days falling within the 11 to 2 day range, we expect an average daily count of $e^{2.729} = 15.329$ tweets. This demonstrates a percentage increase of 41.52% in the expected daily count during this period compared to days outside the range, this increase supports our first hypothesis.

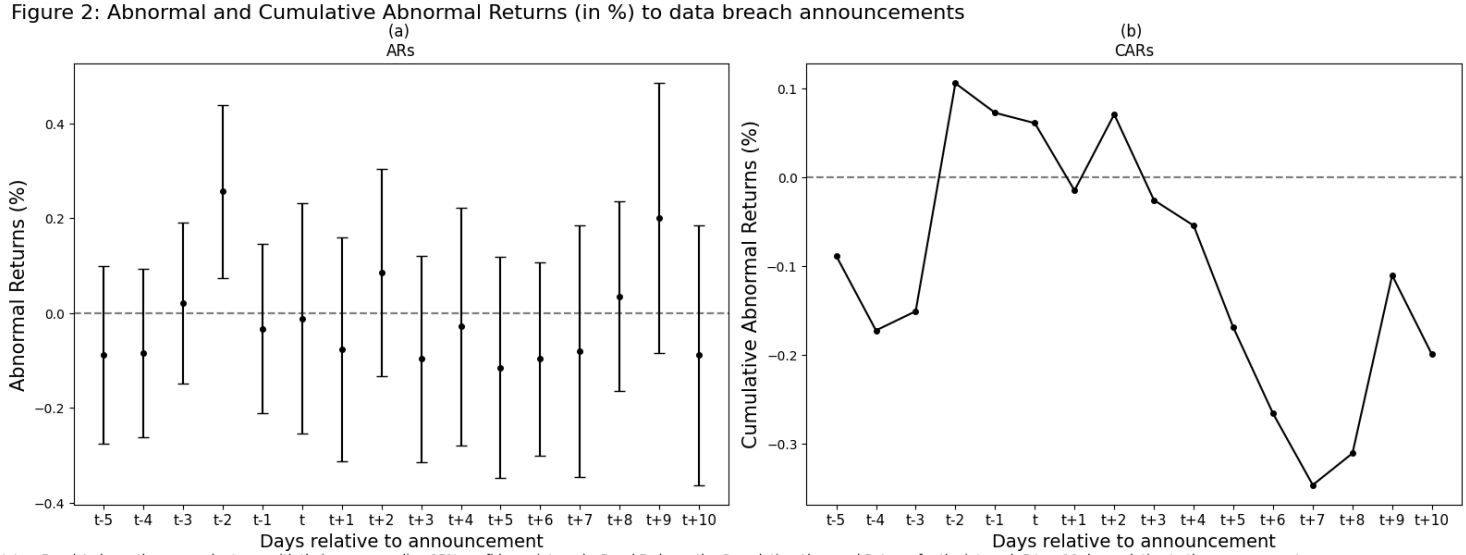
Hypothesis 2

For hypothesis 2, we first examine the abnormal returns and cumulative abnormal returns on the smaller sample of 321 data breach announcements without considering the change in average daily tweets following previous research (Froerder & Schaick (2022). Figure 2, Panel A displays the abnormal returns for each day along with their corresponding 95% confidence intervals. We observe that the day preceding the announcement and the day following the announcement exhibit negative abnormal returns; however, these returns are not statistically significant. Notably, at t-2, there is a significant positive abnormal return.

Moving to Panel B, we focus on the Cumulative Abnormal Returns (CAR) within the time window from t-5 to t+10. The CAR initially starts off in negative territory but turns positive at t-2, driven by the substantial positive abnormal return observed on that day. However, at t+1, the CAR temporarily dips below zero for one period before resuming a positive trend at t+3. Following t+3, the CAR consistently remains negative for the subsequent days. Indicating an overall negative CAR over the t-5 to t+10 time window.

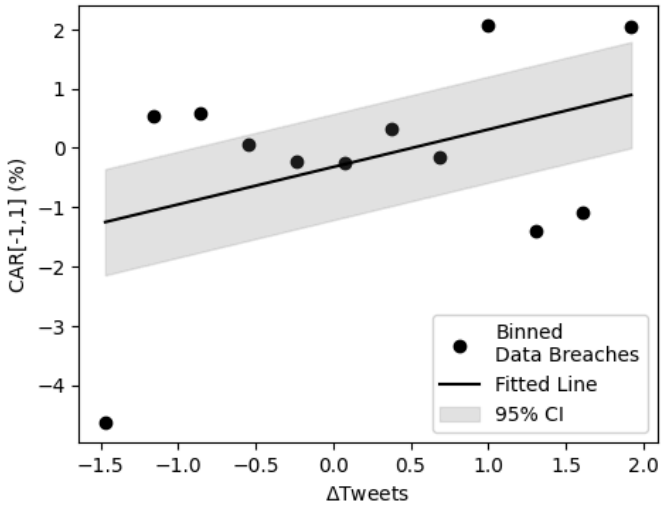
This analysis provides insights into the pattern of abnormal returns and cumulative abnormal returns, highlighting specific days where significant deviations from normal market performance are observed for when we don't

Figure 2: Abnormal and Cumulative Abnormal Returns (in %) to data breach announcements



Notes: Panel A shows the anormal returns with their corresponding 95% confidence intervals. Panel B shows the Cumulative Abnormal Returns for the interval -5 to +10 days relative to the announcemnt

Figure 3: Cumulative abnormal returns and average daily tweets



Notes: This figure plots the Cumulative Abnormal returns for the time interval of 1 day before to 1 day after the data breach announcement against the difference between the average daily tweets in the time inverval of 11 to 2 days before the announcement and the baseline daily average tweets.

account for a change in tweets in the period before an announcement.

Figure 3 plots the cumulative abnormal returns against the difference in average daily tweets in the 11 to 2 days before an announcement compared to a baseline average daily tweets, it provides non-parametric evidence for hypothesis 2 where we can see that there is a positive correlation between daily average tweets before an announcement and the cumulative abnormal returns.

The descriptive statistics for the variables used in the regression analysis are provided in Table 4. Upon analysing the sample, it becomes evident that the cumulative abnormal returns for the time period one day before to one day after the announcement exhibit a negative mean, indicating a negative price reaction following the data breach announcement. This negative trend is also visually observable in Figure 1, Panel B. Furthermore, this sample reveals a negative mean for the ΔTWEETS variable, indicating that on average, there is a decrease in the daily average number of tweets in the days preceding the announcement.

Table 5 displays the regression results obtained for hypothesis 2. The coefficient corresponding to the difference in daily average tweets is positive and statistically significant,

Table 4: Summary statistics.

	N	Mean	SD	Min.	Median	Max.
CAR[-1,1] %	321	-0.034	2.510	-10.788	-0.049	15.685
ΔTWEETS	321	-0.109	0.493	-1.623	-0.087	2.076
log(Assets + 1)	321	10.629	2.251	5.471	10.462	15.035
log(CAPEX +1)	321	4.750	2.617	0.000	5.152	9.920
log(OPEX + 1)	321	9.323	1.428	5.387	9.255	13.163
EBIT	321	8692.400	17011.418	-10253.000	1881.000	72903.000

indicating that an increase in daily average tweets prior to a data breach announcement is associated with a reduction in negative market reactions.

Additionally, the intercept term in the regression model is negative, though only marginally significant at the 10% level (p-value = 0.054). This finding aligns with recent previous research (Froeder & Schaik, 2022) which documents negative intercept for the [1,1] event window. The negative intercept term suggests that the model predicts a negative market reaction to data breaches, when all other variables are equal to zero. The reported regression parameter for the change in average logged daily tweets provides empirical support for hypothesis 2. That is when the average daily tweets increase in the days before the announcement it has a positive effect on the cumulative abnormal returns indicating a reduction of the negative market reaction to a data breach announcement.

Table 5. Regression results

Variable	CAR [-1,1] (%)
ΔTWEETS	0.704** (0.315)
INSD	0.754 (0.672)
PORT	-0.239 (0.957)
PHYS	0.431 (0.599)
HACK	0.299 (0.441)
DISC	0.195 (0.520)
STAT	-0.186 (1.256)
CARD	-0.136 (0.629)
log(Assets + 1)	-0.092 (0.116)
log(CAPEX +1)	-0.076 (0.081)
log(OPEX + 1)	0.369** (0.172)
EBIT	-0.000009 (0.000016)
Intercept (α_0)	-5.739+ (2.969)
N	321
R^2	0.135
Adj R^2	0.004
Time fixed effects	YES

Notes: OLS estimates, Standard errors are in parentheses.
+,*,** and *** indicate significance at the 10%,5%,1% and 0.1% levels, respectively.

6. Discussion

The research presented in the thesis aimed to investigate the role of ex-ante social media engagement and impression management strategies in shaping market reactions to data breach announcements. The study addresses two hypotheses (1) there is a higher level of social media about a firm in the days before a data breach announcement, and (2) a higher level of social media discourse about a firm in the days before a data breach announcement decreases the negative effect of the announcement on cumulative abnormal returns.

6.1 Contributions

The findings of this study contribute to the research and theory on the intersection of social media, impression management, data breaches, and market reactions. First, the study provides empirical evidence supporting the hypothesis that there is a higher level of social media about a firm in the days before a data breach announcement. The analysis revealed a significant increase in the average daily tweet count during the 11 to 2 days interval before the announcement compared to earlier periods, indicating a potential proactive effort by firms to shape public perception and manage potential negative reactions. This finding extends our understanding of the presence of impression management practices in the context of data breaches and highlights the role of social media in impression management.

Second, the study contributes to the literature on confounding factors to the market reaction on data breaches. Where prior research showed conflicting results about the market reaction on data breaches (e.g. Bolster et al., 2010; Cavusoglu et al., 2004; Garg et al., 2003; Goel & Shawky, 2009; Hilary et al., 2016; Yayla & Hu, 2011) and other research found factors that influence this market reaction. (Foerderer & Schuetz, 2022; Gatzlaff & McCullough, 2010; Morse et al., 2011; Rosati et al., 2019). Our research showed a new factor, demonstrating the impact of social media discourse prior to the announcement on market reactions to data breach announcements. The analysis revealed that a higher level of social media discourse about a firm in the days leading up to a data breach announcement was associated with a decrease in the negative effect on cumulative abnormal returns. This suggests that firms can effectively leverage social media engagement as a preemptive measure to attenuate the adverse market reactions caused by data breach announcements. The findings shed light on the importance of strategic communication and active engagement on social media platforms in managing the financial consequences of data breaches.

6.2 Practical Implications

From a practical standpoint, the findings of this study have significant implications for firms and organisations facing data breach incidents. The

results underscore the importance of increasing the level of social media discourse about the firm by for example implementing proactive impression management strategies on social media. By strategically shaping public perception and reducing negative sentiment through active engagement on social media, firms have the potential to mitigate the adverse effects on their stock market performance and reputation. This suggests that firms should invest in developing effective social media strategies and allocate resources to monitor and engage with online discussions related to data breach incidents.

However, it is important to consider the perspective for customers highlighted by Froeder and Schaik (2022). There is a negative impact of impression management on consumers whose data is entrusted to the firm. While an impression management strategy may help alleviate the consequences for the company, it is crucial for the well-being of consumers that efforts are also directed towards strengthening data protection measures. Allocating time and resources to safeguarding customer data can ultimately provide greater benefits and instil confidence in the firm's commitment to data security.

For legislators, this study highlights the fact that when firms have the opportunity to take preemptive measures before publicly announcing a data breach, it may mitigate the intended effects of legislation. Legislators aim to protect customers by mandating the firms to announce their data breaches publicly, leading to economic or reputational damage, in order to encourage better protection for customer data. Therefore, policymakers may consider shortening the time frame for firms to disclose a data breach once it has been detected.

6.3 Limitations

Despite its contributions, this study has certain limitations that should be acknowledged. First, although an increase in social media discourse about a firm before a data breach announcement may suggest the presence of impression management efforts, we cannot definitively conclude that firms engage in impression management based solely on this observation. Therefore, further research is needed to delve deeper into the specific social media strategies employed by firms in the context of data breaches. Furthermore, it is important to note that this study primarily focused on analysing the volume of tweets and did not delve into the sentiment expressed on social media regarding a firm prior to a data breach announcement. Therefore, our findings do not provide insights into the specific sentiment associated with social media engagement during this period. Future research endeavours could explore the sentiment analysis of social media discourse preceding a data breach announcement and examine the potential impact of sentiment on market reactions to data breaches.

Additionally, the study primarily relied on Twitter data and stock market data, neglecting other social media platforms and alternative measures of market reactions. Incorporating a broader range of social media platforms and utilising additional financial metrics could provide a more comprehensive understanding of the relationship between social media discourse and market reactions to data breaches.

6.4 Conclusion

Given the growing prevalence of social media and the conflicting findings regarding market reactions to data breaches, this study aimed to explore two key aspects: first, whether there is an increase in social media discourse about a firm prior to announcing a data breach, indicating the potential use of impression management strategies by firms, and second, whether the level of social media discourse about the firm impacts the market reaction to the data breach announcement. By investigating two hypotheses we found a significant increase in daily tweets during the 11 to 2 days interval leading up to a data breach announcement, suggesting the possibility of strategic utilisation of impression management by firms. Additionally, we observed that this increase in social media discourse was associated with a mitigated negative market reaction to the data breach announcement. These findings shed light on the absence of a confounding variable in previous studies, which overlooked the impact of the level of social media discourse before a data breach announcement.

Annual Data Breach Report. (2022). *ITRC*. Retrieved 10 July 2023, from https://www.idtheftcenter.org/publication/2022-data-breach-report/

Aral, S., Dellarocas, C., & Godes, D. (2013). **Introduction to the Special Issue** —Social Media and Business Transformation: A Framework for Research. *Information Systems Research*, *24*(1), 3–13. https://doi.org/10.1287/isre.1120.0470

Benthaus, J., Risius, M., & Beck, R. (2016). Social media management strategies for organizational impression management and their effect on public perception. *The Journal of Strategic Information Systems*, *25*(2), 127–139. https://doi.org/10.1016/j.jsis.2015.12.001

Bischoff, P. (2019, November 6). How data breaches affect stock market share prices. *Comparitech*. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

Bolino, M. C., Kacmar, K. M., Turnley, W. H., & Gilstrap, J. B. (2008). A Multi-Level Review of Impression Management Motives and Behaviors. *Journal of Management*, *34*(6), 1080–1109. https://doi.org/10.1177/0149206308324325

Bolster, P., Pantalone, C. H., & Trahan, E. A. (2010). Security Breaches and Firm Value. *Journal of Business Valuation and Economic Loss Analysis*, *5*(1). https://doi.org/10.2202/1932-9156.1081

BUSINESS AND COMMERCE CODE CHAPTER 521. UNAUTHORIZED USE OF IDENTIFYING INFORMATION. (2009). https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market*. *Journal of Computer Security*, *11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Dijkmans, C., Kerkhof, P., & Beukeboom, C. J. (2015). A stage to engage: Social media use and corporate reputation. *Tourism Management*, *47*, 58–67. https://doi.org/10.1016/j.tourman.2014.09.005

Elsbach, K. D., Sutton, R. I., & Principe, K. E. (1998). Averting Expected Challenges Through Anticipatory Impression Management: A Study of Hospital Billing. *Organization Science*, *9*(1), 68–86. https://doi.org/10.1287/orsc.9.1.68

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, *25*(2), 383–417. https://doi.org/10.2307/2325486

Fama, E. F., & French, K. R. (1993). Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics*, *33*(1), 3–56. https://doi.org/10.1016/0304-405X(93)90023-5

Foerderer, J., & Schuetz, S. W. (2022). Data Breach Announcements and Stock Market Reactions: A Matter of Timing? *Management Science*, *68*(10), 7298–7322. https://doi.org/10.1287/mnsc.2021.4264

Garg, A., Curtis, J., & Halper, H. (2003). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Systems Security*, *12*(1), 22–33. https://doi.org/10.1201/1086/43325.12.1.20030301/41478.5

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, *13*(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

General Law—Part I, Title XV, Chapter 93H, Section 3. (n.d.). Retrieved 10 July 2023, from https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section3

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

Gomez-Carrasco, P., & Michelon, G. (2017). The Power of Stakeholders' Voice: The Effects of Social

Media Activism on Stock Markets. *Business Strategy and the Environment*, *26*(6), 855–872. https://doi.org/10.1002/bse.1973

Hanna, R., Rohm, A., & Crittenden, V. L. (2011). We're all connected: The power of the social media ecosystem. *Business Horizons*, *54*(3), 265–273. https://doi.org/10.1016/j.bushor.2011.01.007

Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-Risk Disclosure: Who Cares?* (SSRN Scholarly Paper No. 2852519). https://doi.org/10.2139/ssrn.2852519

Johnson, M., Kang, M. J., & Lawson, T. (2017). Stock Price Reaction to Data Breaches. *Journal of Finance Issues*, *16*(2), Article 2. https://doi.org/10.58886/jfi.v16i2.2263

Kannan, K., Rees, J., & Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91. https://doi.org/10.2753/JEC1086-4415120103

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241–251. https://doi.org/10.1016/j.bushor.2011.01.005

Lakonishok, J., & Smidt, S. (1988). Are Seasonal Anomalies Real? A Ninety-Year Perspective. *The Review of Financial Studies*, *1*(4), 403–425. https://doi.org/10.1093/rfs/1.4.403

Lee, L. F., Hutton, A. P., & Shu, S. (2015). *The Role of Social Media in the Capital Market: Evidence from Consumer Product Recalls* (SSRN Scholarly Paper No. 2557212). https://doi.org/10.2139/ssrn.2557212

MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, *35*(1), 13–39.

Mohamed, A. A., Gardner, W. L., & Paolillo, J. (1999). A Taxonomy of Organizational Impression

Management Tactics. *Advances in Competitiveness Research*. https://www.semanticscholar.org/paper/A-Taxonomy-of-Organizational-Impression-Management-Mohamed-Gardner/8575026a0c85da3bca7aa55f57b5aea030fc9533

Morse, E., Raval, V., & Wingender, J. (2011). Market Price Effects of Data Security Breaches. *Information Security Journal: A Global Perspective*, *20*, 263–273. https://doi.org/10.1080/19393555.2011.611860

Nijhuis, M. (2022, March 3). Company Name Matching. *DNB—Data Science Hub*. https://medium.com/dnb-data-science-hub/company-name-matching-6a6330710334

Privacy Rights Clearinghouse Data breaches. (2023). PrivacyRightsClearinghouse. https://privacyrights.org/data-breaches

Ranco, G., Aleksovski, D., Caldarelli, G., Grčar, M., & Mozetič, I. (2015). The Effects of Twitter Sentiment on Stock Price Returns. *PloS One*, *10*(9), e0138441. https://doi.org/10.1371/journal.pone.0138441

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, *47*, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4), 103638. https://doi.org/10.1016/j.im.2022.103638

Schniederjans, D., Cao, E. S., & Schniederjans, M. (2013). Enhancing financial performance with social media: An impression management perspective. *Decision Support Systems*, *55*(4), 911–918. https://doi.org/10.1016/j.dss.2012.12.027

SEC Says Social Media OK for Company Announcements if Investors Are Alerted. (2013). https://www.sec.gov/news/press-release/2013-2013-51htm

State Data Breach Notification Laws | Foley & Lardner LLP. (n.d.). Retrieved 10 July 2023, from https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws

Syed, R., & Dhillon, G. (n.d.). *Dynamics of Data Breaches in Online Social Networks: Understanding Threats to Organizational Information Security Reputation*.

Yayla, A. A., & Hu, Q. (2011). The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4

Zohrehvand, A. (2020). M&As and CEOs: Machine Learning Aided Analyses of Social Media [Doctoral, UCL (University College London)]. In *Doctoral thesis, UCL (University College London)*. UCL (University College London). https://discovery.ucl.ac.uk/id/eprint/10117933/

Zohrehvand, A., Doshi, A. R., & Vanneste, B. (2023). *Generalizing Event Studies Using Synthetic Controls: An Application to the Dollar Tree–Family Dollar Acquisition* (SSRN Scholarly Paper No. 3856879). https://doi.org/10.2139/ssrn.3856879

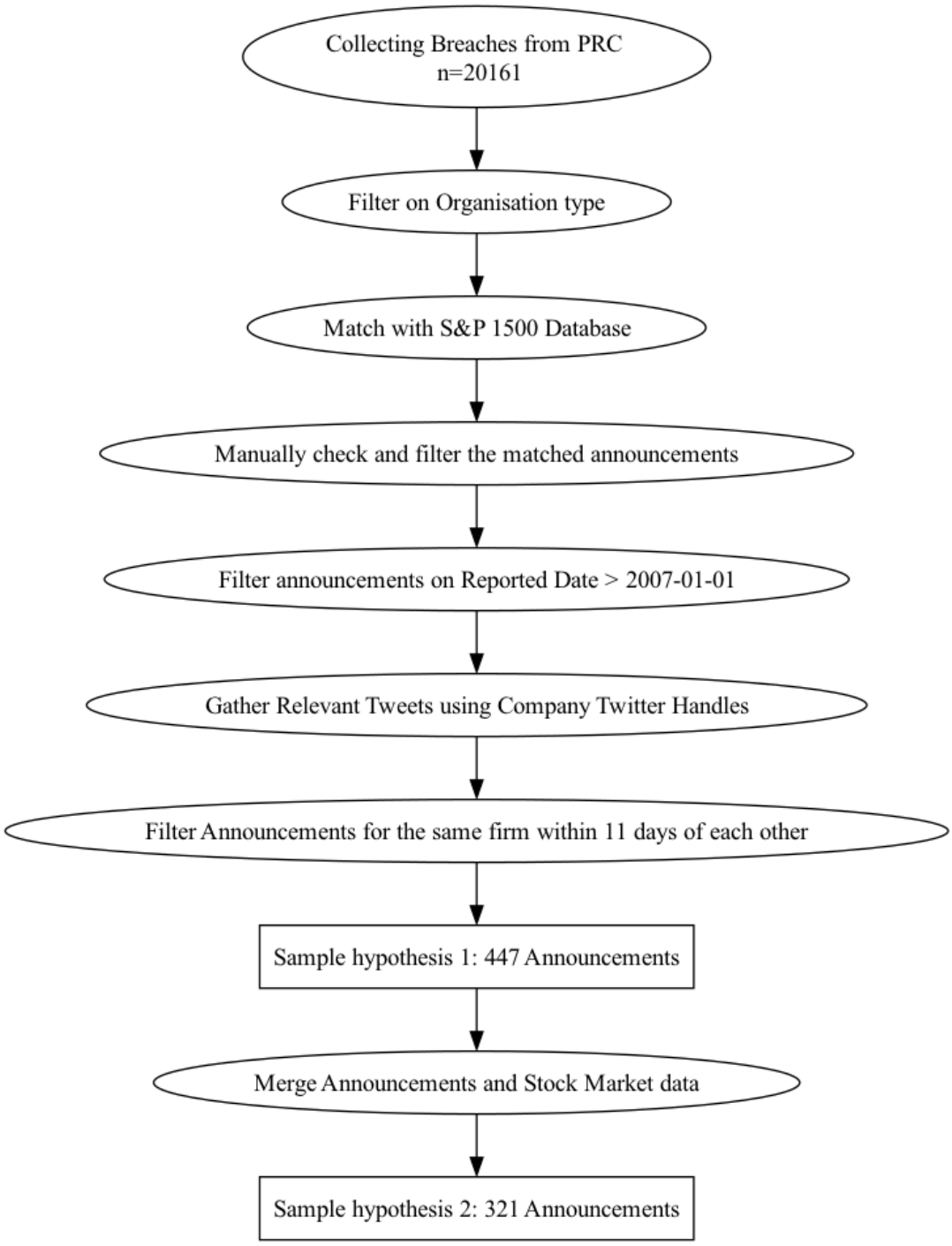
APPENDIX A

Table 1. Privacy Rights Clearinghouse organisation labels

Type of Organisation	Description
BSF	Businesses (Financial Services, Banking, Insurance Services)
BSO	Businesses (Manufacturing, Technology, Communications, Other)
BSR	Businesses (Retail/Merchant including Grocery Stores, Online Retailers, Restaurants)
EDU	Educational Institutions (Schools, Colleges, Universities)
GOV	Government & Military (State & Local Governments, Federal Agencies)
MED	Healthcare and Medical Providers (Hospitals, Medical Insurance Services)
NGO	Nonprofits (Charities and Religious Organisations)
UNKN	Unknown

Table 2. Privacy Rights Clearinghouse breach labels

Type of Breach	Description
CARD	Fraud Involving Debit and Credit Cards Not Via Hacking
HACK	Hacked by an Outside Party or Infected by Malware
INSD	Insider (employee, contractor or customer)
PHYS	Physical (paper documents that are lost, discarded or stolen)
PORT	Portable Device (lost, discarded or stolen laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape, etc.)
STAT	Stationary Computer Loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility)
DISC	Unintended Disclosure Not Involving Hacking, Intentional Breach or Physical Loss (sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax)
UNKN	Unknown (not enough information about breach to know how exactly the information was exposed)


Collecting Breaches from PRC
n=20161
Filter on Organisation type
Match with S&P 1500 Database
Manually check and filter the matched announcements
Filter announcements on Reported Date > 2007-01-01
Gather Relevant Tweets using Company Twitter Handles
Filter Announcements for the same firm within 11 days of each other
Sample hypothesis 1: 447 Announcements
Merge Announcements and Stock Market data
Sample hypothesis 2: 321 Announcements