Summer 6-27-2016

WHO WINS IN A DATA BREACH? - A COMPARATIVE STUDY ON THE INTANGIBLE COSTS OF DATA BREACH INCIDENTS

Griselda Sinanaj
University of Göttingen, griselda.sinanaj@wiwi.uni-goettingen.de

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

WHO WINS IN A DATA BREACH? - A COMPARATIVE STUDY ON THE INTANGIBLE COSTS OF DATA BREACH INCIDENTS

Griselda Sinanaj, Chair of Electronic Finance and Digital Markets, University of Göttingen, Göttingen, Germany, griselda.sinanaj@wiwi.uni-goettingen.de

Humayun Zafar, Coles College of Business, Kennesaw State University, Kennesaw, GA, USA, hzafar@kennesaw.edu

Abstract

Over the years data breaches have become a status quo due to an attacker's repeated ability to successfully infiltrate networks. 2015 was no stranger to these cases. Victims included millions of customers of Anthem, BlueCross BlueShield, Experian/T-Mobile, and Office of Personnel Management, all of whom lost confidential data. Needless to say, data breaches have a significant impact on the financial performance and reputation of firms. Collectively, the majority of the previous security studies on breach announcements have used event study methodology. These studies have focused on the change in market value of the company within a few days of the security breach announcements and concluded that there is a negative impact. But what is the impact of negative publicity due to a data breach on an organization's reputation? How should that be gauged? In this study we compare the financial impact with the reputational damage of data breaches. We performed two event studies: an event study on stock prices and additionally a sentiment event study applied on social media data. In contrast to previous research, shareholders do not react negatively to data breach announcements, whereas the impact on reputation is statistically significant as negative.

Keywords: Data Breaches, Corporate Reputation, Event Study, Sentiment Analysis.

1 INTRODUCTION

Data breaches, which involve the loss or theft of personally identifiable information (Romanosky et al. 2011, p. 256), are crisis events that interrupt the normal progress of daily business activities (Gupta & Ranganathan 2007) and might be very costly for the affected organisations (Ko & Dorantes 2006). Companies having experienced data breach incidents may incur in either tangible costs, such as decreased earnings (Xu et al. 2008) or intangible costs, such as loss of consumer trust (Nofer et al. 2014), loss of productivity and reputation damage (Yayla & Hu 2011). In the last decade, a large body of research in the information security literature has investigated the intangible impact of security breaches, in particular the impact of data breach events on investors' confidence and shareholder wealth (e.g. (Acquisti et al. 2006; Campbell et al. 2003; Gatzlaff & McCullough 2010; Hinz et al. 2015; Morse et al. 2011). Despite the economic and strategic relevance of corporate reputation (Fombrun & Riel 1997) and the reputational risks which arise in crisis situations (Dean 2004), scholars have devoted little attention to the investigation of the impact that data breaches have on reputation.

For the scope of this research, reputation is defined as "the overall opinion about a firm by customers, investors, employees and the general public" (Colleoni et al. 2011, p. 4). A favourable reputation is a valuable economic asset that generates positive outcomes in terms of competitive advantage and business continuity (Fombrun & Riel 1997). Data breaches might have an adverse impact on corporate reputation because of the negative publicity in the news media (Dean 2004) and the transfer of negative information from traditional news media to social media, contributing to the creation of negative word-of-mouth (Coombs 2007). Crisis events draw the attention of a large number of users on social media platforms, who actively engage in online communities to discuss and express their own opinion on the event (Jin et al. 2011). Information related to crisis events posted in the social media have the power to negatively influence perceptions and judgements on a company and thus on its reputation because it is considered by users as a trustworthy information source (Colleoni et al. 2011). As little efforts have been devoted to the reputational impact of data breaches, we argue that more research is needed to better understand the longevity and severity of reputational effects, which is necessary to develop effective crisis management strategies.

In this study we performed a comparative analysis between the reputational effect of data breaches and the impact on shareholder value. First, we measured the impact of data breach events on shareholder value by using the event study approach. In a further step, to quantify the effect of data breach events on corporate reputation we applied the event study approach on social media data. To measure overall user mood, we calculated daily average sentiment in regard to the companies in the sample and then similarly to the classic event study approach, we calculated abnormal sentiment values (and cumulative abnormal sentiment) to measure the impact on reputation. The results were surprising. Cumulative abnormal returns are not statistically significant over the entire event window. The opposite holds for cumulative abnormal sentiment values, which are statistically significant, meaning that data breach events have a negative impact on corporate reputation. Contrary to what previous empirical studies have reported, in actuality shareholders do not react to the announcement of data breach events and completely ignore them. While the judgements and the evaluations of investors on the future economic performance of the companies seem not to be affected from data breach incidents, the overall judgement of users seem to suffer from data breach announcements. From a theoretical perspective, our results contradict previous literature, which have consistently reported a significant negative impact of data breach incidents on the stock market. Since the literature is overwhelmed with studies measuring the impact of data and security breach events on the capital market, research efforts should be focused on other important intangible effects, such as corporate reputation. Only through a deep understanding of the effects and consequences of data breach events, companies can develop optimal crisis response strategies with the scope of mitigating reputational losses.

The remainder of the paper is organized as follows. In section 2 we describe the efficient market hypothesis theory and develop the research hypotheses, after having described the relevant literature. In

section 3 we describe the sample selection process for both event studies. Section 4 presents the methodological approach. Hereby we used the event study method to measure the effect of data breaches on stock prices and the event study combined with the sentiment analysis to measure corporate reputation. The results are presented and discussed in section 5. The study concludes with a summary of the findings and offers suggestions and recommendations for future research opportunities.

2 THEORETICAL BACKGROUND

In this section we describe the relevant literature pertaining to the research objectives and develop the research hypotheses. We first describe the efficient market hypothesis, the theoretical fundament of the event study methodology. In addition, we analyse the body of research investigating the relation between security breach incidents and capital market reaction and derive the first hypothesis. Finally, we describe the theoretical link between the concept of reputation, social media and security breaches, in this study and generally named as crisis events, and derive the second hypothesis.

2.1 Efficient Market Hypothesis (EMH)

This study investigates the impact of data breaches on corporate reputation and on market value. Hereinto we performed two event studies: a classical event study on stock prices and additionally, a sentiment event study applied on social media data. The theoretical basis of the event study method is EMH, considered to be one of the most influential financial theories in modern finance. The theory, developed by Fama in 1969, is built upon the assumption of investor's rationality and postulates that markets are efficient when they fully and quickly reflect all the available information. Market efficiency assumes three different forms, depending on the type of information incorporated in the stock prices: (i) markets are efficient in the weak-form if stock prices reflect only the information concerning past historical returns; (ii) in the semi-strong form, prices reflect not only information on past returns but also publicly available information to all market participants. Public information is defined as relevant information for stock prices movements, such as dividend announcements, stock splits, earnings announcements, mergers and acquisitions etc.; (iii) strong-form, i.e. stock prices fully incorporate three sets of information: information on past prices, public information and private information. EMH goes hand in hand with the Random Theory, which states that future prices follow a random walk and are therefore not predictable (Fama 1970, p. 383).

EMH, which has been embraced for several decades by economists to explain the behaviour of financial markets, has been heavily criticized in the last decades by behavioural economists. Behavioural finance, which focuses on the psychological and sociological aspects of finance, challenges the theoretical foundations of the EMH and provides empirical evidence that markets are inefficient (Shleifer 2000). Anomalies and deviations from the EMH and market efficiency have been documented in several studies (e.g. Bondt & Thaler 1985). In an attempt to overcome the limitations of the EMH, Lo developed the "Adapted Market Hypothesis", a concept which binds together the classical form of the EMH with concepts of behavioural finance and psychology (Lo 2004). Financial markets are not static environments, but they are rather described as dynamic ecological systems subject to continuous changes in the course of time. The author applies concepts borrowed from the discipline of evolutionary biology to explain market efficiency: competition, adaptation and natural selection. As markets evolve, the combination and the interaction of the aforementioned forces dictate the degree of efficiency the market can achieve (Lo 2005). This framework offers thus a common solution for both opponents and supporters of the EMH.

2.2 Intangible Costs of Security Breaches

2.2.1 Impact of Data Breach Announcements on Shareholder Value

Security breach incidents are problematic because they might expose the affected organisations to a long list of added costs. These costs might be tangible or intangible (reputational damage, loss of consumer trust, loss of market value) and might arise either short after the event announcement or months later (Ko & Dorantes 2006). Economics of information security is the research stream within the information security literature investigating the economic consequences of security breach incidents at the organisational level (Camp & Lewis 2006). In particular, the quantification of the intangible costs represents the biggest challenge for researchers as these costs are difficult to quantify (Cavusoglu et al. 2004). Most of the existing research on information security breaches has focused on the empirical investigation of the financial impact of these events. Hereby scholars applied the event study method to determine if these events will be negatively perceived by investors and will cause negative abnormal returns. This body of research has delivered mixed results. Table 1 offers a summary of the most relevant studies, which we classified in two groups, based on the significance of the empirical results. As can be seen from Table 1, the majority of the studies have shown that security breaches are perceived negatively by investors and have an adverse effect on firms' stock prices. Additionally, while security breaches, which entail the whole spectrum of security incidents and not solely data breaches are not always associated with a pronounced negative reaction on the capital market, the effect of data breaches on stock prices is systematically negative and strongly significant. With regard to the type of breach, one part of the studies focus on all types of security breaches, while others deal with one particular type of security breach. The studies of Acquisti et al. (2006); Gatzlaff and McCullough (2010); Hinz et al. (2015) measure the financial impact of data breach events, which imply the loss or theft of private sensitive information, whose improper use might lead to identity theft (Romanosky et al. 2011). All the studies report statistically significant negative cumulative abnormal returns around the event date.

Author(s)	**Breach type**	**Event window**
Negative and statistically significant *cumulative abnormal returns (CAR)*		
(Acquisti et al. 2006)	Data breaches	(-1;+1)
(Campbell et al. 2003)	Confidential data	(-1;+1)
(Cavusoglu et al. 2004)	Security breaches	(0;+1)
(Hinz et al. 2015)	Data theft	(0;+3)
(Gordon et al. 2011)	Security breaches	(-1;+1)
(Gatzlaff & McCullough 2010)	Data breaches	(-1;0) (0;+39)
(Pirounias et al. 2014)	Data breaches	(0;0)
(Yayla & Hu 2011)	Security breaches	(-1;+1) (-1;+10)
Cumulative abnormal returns (CAR) not significant		
(Hovav & D'Arcy 2003)	Denial-of-Service attacks	
(Hovav & D'Arcy 2004)	Computer virus	
(Kannan et al. 2007)	Security breaches	

Table 1. Overview of studies investigating the impact of security breaches on stock prices

The second part of the table presents the studies that do not report a significant effect of security breach incidents on shareholder value. Hovav and D'Arcy (2003) and Hovav and D'Arcy (2004), who investigated the financial impact of computer viruses and DOS attacks, found that these events have a light negative effect on stock prices which isn't statistically significant. Unlike data breaches, computer viruses and DOS attacks do not involve the breach of personal private information, such as customer or employee data. While computer viruses might damage either information integrity or information availability, DOS attacks, e.g. shutdown of a website, are described as availability breaches, as they impede users to access the desired information (Gordon et al. 2011).

In line with previous research (Acquisti et al. 2006; Gatzlaff & McCullough 2010; Hinz et al. 2015), this study also investigates the impact of data breach incidents on shareholder value. While the majority of the studies described above, with few exceptions, focus exclusively on companies traded at a U.S. stock exchange, we in our sample also included companies from different countries. Based on these theoretical considerations, we formulate the first research hypothesis as follows:

Hypothesis 1: The announcement of data breach events will be negatively reflected into the stock market and will cause negative abnormal returns.

2.2.2 Impact of Data Breach Announcements on Corporate Reputation

A crisis "is a major occurrence with a potentially negative outcome affecting an organization, company, or industry, as well as publics, products, services or good name. A crisis interrupts normal business transactions and can sometimes threaten the existence of the organization" (Fearn-Banks 2010, p. 2). Therefore crisis events indicate unexpected and sudden negative events, such as an earthquake, fire, explosion, security breach, natural disaster, which create an emergency situation that necessitates quick responses (Gupta & Ranganathan 2007). Organisations fear crisis events because they might have an adverse impact both at the stakeholder and at the organisational level (Coombs 2007). Crisis events might produce a wide range of negative economic consequences on the affected organisations: loss of sales, damage of corporate reputation and brand image and even threaten the existence of the company (Coombs 2014). Once the data breach incident has been discovered, the affected companies take several actions to repair the compromised infrastructure, investigate the incident causes and identify the authors. These expenses imply tangible costs, whereas reputation damage, loss of consumer trust and loss of shareholder wealth are known as intangible costs (Cavusoglu 2002; Kannan et al. 2007).

Because crisis events have the potential to damage the asset of reputation (Coombs 2007), the study of the impact of crisis events on organizational reputation has received significant attention among communication research scholars (Cooley & Cooley 2011). The amount of reputational damage caused by crisis situations depends to a large extent on the post-crisis response strategy that the affected companies take. As there is no general consensus or a specific guideline to define the optimal response strategy, scholars develop new theories to cover this theoretical gap (Coombs & Holladay 2002). With this regard, Situational Crisis Communication Theory (SCCT) was developed to contribute to this knowledge gap and represents one of the leading theories in crisis communication research. Attribution of responsibility, i.e. the level of responsibility the public appoints to the organization for the crisis event is the key variable of SCCT and is directly related to reputational threat. According to SCCT, intentional crisis events are associated with higher levels of responsibility and lead to a stronger negative impact on reputation. Unintentional crisis events are in contrast due to external factors and are characterized by a lower level of crisis responsibility and thus have a milder impact on reputation. SCCT posits that crisis response plans should take into account three factors: type of crisis event, level of crisis responsibility and reputational damage (Coombs 2007; Coombs & Holladay 2002).

The measurement of corporate reputation has for many years been object of study among reputation scholars (Rindova et al. 2005; Wartick 2002). Different reputation measurement approaches are available in the literature, such as reputation surveys, the Reputation Quotient (Fombrun et al. 2000), RepTrak™ Pulse (Ponzi et al. 2011) etc. America's Most Admired Companies index (AMAC), for the first time released in 1984 by *Fortune*, is the first and at the same time the most popular reputation

measure in research (Sarstedt et al. 2013). With the advent and rapid diffusion of social media, more research efforts have been invested on corporate reputation measurement. The goal is to develop novel measurement approaches that overcome the drawbacks of the traditional existent approaches (Colleoni et al. 2011).

In recent years researchers have proposed new reputation measures derived from social media content. The study of Benthaus et al. (2013) is one of the first to propose a novel reputation measure which resumes the opinions and judgements of social media users. Reputation measures developed from social media content have several advantages over traditional survey-based approaches. Surveys built upon the opinions and knowledge of managers and financial analysts, whereas social media sentiment reflects public's opinion. In addition, social media-based reputation measures can be calculated within a short time, in contrast to reputation surveys (Benthaus et al. 2013).

The investigation of the reputational effect of data breach incidents has received little attention in research. In the context of data breach incidents, the study of Sinanaj et al. (2015) applies a sentiment based event study to measure the reputational impact of data breaches. The metric used to quantify reputation is abnormal sentiment, i.e. the difference between actual sentiment and expected sentiment. In line with the study of Sinanaj et al. (2015), we also applied a sentiment based event study.

To summarize, given the variety of reputation measures the biggest challenge for reputation scholars in the future will be the development of a widely accepted reputation measure that best captures the multidimensional character of reputation and overcomes the limitations of the traditional measurement approaches. Based on this theoretical background, we derive the second research hypothesis:

Hypothesis 2: Data breach events are perceived negatively by social media users and have a negative impact on corporate reputation.

3 SAMPLE SELECTION AND DATA

In this paper we performed two analysis: first, we analysed the impact of data breaches on capital market based on the event study method. Furthermore, we conducted a sentiment event study on social media data. To determine the final samples for both analysis we applied several selection criteria: common selection criteria and specific criteria to each approach. We collected data breach incidents through the global database datalossdb.org, which offers a chronological history of data breach events occurred worldwide. The website of datalossdb.org is curated by volunteers, who constantly enlarge the database by inserting the latest data breach events announced through traditional media outlets. For each data breach listed in the database, the following information is given: date of event, name of organization(s), location, source of breach (inside accidental, inside malicious, outside, unknown), breach type (hack, stolen laptop, fraud-se, lost tape, missing media and unknown) as well as news media reports. Several information security studies have used datalossdb.org to investigate the economic impact of security breach incidents (Hinz et al. 2015; Morse et al. 2011; Pirounias et al. 2014).

The initial sample of data breaches comprised events occurred between 1.11.2011 and 31.12.2013. Because of the classical event study method, we selected only publicly traded companies and accordingly removed GOs, education institutions and non-profit organizations. The next criteria regards loss size. We focused on breaches having affected a large number of customers (number of ID's lost/stolen at least 10.000) as for these events it is reasonable to expect a relevant economic impact, in contract to less relevant incidents. When performing the event study it is essential to remove from the sample the events having experienced other business events i.e. confounding events (e.g. departure of directors, dividend announcements etc.) over the event window (-1;+10). By doing so, we are able to isolate the net effect of the breach events both on capital market and social media. Next we apply specific criteria for the classical event study and the social media event study. The requisite for the adapted event study is social media data availability for all the companies in the sample over the estimation- and event window, i.e. over the window (-44;+10). The source of social media data is SDL-SM2, a proprietary social media monitoring software, which provides historical social media data for businesses from

different social media platforms such as microblogs, social networks and blogs. For the classical event study approach we considered only listed firms during the estimation- and the event window. Table 2 reports the selection criteria for both cases.

At this point it is important to highlight and explain the differences in the sample sizes between the sentiment event study on social media data and the classic event study. As can be seen from Table 2, the number of confounding events in the two samples is different, despite identical event windows. This effect is due to the different data type and data availability at the basis of each approach. Stock prices are structured data available on working days only, while social media data are unstructured data available on a daily basis, including official holidays and weekends. This leads to a shift effect within the event window, which at the same time affects the number of confounding events to be eliminated and the sample size too. In sum, the classical event study method was applied on a sample of 28 data breach events, while social media based - event study was applied on a sample of 31 events.

Criteria	**Event study**	**Sentiment event study**
	# events left	**# events left**
Initial sample	2266	2266
Listed firms	285	285
Loss size	56	56
Social media data	-	46
Stock prices data	50	-
Confounding events	28	31

Table 2. Sample selection criteria

4 METHODOLOGY

Event studies allow researchers to investigate the impact of corporate announcements on stock prices. The metric that quantifies the event impact on stock prices is the abnormal return, calculated as the difference between actual returns and normal returns (Binder 1998). Event studies have been applied not only to investigate the impact of business events on stock prices but also on trading volume. In this paper we conducted two event studies: first, a classic event study on stock returns data to analyse the financial impact of data breaches; second, an event study on social media sentiment data to measure data breaches impact on corporate reputation. In the classic event study we used daily stock returns, while in the adapted event study approach the variable of interest is daily sentiment, which resumes the overall users' opinions and evaluations on a particular company.

The event study requires the specification of the following criteria: (i) length of estimation window, (ii) length of event window and (iii) model choice for normal returns (Campbell et al. 1997). We chose a 43 day-long estimation window, starting 44 days prior to the event until two days before the event date. Studies on the cost of data breaches typically use longer estimation windows comprising at least 100 trading days (Yayla & Hu 2011). The relatively short estimation window is due to reasons related to the collection and preparation of social media data for the sentiment event study. The event study has been conducted both on daily stock prices and daily sentiment data. While financial data are structured and easily retrievable, the process of collection and analysis of social media data presents a higher degree of

difficulty. The event window comprises 12 days, starting one day before the event date until day 10 afterwards, while t_0 indicates the event date.

We used sentiment analysis to determine daily sentiment polarity values over the estimation and event window. Sentiment analysis or *opinion mining* implies procedures and approaches to analyse and quantify opinions, judgements, evaluations and emotions of people (Pang & Lee 2008). In this paper we applied a dictionary-based approach to determine the sentiment for each social media posting by using the General Inquirer software (Stone et al. 1966). To measure the polarity of each document, we used two word lists from General Inquirer, positive and negative. The polarity is calculated with the following formula as in the study of Sinanaj et al. (2015),

$$\text{sentiment polarity} = \frac{n_{pos} - n_{neg}}{n_{pos} + n_{neg}}$$

where n_{pos} indicates the number of positive words and n_{neg} the number of negative words. In contrast to the study of Sinanaj et al. (2015) that uses absolute sentiment values, we calculated the daily change of sentiment values. To ensure consistency between the two event studies, we calculated daily polarity changes (%) for each event, between two consecutive days, in a similar way as the calculation of stock price returns:

$$\text{sentiment polarity (\%)} = \frac{\text{polarity}_t - \text{polarity}_{t-1}}{\text{polarity}_{t-1}} * 100\%$$

In both event studies, expected returns and expected sentiment are calculated with the constant-mean return model, which assumes a constant average return (average sentiment) over the estimation window. Abnormal returns measure the effect of data breaches on stock prices and are calculated as the difference between actual returns and expected returns (Campbell et al. 1997):

$$ar_{it} = r_{it} - E(r_{it})$$

Abnormal sentiment expresses the difference between actual sentiment and expected sentiment and is calculated in the following way (Sinanaj et al. 2015):

$$as_{it} = s_{it} - E(s_{it})$$

Since we are using the constant-mean return model to calculate expected returns, the expected returns for a company i are constant (Campbell et al. 1997):

$$ar_{it} = r_{it} - \mu$$

Similarly, the average sentiment is calculated as follows (Sinanaj et al. 2015):

$$as_{it} = s_{it} - \mu$$

To aggregate abnormal returns for a company i over t days of the event window, the following formula is used (Campbell et al. 1997):

$$car_{it} = \sum_{t=1}^{N} ar_{it}$$

Similarly, cumulative abnormal sentiment is obtained by aggregating sentiment values over the event window (Sinanaj et al. 2015):

$$cas_{it} = \sum_{t=1}^{N} as_{it}$$

The statistical significance of cumulative abnormal sentiment values (CAS) was tested with both parametric and non-parametric tests. Parametric procedures can be applied on large sample sizes (>30) without a prior testing of the normality assumption, since the sampling distribution tends to be normal. Both tests generated similar results in terms of statistical significance. With respect to CAR values, the normality assumption does not hold due to the small sample size (<30) and the normality of the data

should be tested before applying the tests. Both normality tests applied on CAR, Shapiro-Wilk and Kolmogorov-Smirnov show that the data does not follow a normal distribution. Wilcoxon signed-rank test was used to test the statistical significance of CAR values.

5 RESULTS AND DISCUSSION

In this section we present the empirical results and discuss the theoretical and practical implications.

Impact of Data Breaches on Shareholder Value

The results of the event study on stock prices are presented in Table 3. Due to the small sample size (<30), we tested the statistical significance of CAR with a non-parametric test, the Wilcoxon signed-rank test. Abnormal returns assume negative values only on day -1 and day 0, yet not statistically significant. Overall data breaches do not have a significant impact on shareholder value.

Day	Median CAR (%)	W-statistic (p-value)
-1	-0.06	218 (0.636)
0	-0.30	196 (0.442)
+1	0.22	233 (0.753)
+2	0.82	247 (0.842)
+3	0.82	258 (0.895)
+4	0.30	249 (0.853)
+5	0.88	258 (0.895)
+6	1.31	276 (0.953)
+7	2.25	281 (0.963)
+8	1.46	278 (0.957)
+9	2.21	264 (0.918)
+10	1.70	258 (0.895)

Table 3. Cumulative abnormal returns over the event window (-1;+10)

Impact of Data Breaches on Corporate Reputation

To quantify the impact of the security breach events on social media and corporate reputation, we calculated cumulative abnormal sentiment values over the event window (-1;+10), which are summarized in Table 4. Negative values of CAS denote the reputational damage of the data breach events on the affected organizations. As shown in Table 4, CAS assume negative and statistically significant values over the event window (-1;+3), clearly showing the negative effect of such events on social media and corporate reputation. According to our definition, corporate reputation is represented by the way a specific company is perceived by the on-line community, engaged in the creation and exchange of content with regard to a specific company. The day prior to the event has been included in the event window in order to capture a possible anticipated effect of the data breaches on social media, typically due to a leak of information prior to the official announcement. Mean and median CAS on the days preceding the event announcement are negative and statistically significant at the 5% significance level. According to these results, there is an information leakage effect of data breaches on social media. On the event date, both mean CAS and median CAS are statistically significant at the 5% significance level, clearly showing that data breaches are negatively perceived by users and heavily discussed on social media, leading to a negative impact on corporate reputation. This effect persists until day +3 of the event window. Both parametric and non-parametric tests report consistent results in terms of statistical significance with exception of day +3. Based on the results displayed in Table 4, we can reject $H2_0: \mu_{CAS} \geq 0$ in favour of $H2_1: \mu_{CAS} < 0$, which asserts that data breaches tarnish corporate reputation.

	Parametric test		Nonparametric test	
Day/Window	**Mean CAS (%)**	**t-statistic (p-value)**	**Median CAS (%)**	**W-statistic (p-value)**
-1	-12.86	-1.713 (0.048**)	-10.34	149 (0.026**)
0	-57.14	-2.203 (0.018**)	-16.92	133 (0.012**)
+1	-93.77	-2.271 (0.015**)	-34.05	118 (0.005***)
+2	-75.37	-1.434 (0.081*)	-4.56	174 (0.076*)
+3	-106.92	-1.012 (0.160)	-11.99	162 (0.047**)
+4	-82.93	-0.743 (0.232)	-1.49	229 (0.360)
+5	-113.63	-0.980 (0.167)	-7.41	198 (0.168)
+6	-111.23	-0.874 (0.194)	3.65	232 (0.382)
+7	-106.03	-0.853 (0.200)	8.12	229 (0.360)
+8	-107.11	-0.835 (0.205)	-6.11	219 (0.291)
+9	-77.83	-0.641 (0.263)	-12.18	205 (0.205)
+10	-84.50	-0.680 (0.251)	-3.87	222 (0.311)
(0;+1)	-80.91	-2.226 (0.017**)	-27.90	121 (0.006***)
(0;+3)	-94.06	-0.900 (0.188)	-11.83	163 (0.049**)
(0;+5)	-100.78	-0.881 (0.193)	-16.09	199 (0.173)
(0;+10)	-71.64	-0.585 (0.282)	-17.26	213 (0.252)
*p<10%, **p<5%, ***p<1% (one-tailed test)				

Table 4. Cumulative abnormal sentiment values over the event window (-1;+10)

While the impact on social media and corporate reputation is immediate, and statistically significant over the event window (-1;+3), quite the opposite holds for the impact on capital markets. Despite the fact that in this sample we included relevant data breaches with a number of records greater than 10.000, the breach size criteria does not correlate with the reaction on the capital market. In contrast to social media users, who are very sensitive to the disclosure of data breach incidents, investors on the other hand seem to ignore them. The lack of a significant impact of data breach announcements on the stock market has been also reported in the news media. Two massive data breach incidents which affected Ebay Inc. in 2014 and Target Corporation in 2013 and having affected 145 million and 40 million customers respectively, despite the huge breach size and the intense media exposure, did not affect the stock prices during the trading day (Bloomberg 2014).

The lack of a significant impact of data breach incidents on the stock market signals that data breach events are not perceived by the investors' community as crisis events. Particularly relevant data breaches having affected large companies, have been very often publicized in national and international news media and investors might have developed a certain grade of "*immunity"* towards data breach events over time. A plausible explanation for the investors' reaction towards data breach announcements might be the fact that these events nowadays do not represent a new phenomenon for companies to face. The more firms assemble and store large amounts of customer data to increase the number of customers and profits, the more increases the risk of data breach incidents and privacy violations (IISP 2016). Companies are therefore aware of security risks and expect to experience data and security breach incidents in the future (Pwc 2015). The stock market does not penalize data breach events because investors consider them part of daily business activities (Manworren et al. 2016).

In contrast to investors' behaviour, data breach announcements are perceived by social media users as crisis events and generate negative sentiment, which in turn damages corporate reputation. While the stock market reaction is the result of the behaviour of a single category of stakeholders, social media sentiment reflects the average mood of different stakeholders, such as investors, consumers, potential

customers and actual customers. Cyber-attacks and data breaches could be interpreted by the public as a sign of the inability of the companies to guarantee the safety and confidentiality of customer data. Data breach announcements damage corporate reputation because of the *negativity bias* effect (Ito et al. 1998, p. 887), implying the predominance of negative information over favourable information in terms of perceived relevance. Unconsciously, people discriminate between positive and negative information and sense non favourable information as more relevant than favourable information. Negative information has therefore a great influential power on shaping the perceptions, opinions and ideas of people (Ito et al. 1998). Data breach announcements create negative sentiment in the public which is also reflected on reputation.

From a research perspective, prior studies that have analysed the financial impact of data breach events report statistically significant negative cumulative abnormal returns around the event date, contrary to our results. With regard to the type of breach, investors and the stock market penalized in the past data breaches at a great extent and ignored other types of security breaches, such as DOS attacks (Hovav & D'Arcy 2003) or availability breaches (Campbell et al. 2003). In addition, prior research provides evidence of a positive correlation between breach size and abnormal returns (Gatzlaff & McCullough 2010). Other intangible costs caused by data breach incidents, such as damage of corporate reputation, have received little attention by researchers, despite of all the evident risks social media creates around reputation in crisis situations. Our study offers interesting insights on the intangible cost of data breaches and contributes to the information security literature. In summary, our findings should be understood by scholars as an opportunity to explore other facets related to the economic and financial impact of data breaches which have received little attention, despite their high relevance both in research and practise.

From a practical point of view, our results regarding corporate reputation point to the necessity of crisis management strategies in organisations. Data breach events have an adverse effect on corporate reputation and companies can leverage social media communication platforms to monitor the longevity and degree of reputation damage in the aftermath of crisis events. Companies do not have control on the information released in the news media and social media and cannot predict how the public and the stakeholders will react to such information. Furthermore, users' reaction in social media depends on if and to which extent consumers blame the company for the crisis event. It is essential to communicate and deliver a message to the customers affected by breach incidents and social media can be a very useful tool to achieve this goal.

6 CONCLUSIONS

In this paper we investigated the effect of data breach incidents on corporate reputation and on shareholder value based on the event study approach. The event study was applied on two types of data: on stock prices to measure abnormal returns and on social media data to quantify reputational changes. We found that data breach incidents do not have a significant effect on investors' community in contrast to prior research, which consistently reports negative and significant cumulative abnormal returns. Additionally, we found that data breaches are discussed with negative tones on social media and cause therefore reputation damage. Our results indicate that firms affected by data breach incidents should focus on the asset of reputation and design response plans with the goal of limiting reputational losses.

Our findings offer several directions for future research opportunities. Future research could explore the relationship between the reputation status prior to the crisis event and the impact on reputation post event based on the "*reservoir hypothesis*". According to this hypothesis, reputation, described as a "*reservoir of goodwill*" is a valuable resource during periods of crisis because it has a protective function (Jones et al. 2000). Prior research provides evidence of the protective power of reputation in presence of crisis situations. Jones et al. (2000) show that the market crash in 1987 had a milder negative impact on the market value of firms with good reputation. Companies with a strong reputation before crisis events have a higher degree of immunity, thus suffer less reputational losses than companies with a less good reputation (Coombs 2007).

In future research we aim to extend this study and additionally investigate the reputational impact of data breaches based on news media content. While traditional media and social media are both important information sources for a firm's stakeholders, there are substantial differences between the professional content of news media and user generated content in social media. Our objective is to measure the reputational effect of data breaches with two different media sources and uncover the differences between the two approaches.

References

Acquisti, A., Friedman, A. and Telang, R. (2006). Is there a cost to privacy breaches? An event study. In Proceedings of the 21st International Conference on Information Systems (ICIS), 1563-1580, Milwaukee, Wisconsin.

Benthaus, J., Pahlke, I., Beck, R. and Seebach, C. (2013). Improving sensing and seizing capabilities of a firm by measuring corporate reputation based on social media data. In Proceedings of the 21st European Conference on Information Systems (ECIS), 1-12, Utrecht, Holland.

Binder, J. (1998). The event study methodology since 1969. Review of Quantitative Finance and Accounting, 11 (2), 111-137.

Bloomberg (2014). http://www.bloomberg.com/news/articles/2014-05-23/investors-couldnt-care-less-about-data-breaches. Last accessed: April 1st, 2016.

Bondt, W. F. and Thaler, R. (1985). Does the stock market overreact?. The Journal of Finance, 40 (3), 793-805.

Camp, L. J. and Lewis, S. (2006). Economics of Information Security. Springer Science & Business Media.

Campbell, K., Gordon, L. A., Loeb, M. P. and 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.

Campbell, J. Y., Lo, A. W. C. and MacKinlay, A. C. (1997). The Econometrics of Financial Markets. Princeton University Press, Princeton.

Cavusoglu, H. (2002). The economics of information technology (IT) security. AMCIS 2002 Proceedings, 344.

Cavusoglu, H., Mishra, B. and 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.

Colleoni, E., Arvidsson, A., Hansen, L. K. and Marchesini, M. (2011). Measuring corporate reputation using sentiment analysis. In Proceedings of the 15th International Conference on Corporate Reputation (available at http://openarchive.cbs.dk/handle/10398/8730).

Cooley, S. C. and Cooley, A. B. (2011). An examination of the situational crisis communication theory through the general motors bankruptcy. Journal of Media and Communication Studies, 3 (6), 203-211.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate Reputation Review, 10 (3), 163-176.

Coombs, W. T. (2014). Ongoing Crisis Communication: Planning, Managing, and Responding: Planning, Managing, and Responding. Sage Publications Inc., Thousand Oaks.

Coombs, W. T. and Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial tests of the situational crisis communication theory. Management Communication Quarterly, 16 (2), 165-186.

Dean, D. H. (2004). Consumer reaction to negative publicity: Effects of corporate reputation, response, and responsibility for a crisis event. Journal of Business Communication, 41 (2), 192-211.

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

Fearn-Banks, K. (2010). Crisis Communications: A Casebook Approach. Routledge.
Fombrun, C. and Riel, C. B. M. (1997). The reputational landscape. Corporate Reputation Review, 1 (1-2), 1-16.
Fombrun, C. J., Gardberg, N. A. and Sever, J. M. (2000). The Reputation QuotientSM: A multi-stakeholder measure of corporate reputation. Journal of Brand Management, 7 (4), 241-255.
Gatzlaff, K. M. and McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13 (1), 61-83.
Gordon, L. A., Loeb, M. P. and Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 19 (1), 33-56.
Gupta, U. and Ranganathan, N. (2007). Multievent crisis management using noncooperative multistep games. IEEE Transactions on Computers, 56 (5), 577-589.
Hinz, O., Nofer, M., Schiereck, D. and Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. Information and Management 52 (3), 337-347.
Hovav, A. and D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review, 6 (2), 97-121.
Hovav, A. and D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. Information Systems Security, 13 (3), 32-40.
Institute for Information Security and Privacy (IISP) (2016). Emerging cyber threats report. Giorgia Institute for Technology.
Ito, T. A., Larsen, J. T., Smith, N. K. and Cacioppo, J. T. (1998). Negative information weighs more heavily on the brain: The negativity bias in evaluative categorizations. Journal of Personality and Social Psychology, 75 (4), 887-900.
Jin, Y., Liu, B. F. and Austin, L. L. (2011). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses. Communication Research, 19 (3), 255-281.
Jones, G. H., Jones, B. H. and Little, P. (2000). Reputation as reservoir: Buffering against loss in times of economic crisis. Corporate Reputation Review, 3 (1), 21-29.
Kannan, K., Rees, J. and Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. International Journal of Electronic Commerce, 12 (1), 69-91.
Ko, M. and Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. Journal of Information Technology Management, 17 (2), 13-22.
Lo, A. W. (2004). The adaptive markets hypothesis: Market efficiency from an evolutionary perspective. Journal of Portfolio Management, 30, 15-29.
Lo, A. W. (2005). Reconciling efficient markets with behavioral finance: The adaptive markets hypothesis. Journal of Investment Consulting, 7 (2), 21-44.
Manworren, N., Letwat, J. and Daily, O. (2016). Why you should care about the Target data breach. Business Horizons, 59 (3), 257-266.
Morse, E. A., Raval, V. and Wingender, J. R. (2011). Market price effects of data security breaches. Information Security Journal: A Global Perspective, 20 (6), 263-273.
Nofer, M., Hinz, O., Muntermann, J. and Roßnagel, H. (2014). The Economic impact of privacy violations and security breaches: A laboratory experiment. Business & Information Systems Engineering, 89-108. (doi: 10.1007/s12599-014-0351-3).
Pang, B. and Lee, L. (2008). Opinion mining and sentiment analysis. Foundations and Trends in Information Retrieval, 2 (1-2), 1-135.
Pirounias, S., Mermigas, D. and Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. Journal of Information Security and Applications, 19 (4-5), 257-271.
Ponzi, L. J., Fombrun, C. J. and Gardberg, N. A. (2011). RepTrak™ pulse: Conceptualizing and validating a short-form measure of corporate reputation. Corporate Reputation Review, 14 (1), 15-35.

Pwc (2015). Information security breaches survey. Survey conducted by Pwc in association with Info Security Europe.
Rindova, V. P., Williamson, I. O., Petkova, A. P. and Sever, J. M. (2005). Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. Academy of Management Journal, 48 (6), 1033-1049.
Romanosky, S., Telang, R. and Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30 (2), 256-286.
Sarstedt, M., Wilczynski, P. and Melewar, T. C. (2013). Measuring reputation in global markets-A comparison of reputation measures' convergent and criterion validities. Journal of World Business, 48 (3), 329-339.
Shleifer, A. (2000). Inefficient Markets: An Introduction to Behavioral Finance. Oxford University Press Inc., New York.
Sinanaj, G., Muntermann, J. and Cziesla, T. (2015). How data breaches ruin firm reputation on social media!-Insights from a sentiment-based event study. In Proceedings of Wirtschaftsinformatik, 902-916. (available at http://www.wi2015.uni-osnabrueck.de/Files/WI2015-D-14-00293.pdf).
Stone, P.J., Dunphy, D.C., Smith, M.S. and Ogilive, D.M. (1966). The General Inquirer. The M.I.T. Press, Massachusetts.
Wartick, S. L. (2002). Measuring corporate reputation definition and data. Business and Society, 41 (4), 371-392.
Xu, W., Grant, G., Nguyen, H. and Dai, X. (2008). Security breach: The case of TJX companies, Inc. Communications of the Association for Information Systems, 23 (31), 575-590.
Yayla, A. A. and 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.