6-2013

Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis

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

Jan Muntermann
University of Göttingen, Germany, muntermann@wiwi.uni-goettingen.de

26th Bled eConference

eInnovations:
Challenges and Impacts for Individuals, Organizations and Society

June 9, 2013 – June 13, 2013; Bled, Slovenia

Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis

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

Jan Muntermann
University of Göttingen, Germany
muntermann@wiwi.uni-goettingen.de

Abstract

Corporate reputation represents a core asset of companies and research has shown that better reputation can have positive effects such as increased revenues and sales. On the other hand, companies may suffer reputational damage that can result from internal or external and potentially unforeseen events such as operational losses. In this paper, we present an empirical analysis of how unforeseen IT security incidents have an impact on corporate reputation. With a focus on data breaches, i.e. situations in which internal information has been lost or stolen, we have conducted an event study providing evidence that newly published data breach has a negative effect on firm value. While this finding confirms existing research in this field, we also applied a method that aims at isolating the related reputation effects in the context of data breaches. Thereby, our results provide new insights into how IT security incidents do negatively impact corporate reputation.

Keywords: IT security, data breach, corporate reputation, event study

1 Introduction

Unforeseen IT security incidents can have a wide range of different consequences such as system outages, privacy violations or direct financial losses. Such events are certainly relevant regarding the reputation of a firm that is affected by the IT security incidents. In a recent study on "Reputational risk and IT" conducted by IBM (2012), senior executives highlight their perception that IT security has a strong link to reputational risk. With regard to IT security incidents posing the greatest threats to corporate reputation, data breaches and losses are among the top 3 events that do negatively affect corporate reputation (IBM, 2012). However, little insight is provided on *how* these events affect corporate reputation. Against this background, our study explores how data breaches and losses negatively affect corporate reputation. We follow the definition of Brown et al (2006, p.104) who define corporate reputation as "… a perception of the organization actually held by external stakeholders".

Despite the crucial importance of corporate reputation and the considerable attention that reputational risk has received in the recent years, this category of risk remains underexplored, which calls for further research contributions (Soprano et al., 2009). Since there are no direct approaches or risk measures available, indirect approaches for the quantification of reputational risk have been suggested. More specifically, an indirect approach that aims at measuring the reputational impact of operational losses has been proposed (de Fontnouvelle and Perry, 2005; Gillet, Hübner, and Plunus, 2010).

To our knowledge there are no articles that investigate the relation between the impact of IT security incidents and reputational risk. Therefore, we have adapted the methodology proposed in the context of operational losses (de Fontnouvlle and Perry, 2005; Gillet, Hübner, and Plunus, 2010; Fiordelisi, Soana, and Schwizer, 2012). Thus, we first apply an event study methodology for analyzing the overall stock price reaction and then correct for the reputational damage triggered by the occurrence of unexpected data breach incidents.

In this work we consider a sample of 72 data breach events occurred between 2004 and 2011 worldwide. Unlike the previous studies dealing with reputational risk, we do not focus our analysis exclusively on the financial sector. Accordingly, our sample is composed of financial sector companies but also of firms belonging to other industry sectors. The results confirm that the firms experience significant reputational damage attributable to the announcement of the data breach incidents.

The remainder of this paper is organized in the following order: Section 2 is dedicated to the theoretical background related to this work and the formulation of the research hypotheses. Section 3 provides a detailed description of our dataset and section 4 the methodological framework applied. The empirical results are reported in section 5. Finally, we summarize and discuss our findings and suggest avenues of future research.

2 Theoretical Background and Hypothesis

2.1 IT Security and Data Breaches

In business environments, inappropriate security practices can result in data breaches that can lead to significant consequences to both the firm as well as to the entity, whose data is affected. Data breaches and losses can be defined as situations in which "personally identifiable information such as names, Social Security numbers, and credit card numbers are accidentally lost or maliciously stolen" (Romanosky, Telang, and Acquisti, 2011, p. 256). The consequences of such incidents have been explored in the literature from the affected firm's perspective on the basis of event study analyses.

Here, the breach impact on the firm value is measured by calculating abnormal stock price reactions that can be observed subsequent to the date when the breach becomes public. Several related event studies explore these price effects and show mixed result regarding the magnitude of the observed price impact. While Andoh-Baidoo, Amoako-Gyampah, and Osei-Bryson (2010) report a substantial decrease of more than 3% on average within a three day

period, other studies report significant but small effect sizes only (Acquisti, Friedman, and Telang 2006; Muntermann and Roßnagel, 2009).

As the potential price impact of a data breach on a firm's value will provide the basis for our exploration of a related reputational damage, we formulate our first hypothesis *H1* on the potential market value effect of published data breaches.

H1: A firm's market value will be negatively affected whenever a data breach is being published.

2.2 Corporate Reputation and Reputational Risk

In this work we aim at analyzing and quantifying the impact of security incidents, i.e. data breaches, on the reputational status of a firm. There are few research papers that have tackled this problem domain of quantifying reputational risk. So far, the only approach followed in literature is through analyzing indirectly the impact of operational[1] losses on the reputation of financial institutions by applying an adjusted event study methodology.

de Fontnouvelle and Perry (2005) are among the first who presented a quantitative approach to quantify the impact of negative events on a firm´s reputation and to assess reputational risk. With a focus on the effect of operational losses, the authors present an event study covering operational loss events occurred worldwide between 1974 and 2004 that have affected financial institutions. Here, operational loss events were taken from the two proprietary databases Algo OpData and OpVantage FIRST. The reputational losses have been measured by examining the impact of the operational losses on the market value of the affected financial institutions. Reputational damage or reputational loss is interpreted as the difference between the firm's market value decline after the loss announcement and the suffered loss. More precisely, reputational loss or damage occurs only if the market value decrease following the loss announcement exceeds the actual loss amount itself. In addition, de Fontnouvelle and Perry (2005) investigate the influence of different categories of operational losses on the firms' market values. In particular, they observed no reputational damage if losses are triggered by external factors. On the contrary, if the losses derive from internal fraud events, the magnitude on the stock market value exceeds the loss percentage, thus attributing the difference to the reputational damage.

Gillet, Hübner, and Plunus (2010) build upon the work of de Fontnouvelle and Perry (2005) but propose a more precise measure of reputational risk that permits to isolate the pure reputational effect. The sample used for the analysis is composed of the 152 largest operational losses occurred between April 1994 and July 2006. More precisely, 104 losses have affected US companies, whereas the remaining 49 losses are related to European financial institutions, thus focusing the attention on the US market. The empirical results show significant negative stock prices reactions and abnormal trading volumes. Similarly as in de Fontnouvelle and Perry (2005), it emerges that in case of internal fraud the market value

[1] Operational loss is defined as "the loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee,2003a, p. 2).

decrease is larger than the operational loss amount announced, which is interpreted as a sign of reputational damage. Another finding from the study of Gillet, Hübner, and Plunus (2010) shows that when the loss amount is not known, the market exhibits an overreaction compared to the case when the quantification of the occurred losses has been announced.

Evidence about the reputational losses following operational losses in banking industry has been provided by the study of Fiordelisi, Soana and Schwizer (2012). The authors have analyzed the reputational impact of 430 cases of operational losses greater than 1 million US$ regarding a large sample of banks in Europe and the USA between 1994 and 2008. The overall results provide evidence that whenever a firm suffers operational losses, there is also an additional impact on the reputational status. Considering the event type, it emerges that the event type "external frauds" cause the larger reputational damage compared to other operational loss categories. This result is similar to previous studies (de Fontnouvelle and Perry, 2005) and evidences that incidents such as operational losses are of substantial relevance for the negative stock price reaction and contribute of reputational damage of the specific company, at which the incident took place. Further, the authors show that the reputational losses originating from operational losses are higher for European banks rather than for US banks.

In contrast to former academic works (de Fontnouvelle and Perry, 2005; Gillet, Hübner, and Plunus, 2010), which have analyzed the impact of operational losses events occurred at international financial companies, Sturm (2013) considers exclusively European banks. The sample used for the analysis is composed of 136 operational losses with settlements reported between January 2000 and December 2009 which derive from a proprietary database of publicly reported operational losses (ÖffSchOR) provided by the Association of German Public Sector Banks (Bundesverband öffentlicher Banken, VÖB). The obtained results evidence a significant negative stock price reaction to the first press announcement of operational losses. Furthermore, the reaction of the stock market is stronger at the settlement date when the loss amounts are announced in comparison to the first press announcement date. In contrast to previous studies (de Fontnouvelle and Perry, 2005; Gillet, Hübner, and Plunus, 2010), the event characteristics do not affect the reputational damage measured.

The existing literature provides evidence that when a firm has suffered operational losses, the impact on the stock market value exceeds the loss amount itself, therefore provoking damage to reputation. In this paper, we follow this line of research but instead of focusing on operational losses, we aim to explore the potential reputational damage that may result from data breaches that became public. We therefore state our second research hypothesis as follows:

H2: Whenever a data breach is being published for a firm, it faces a reputational damage.

3 Dataset Description

Our dataset of data breach events has been acquired from DataLossDB[2] operated by the Open Security Foundation, a non-profit organization that aims at tracking websites and blogs and reporting data breaches related to personal information. All detected data breach news is subsequently recorded in the database. For every data breach reported, a summary of the incident characteristics is provided: date of the incident, source, number of records lost, name of the organization, location(s) affected and links to electronic media that reported on the incident.

In order to build our data set, we take into the consideration incident events occurred worldwide in between 2004 and 2011. To obtain the final sample, which is going to be further analyzed, several filter rules set have been applied. Firstly, all incidents which are not pertinent to companies and more precisely to companies whose stocks are listed and traded at an exchange are eliminated. This step is necessary for two reasons. First, the goal of this work is to study corporate reputational risk, and secondly for measuring the market impact of the incident event, stock prices need to be analyzed. The majority of the companies obtained after applying the first filter rule are located in the USA, whereas the rest of the sample is divided between Europe, Japan, China, Russia and Australia.

Further, also those incidents for which no "number of records lost" data was available needed to be removed from the sample since this information is required to estimate the actual loss. The final sample consists of 72 data breach events that took place at international listed firms.

Further, we need to discard events that were observed along with other (so-called confounding) events. Since the aim is to analyze and capture the impact of data breaches on the firm´s market value, by considering the confounding events it would not be clear to determine what caused the subsequent market variation (Konchitchki and O'Leary, 2011). Accordingly, we checked if other relevant events (such as quarterly figures) were published in the news. Accordingly, these events have been removed from the sample since their inclusion would distort the results.

Location	USA	GB	Russia	Japan	China	Germany
Number of observations	56	6	1	4	3	2

Table 1. Data Breach Sample

The historical stock prices with daily frequency have been retrieved from Yahoo Finance. In addition, the stock prices are adjusted for stock splits and dividends. To estimate the market model for the calculation of the abnormal returns, the following indices serve as benchmark: S&P500 for US companies, FTSE100 for UK, DAX for Germany, Nikkei225 for Japan, SSE Composite Index for China and S&P/ASX for Australia. The time series for each index have been downloaded from Yahoo Finance.

[2] http://datalossdb.org/.

4 Methodology

For the measurement of reputational risk we combine two methods, an event study methodology (Campbell, Lo, and MacKinlay, 1997) and an approach to isolate the reputation effect from the abnormal market reaction (Gillet, Hübner, and Plunus, 2010; Fiordelisi, Soana, and Schwizer, 2012).

4.1 Event Study Analysis

The event study methodology is a quantitative method that has been applied in a wide range of different fields including finance and applied economics in order to observe the response of share prices to a specific unanticipated event, such as mergers and acquisitions or earnings announcements (Campbell, Lo, and MacKinlay, 1997). The theoretical foundation of the event study methodology is provided by the Efficient Market Hypothesis, which claims that the security prices fully incorporate available information. Thus, a variation in stock prices will originate only if there is new relevant information made available to the market (Fama, 1991). Therefore, the impact of a firm-related event on the stock price can be observed since there is rationality in the market (Mackinley, 1997).

In this paper, we analyze how stock prices react to data breaches as a category of IT security incidents. By conducting an event study, the abnormal reaction of the stock returns value expressed in terms of abnormal returns can be measured as the difference between the actual and the predicted returns. Throughout the analysis, we use the market model for calculating the predicted returns or the normal performance of the stock returns in absence of the event (Campbell, Lo, and MacKinlay, 1997). Abnormal returns and cumulated abnormal returns are calculated accordingly:

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i R_{m,t}) \qquad CAR_{i,t1,t2} = \sum_{t=t1}^{t2} AR_{i,t}$$

where :

$AR_{i,t}$ = Abnormal stock return of firm i on day t

$CAR_{i,t1,t2}$ = Cumulative abnormal stock return of firm i cumulated from day $t1$ to $t2$

$R_{i,t}$ = Stock return of firm i on day t

$R_{m,t}$ = Rate of return the market index on day t

α_t, β_t = OLS estimates of the linear model that describes the sensitivity of $R_{i,t}$ to the market index $R_{m,t}$ (calculated for an estimation windows of 100 days in length that ends 50 days prior to the event date).

In order to measure the abnormal stock price reaction related to the data breach event, first the expected returns over the event window are calculated. For this purpose we estimate the market model parameters α_i and β_i by using OLS regression during the estimation window prior to the data breach event date. We choose as an estimation window the time interval between the 100th and 50th day prior to the the data breach (i.e. the event date). The

estimated parameters are then used for calculating the expected returns in the event window. As an event window we chose the time span between the 5th day before and after the event date [t_{-5}; t_{+5}], denoting the event date as t_0. In the contrary, the choice of a long event window would harshly reduce the power of the test statistics (Brown and Warner, 1985). In addition, by deciding for a short event window the probability that confounding events might interfere with the market reaction is considerably reduced (Konchitchki and O'Leary, 2011).

4.2 Isolation of Reputation Effects

Yet, there are no direct risk measures designated for the measurement of this risk category, thus only indirect methods are so far proposed in the respective literature (de Fontnouvelle and Perry, 2005). For measuring the reputational damage related to data breaches, we adopt the method proposed by Gillet, Hübner, and Plunus (2010) for measuring the impact on corporate reputation of a loss event. The approach proposed by the authors aims at disentangling the reputational risk by quantifying the reputational damage due to a loss event as the sum of two elements: the shock reaction of the firm´s stock price and the ratio between the effective loss amount disclosed and the market capitalization of the firm affected. In line with this research on how to assess the reputational damage that result from operational losses (Gillet, Hübner, and Plunus, 2010), we adjust the calculated abnormal return by the ratio of actual cost estimate of the data breach and the firm's market capitalization as follows:

$$AR_{i,t}(REP) = AR_{i,t} + \left\lfloor \frac{\cos ts_i}{MarketCap_i} \right\rfloor$$

where:

$AR_{i,t}$ (REP) = $AR_{i,t}$ corrected for the market exposure and the mechanical impact of data breach costs

$AR_{i,t}$ = Abnormal stock return of firm i on day t

$cost_i$ = Direct[3] and indirect cost[4] of data breaches suffered by firm i on the basis of estimates of Ponemon Institute LLC (2011)

$MarketCap_i$ = Market capitalization of firm i on day t.

Here, $AR_{i,t}$ measures the entire stock market reaction subsequent to the data breach announcement, whereas $AR_{i,t}(REP)$ expresses the market reaction corrected for the mechanical effect of the loss originated from the data breaches. This allows us to isolate and therefore measure the reputational damage suffered by the firm (Sturm, 2013). Accordingly, the expression $CAR_{i,t}(REP)$ denotes the adjusted cumulative abnormal returns for the data breach loss effect.The total cost (the sum of direct and indirect cost) of every data breach is estimated according to actual estimates provided by Ponemon Institute LLC (2011).

[3] Direct costs refer to the direct expense outlay to accomplish a given activity such as hiring a law firm or offering identity protection services to victims (Ponemon Institute LLC, 2011, p.18).

[4] Indirect costs are related to the amount of time, effort and other organizational resources spent such as using existing employees to help in the data breach notification efforts or in the investigation of the incident (Ponemon Institute LLC, 2011, p.18).

5 Empirical Results

The following sections present the empirical results obtained from the standard event study and the isolation of the reputational impact of the data breach events.

5.1 Impact on Firms' Value

Table 2 reports the results obtained for the abnormal returns $AR_{i,}$ on different days prior and subsequent to the event date. Mean abnormal returns can be observed from the 1st day before the event date, until 4 days after the data breach has been announced. In addition, we observe that at the event date the the highest percentage of negative abnormal returns, i.e. 55%, can be observed. Furthermore, the *t*-test values provide statistical evidence for abnormal stock abnormal returns (H_0: $AR > 0$ rejected at the 90% confidence level). These results and the persistence of negative abnormal returns confirm our first hypothesis according to which the firm´s market value is negatively affected after a data breach event has been disclosed.

	Day										
	t_{-5}	t_{-4}	t_{-3}	t_{-2}	t_{-1}	t_0	t_{+1}	t_{+2}	t_{+3}	t_{+4}	t_{+5}
Mean *AR* (%)	0.40	0.00	-0.19	0.05	-0.23	-0.40	-0.28	-0.25	-0.15	-0.37	0.29
t-value	1.10	0.00	-0.55	0.14	-1.12	-1.40*	-0.89	-0.41	-0.54	-1.58*	0.88
% neg. ARs	41.3	45.0	53.8	43.8	43.8	55.0	53.8	42.5	48,8	51.3	47.5

* indicates statistical significance at the 10% level (unilateral test)

Table 2. AR results for t = -5 to +5 days

Our first hypothesis is confirmed also from the cumulated abnormal returns CAR_i results summarized in Table 3. CAR_i have been calculated for different event windows starting from the 5th day prior to the data breach disclosure up to 5 days afterwards. The cumulated returns are positive on the first event window (t_{-5}, t_0) since there is no information leakage about the data breaches. Subsequently, the cumulative abnormal returns assume negative value over the following event windows evidencing the incorporation of the event announcement in the market stock prices. Similarly as for the abnormal returns, the percentage of negative CAR_i exceeds 50% of the overall sample over the event windows ($t_{0,}$ t_2), ($t_{0,}$ t_3), ($t_{0,}$ t_4) and ($t_{0,}$ t_4).

The *t*-test values, -1.48 in ($t_{0,}$ t_1), -1.46 in ($t_{0,}$ t_3) and -1.35 in ($t_{0,}$ t_5), provide statistical evidence for abnormal stock abnormal returns (H_0: CAR>0 rejected at the 90% confidence level). The *CAR* show statistical significance at the 5% level over the window ($t_{0,}$ t_4) with a *t*-value of -1.71.

	Period (t_1; t_2)					
	(t_{-5}, t_{-1})	(t_0, t_1)	(t_0, t_2)	(t_0, t_3)	(t_0, t_4)	(t_0, t_5)
Mean *CAR* (%)	0.04	-0.72	-1.02	-1.18	-1.55	-1.25
t-value	0.04	-1.48*	-1.20	-1.46*	-1.71**	-1.35*
% neg. *CAR*'s	48.6	48.6	50.0	56.9	61.1	52.8

* indicates statistical significance at the 10% level (unilateral test)

** indicates statistical significance at the 5% level (unilateral test)

Table 3. CAR results for t = -5 to +5 days

Figure 1 provides a graphical overview of the results summarized previously. The horizontal axis indicates the day *t* on which the abnormal return was recorded, and the vertical axis indicates respectively the average value of the abnormal return (mean *AR*) and the average cumulative abnormal return (mean *CAR*). Mean *AR* assumes negative values over the window (t_{-4}, t_4) (except for a positive value, 0.05, in day t_{-2} and reaches the peak on the event date. The cumulated abnormal returns show negative values starting from day 1 prior to the event date consequently the disclosure of the data breaches concerning the sample of companies under investigation.

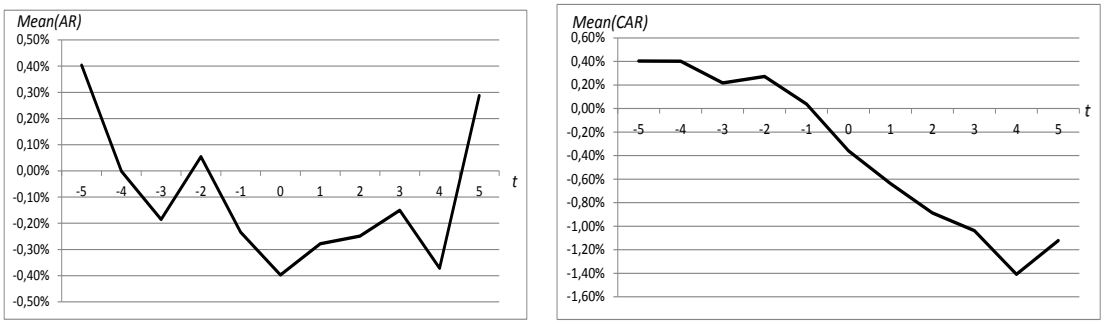

Figure 1. Mean (AR) and Mean (CAR) charts for t = -5 to +5 days

The persistence of negative *CAR* up to five days after the data breach announcement in the press indicate that the new information conveyed to the market has been incorporated in the stock prices, thus originating a shock reaction on the firm´s stock price.

5.2 Reputational Damage

The abnormal returns corrected for the mechanical impact of the data breach impact, *AR*(*REP*), display negative values over the entire event window. This persistence up to 5 days after the incident date evidences delayed market reaction to the news announced.

Furthermore, almost more than 40 percent of $AR_{i,}$ in relation to the overall number of abnormal returns is negative starting from the third day prior to the event date and five days after the event date, with the highest percentage of negative abnormal returns, i.e. 48.8%, reached at the event date.

	Period(t_1; t_2)				
	t_{-5}	t_{-4}	t_{-3}	t_{-2}	t_{-1}
Mean *AR*(*REP*) (%)	-0.51	-0.73	-0.91	-0.70	-0.65
% neg. AR's	33.8	37.5	45.0	38.8	37.5

Table 4. AR(REP) results for t = -5 to -1 days

	Period(t_1; t_2)					
	t_0	t_{+1}	t_{+2}	t_{+3}	t_{+4}	t_{+5}
Mean *AR*(*REP*) (%)	-0.83	-0.57	-0.85	-0.77	-0.64	-0.83
% neg. AR's	48.8	45.0	36.3	40.0	45.0	41.3

Table 5. AR(REP) results for t = 0 to +5 days

Table 6 reports the *CAR*(*REP*) results, which show the isolated reputational damage of firms that suffer a data breach incident. Over the entire event window, reputational losses occur given the negative values of the *AR*(*REP*). This shows evidence of significant and persistent reputational losses over the window (t_{-5};t_{+5}).

	Period(t_1; t_2)					
	(t_{-5}, t_{-1})	(t_0, t_1)	(t_0, t_2)	(t_0, t_3)	(t_0, t_4)	(t_0, t_5)
Mean *CAR*(*REP*) (%)	-3.12	-1.79	-2.13	-2.89	-3.58	-4.15
% neg. *CAR*'s	82.67	73.53	73.33	78.67	82.67	85.33

Table 6. CAR(REP) results for t = -5 to +5 days

Considering the aforementioned results, we can also confirm our second formulated hypothesis, which stated that the disclosure of data breach incidents has an impact on the corporate reputation. Due to the relative small size of the selected sample, the significance *t*-test has not been conducted.

6 Summary and Conclusions

In this paper we have examined and presented the results of an empirical analysis of the impact of data breach incidents on corporate reputation. In line with previous research on reputational risk, we have conducted an event study and consequently applied a method for estimating the reputational damage following the announcement of the breach incidents.

Our results demonstrate that there is an impact of IT security incidents, here data breaches, on the market value of the affected firms. Furthermore, reputational losses due to the incident event were recorded throughout the event windows observed.

To our knowledge this is the first empirical study that addresses the question of reputational damage from an IT security perspective. The previous studies dealing with reputational risk have analyzed the indirect impact of operational losses on corporate reputation exclusively for financial companies. In contrast, our research explores the impact of IT security incidents and incorporates other industries than the finance sector.

Our paper also contributes from the methodological perspective, as our study provides new insights on how to adapt an existing approach to measure reputational damage to an IT security context.

In future research, we plan to conduct content analyses of electronic media publications involved in the disclosure of data breach incidents in order to explore reputational damage from a media sentiment perspective.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) within the context of the Project FIRST, Large scale information extraction and integration infrastructure for supporting financial decision making, under grant agreement n. 257928.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study, in (Eds.) *Proceedings of the Twenty-Seventh International Conference on Information Systems*, 1563-1580. Milwaukee.

Andoh-Baidoo, F.K., Amoako-Gyampah, K., & Osei-Bryson, K.-M. (2010). How Internet Security Breaches Harm Market Value. *IEEE Security & Privacy*. 8(1), 36-42.

Basel Committee, 2003a. Sound Practices for the Management and Supervision of Operational Risk. Bank for International Settlements: Basel Committee Publications No. 96.

Brown, S.J, & Warner, J.B. (1985). Using daily stock returns: the case of event studies. *Journal of Financial Econonomics,* 14(1), 3-31.

Brown, T.J., Dacin, P.A., Pratt, M.G., & Whetten, D.A. (2006) Identity, Intended Image, Construed Image, and Reputation: An Interdisciplinary Framework and Suggested Terminology. *Journal of the Academy of Marketing Science.* 34 (2), 99-106.

Campbell, J.Y., Lo, A.W., & MacKinlay, A.C. (1997). The Econometrics of Financial Markets. Princeton, NJ: Princeton Univ. Press.

de Fontnouvelle, P., Perry, J. (2005). Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements. Working Paper, Federal Reserve Bank of Boston.

Fama E. (1991). Efficient capital markets II. *Journal of Finance*. 46(5), 1575–1617.

Fiordelisi, F., Soana, M-G., & Schwizer, Paola. (2012, forthcoming). Reputational losses and operational risk in banking. The European Journal of Finance. 1–20

G., Hübner, G. and Plunus, S. (2010). Operational Risk and Reputation in the Financial Industry. *Journal of Banking and Finance.* 34(1), 224 - 235.

IBM Global Technology Services (2012) Reputational risk and IT: How security and business continuity can shape the reputation and value of your company, Somers, NY.

Konchitchki, Y., & O'Leary, E., D. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems*. 12(2), 99-115.

Muntermann, J., & Roßnagel, H. (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market, in: *Lecture Notes in Computer Science*, A. Jøsang, T. Maseng and S. Knapskog (eds.), Springer Berlin / Heidelberg, 1-14.

Ponemon Institute LLC (2011). 2011 Cost of Data Breach Study, Traverse City, MA.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*. 30(2), 256-286.

Soprano, A., Crielaard, B., Piacenza, F., Ruspantini, D. (2009). Measuring operational and reputational risk. A practitioner approach. England: John Wiley & Sons Ltd.

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization*, 85, 191– 206.