Firm Actions Toward Data Breach Incidents and Firm Equity Value: An Empirical Study

Ziqian Song
Virginia Tech
ziqian@vt.edu

G. Alan Wang
Virginia Tech
alanwang@vt.edu

Weiguo Fan
Virginia Tech
wfan@vt.edu

Abstract

Managing information resources including protecting the privacy of customer data plays a critical role in most firms. Data breach incidents may be extremely costly for firms. In the face of a data breach event, some firms are reluctant to disclose information to the public. Firm may be concerned with the potential drop in the market value following the revelation of a data breach. This paper examines the impact of data breach incidents to the firm's market value/equity value, and explores the possibility that certain firm behaviors may reduce the cost of the incidents. We use regression analysis to identify the factors that affect cumulative abnormal stock return (CAR). Our results indicate that when data breach happens, firms not only should notify customers or the public timely, but also try to control the amount of information disclosed. These findings should provide corporate executives with guidance on managing public disclosure of data breach incidents.

1. Introduction

As the information technology in business develops, many companies store and process large sets of customer data, which may include sensitive personal information. Incidents of data breaches that reveal company secrets or confidential client information can affect the firm seriously [1][17]. Leakage of sensitive information may cause customers to lose trust in the company and lead to the loss of a firm's market value [1]. Several studies have demonstrated the impacts of data breach incidents on stock price [1][15][17]. These studies show that data breach announcements lead to significant negative market return. For example, Telang and Wattel [25] evaluate the impact of software vulnerability announcement on firms, and find that firms will lose 0.6% of their market value. Cavusoglu et al. [9] conclude that firms lose 2.1% of their market value within two days after the announcement of a breach event. Several studies state that the exposure of confidential data will result in negative CAR [1][15][17].

Different characteristics of data breach events have been identified in the previous literature. Researchers extract different characteristics of these incidents and evaluate their impacts to firm's market value. They find that some of the variables have very significant impacts on the stock return. Some of the recent studies are listed in Table 1. As shown in Table 1, researchers have mainly focused on evaluating the impacts of breach types, time, firm's characteristics and types of industry to firm's market value. Chai et al. [26] evaluate the SOX law's impact to the market reaction and conclude that CAR is more positive after the law. Firms that belong to different industries will have different market reactions to breach events. CAR due to information security breach is larger for BSFI (Business, financial, service, insurance) firms [19]. Internet specific companies suffer more on stock value after security breach incidents [2].

Although there are extensive empirical studies on the impacts of breach types, industry types and firm characteristics on firm's market value, little is known about the firm's actions toward data breach incidents, and how investors react to firms' actions. Our paper differs from previous studies in that *we aim to examine whether the variations of market reactions can be explained by the firm actions after the breach events (see Table 1)*. In the face of data breach events, different companies may take different actions. The content of news media may reflect these actions. But from the literature review, we find that few papers mention possible firm actions toward the data breach events and their impacts to firms' equity value.

According to previous literature [13] and our observation of data breach incidents, we know that some firms are reluctant to disclose information about data breaches to their customers or the public. Firms may be concerned with the potential drop in firm equity value following the revelation of a data breach. In this paper, we believe whether the firm chose to disclose information to the public after the data breach

URI: http://hdl.handle.net/10125/41764
ISBN: 978-0-9981331-0-2

Table 1 Summaries of previous literature and comparison with this paper

Categories	Variables	Studies	Findings
Breach type	Vulnerabilities of software	Telang and Wattel (2007)	Lose 0.6% market value
	Availability	Gordon (2011)	CAR significantly impacted by breach type availability
	Exposure of confidential data	Acquisti et al. and Gatzlaff (2006)	Negative CAR
		Gatzlaff, K. M., & McCullough, K. A. (2010)	Negative CAR
		Campbell et al. (2003)	Negative CAR
Time	Before or after law (SOX)	Chai et al. (2011)	CAR more positive after the law
	Earlier discovery of breaches	Cavusoglu et al. (2004)	Earlier discovery is better
	Before or after 911	Gordon (2011)	Pre 911 significant, after not
		Telang and Wattel (2007)	Pre 911 not significant, after 911 significantly negative
Firm characteristics	Firm Competitiveness	Telang and Wattel (2007)	Significantly negative
	Firm Size	Das et al. (2012)	CAR is larger for smaller firms
		Cavusoglu et al. (2004)	Smaller firms lose more
		Acquisti et al. (2006)	Large companies have positive CAR
	Firm Growth	Goldstein et.al (2011)	Negatively affected by security breach
Type of industry	Internet specific industry	Das et al. (2012)	CAR due to IS breach is larger for internet firms
		Cavusoglu et al. (2004)	Internet firms lose big
		A. Hovava and J. D'Arcy (2003)	Internet specific company suffer more
	BFSI (Business, financial, service, insurance)	Das et al. (2012)	CAR due to IS breach is larger for BSFI firms
	SIC60/62	Leung and Bose (2008)	Negatively affected by security breach
		Goldstein et.al (2011)	Negatively associated with CAR
Severity	Number of individuals affected	Acquisti et al. (2006)	>100000 significant
	Number of records breached	*This paper*	*CAR significantly negative*
	Damage potency	Telang and Wattel (2007)	More severe significantly negative
Firm actions (not related to events)	Clustering the textual contents of information security in 10-K report	Tawei Wang et al. (2013)	Significant if disclosing security risk factor with action-oriented terms in 10-K
	Investment for IT security improvement	Chai et al. (2011)	Positive CAR
Firm reactions related to events	Provide patches	Telang and Wattel (2007)	CAR significantly positive
	Notify customer or public	*This paper*	*CAR significantly Positive*
	More event information disclosed	*This paper*	*CAR significantly Negative*

is a strategic action. This decision may determine the change of market value of the firm.

In order to obtain information about the different firm actions after the data breach events, we utilize data collected by The Privacy Rights Clearinghouse[1]. This database provides a description of each data breach event. We find that whether the firm initiates to disclose data breach information to the public can be revealed from the textual contents of the description. We seek to discover whether this type of firm action will impact the firm's market value during the data breach event period.[2] Using content analysis on the description of the data breach events, we evaluate whether the results will have impacts on the firm's equity value through an empirical study. Our findings on the anticipated market reaction should provide corporate executives with guidance on managing public disclosure of data breach incidents.

The rest of the paper is structured as follows. After the introduction, four hypotheses are derived in Section 2. We then describe the data collection process and methodology in Section 3. Next, we analyze the textual data of the disclosed information about the data breach events and present the results of data analysis and implications in Section 4. Finally, we conclude the paper with a discussion of contributions, limitations and future research in Section 5.

2. Theoretical backgrounds and hypotheses development

Previous event studies [1][15][17] show that the announcement of a data breach incident will cause a negative effect to firm's market value. But no literature considers the firm's decision to notify the data breach event to customers or the public as a factor to impact the market return. In our view, timely disclosure can be used to reduce the legal and reputation cost of bad news [25]. Firm's disclosure behavior also prevents competitors from unambiguously inferring that these firms are hiding information [8]. A previous study shows that voluntary disclosure of bad news is a special type of disclosure sometimes necessary for firms [22]. Other studies find that stock price responses to voluntary disclosures vary [8][24]. As mentioned previously, most firms seek to withhold data breach information in fear that the breach disclosure may affect their market value. Early research in Accounting shows that firms chose to disclose only when it can maximize their profit [28]. We believe that although data breach announcements may lead to negative market reactions, if a firm initiates the notification to their customers or the public early, the result could be different since this will add confidence to the investors due to timely disclosure. Even though companies could try to withhold the breach information, the events may be disclosed by other news media, which may cause the investors to lose trust in the company.

However, although we believe that a firm would benefit from voluntary disclosure of data breach events, the effect may not be equal for all the events. The severity of the event would weaken the benefit of voluntary disclosure. Previous research shows that if the breach announcement suggests that the breach is severe, it could cause a significantly negative impact to the firm's CAR [25]. We believe the disclosure of a data breach event with larger data record loss could lead to more negative confidence on a firm's security controls. The notification of severe data breach events could damage a firm's reputation and cause loss in share price. Therefore, the benefit of voluntary disclosure would depend on the severity of the event. We believe that the number of records breached could be a good proxy to measure the severity of the data breach event. Thus, we hypothesize:

H1a: Firms' early initiation of notifications to customers or the public about data breach incidents will positively affect CAR.

H1b: Higher number of breached records would weaken the positive effect that voluntarily disclosure would bring.

The amount of breach related information to disclose is another issue that firm managers need to consider. To determine the amount and type of information to disclose, firms face a number of trade-offs. Better disclosure can increase investor awareness of the firm and hence reduce the cost of capital and increase equity valuation [5]. According to Berglöf and Pajuste [5], when providing firm information to shareholders, better performing firms should disclose more. Greater disclosure benefits the firms with good news, but the effect is exact opposite for firms with bad news to disclose [29]. It suggests that the disclosure of more bad news information may carry direct financial costs to the firm. Research also shows that there are increased costs from increased transparency [13]. Based on the previous research, we believe that firms

[1] It is a nationally recognized consumer education and advocacy nonprofit dedicated to protecting the privacy of American consumers. Data were collected from http://www.privacyrights.org/data-breach

[2] The information on the database is usually updated 1 or 2 days after the event happened. From our observation, we think the content of the event description usually can reflect the main information that was related to the event. We assume the description of the events can reflect some actions performed by the breach company 1 or 2 days after the data breach.

have to weigh the costs and benefits of the amount of information disclosed to the public. We think that for bad news like data breach incidents, too much information disclosure may signal higher severity and cost to remedy the incident and may cause negative impact to the company's equity value. Therefore, we hypothesize:

H2: More information disclosed related to the data breach events will lead to more negative CAR.

By studying 79 breach events, Acquisti et al. [1] states that a breach of more than 100,000 subjects will reduce the return on stock price by 1.2%. A company's costs for data breach events depend on the number of individuals whose information has been compromised. Telang and Wattel [25] manually categorize breach events as severe or not, and find that the security breach events categorized as severe could cause a significantly negative impact to the firm's CAR. As mentioned earlier, we believe that the number of records breached could be used to measure the severity of the data breach event. Larger data record loss could lead to larger financial losses due to litigation and remedy measures. Thus we have:

H3: The number of records breached will negatively affect the CAR.

Repeated disclosure of severe data breaches and newspaper headlines could lead to a significant reputation damage and loss in share price [1]. We believe that for severe data breach events, exposure of larger amount of event related information may draw investors more attention on the severity of breach events, and more likely lead to loss in reputation and investor trust. If both the amount of event related information disclosed and breach records are in relatively high levels, we expect that negative cumulative abnormal market return would be higher than if there were higher amount of event information disclosed but a lower number of breach records. We would also expect that negative CAR would be lower if there are low levels of both the amount of information disclosed and breach records. Therefore, we hypothesize:

H4: Higher amount of breach event related information disclosed and higher number of breached records will cause more negative CAR to a company than otherwise.

3. Data collection and methodology

3.1. Data collection

Our data collection consists of a two-step process. First we use data breach events provided by Privacy Rights Clearinghouse. The information of Privacy Rights Clearinghouse is obtained from verifiable media sources, government web sites, or blog posts with information pertinent to the breach incidents in question. The database contains a chronology of data breach incidents from 2005 to present. We use the events that happened between 2005 and 2015. There are 4712 events collected from the database during this time period. The data breach events are included in our sample if the firms are public trading companies in the USA. After filtering, we included 517 events. Then, in order to verify the data sources, we also extracted events from news articles using keyword searching in Factiva. We collected news articles about these public trading firms that have breach announcements reported in major news media during the 10-year window. We searched in the Factiva database and used the following terms: (1) data breach, (2) hack, (3) virus, (4) privacy breach, (5) cyber attack, (6) unauthorized access, (7) data theft, (8) identity theft, (9) phishing, (10) denial of service. This method is similar to one used in previous studies [15][16][32] for finding breach events. After this process, we identified 101 data breach events that happened to firms traded in the USA. We find that in all case the 101 events are included the Privacy Rights Clearinghouse database within 1 or 2 days after the event happened.

Table 2. Distribution of events by year

Year	Number of Events
2005	25
2006	71
2007	63
2008	30
2009	22
2010	77
2011	47
2012	60
2013	63
2014	48
2015	24

3.1. Methodology

In this paper, we use the event study method to compute the cumulative abnormal return (CAR), based

on a sample of 517 data breach events that happened to the publicly traded companies in the US. Event study methodology has been used extensively in management science and finance to measure the impact of various corporate events [1][15][27]. To better compare our results to the previous research, we used similar methodology applied in earlier event studies about market reactions to breach events [1][21][25].

We estimate CAR using the four-factor model [6][20]. Several studies have estimated abnormal returns using the four-factor model [30][33]. The four-factor model posits a linear relationship between the stock return and four factors over a given time period (Formula 1):

$$R_{it} = \alpha_i + R_{ft} + \beta_{i1}[R_{mt} - R_{ft}] + \beta_{i2}SMB_t + \beta_{i3}HML_t + \beta_{i4}UMD_t + \varepsilon_{it} \quad (1)$$

where R_{it} is the return of stock i on day t, α_i is the intercept of the relationship for stock i, R_{ft} is the risk-free return on day t, R_{mt} is the return on the market portfolio on day t, SMB_t is the small minus big size portfolio return on day t, HML_t is the high minus low book-to-market portfolio return on day t, UMD_t is the past-one-year winners-minus-losers stock portfolio return on day t, and ε_{it} is the error term [14]. Abnormal returns are defined as the difference between the actual return and an estimated expected return in the absence of an event. The estimation window is generally between 120 days and 200 days. In our case, we define a 200-day estimation period, starting at day -200 until day -11 before the event announcement. We end the estimation period 10 trading days prior to the event day.

Using OLS regression over the estimation period of 200 trading days, we estimate the parameters of the four-factor model. The abnormal return AR_{it} for firm i on day t is the difference between the actual and the expected return. The abnormal return from the four-factor model is as follows:

$$AR_{it} = R_{it} - (\hat{\alpha}_i + R_{ft} + \hat{\beta}_{i1}[R_{mt} - R_{ft}] + \hat{\beta}_{i2}SMB_t + \hat{\beta}_{i3}HML_t + \hat{\beta}_{i4}UMD_t + \varepsilon_{it} \quad (2)$$

Since we have N observations (N = 517 events), the mean abnormal return across all observations can be calculated as $\overline{A}_t = \sum_{i=1}^{N} AR_{it}$. The cumulative abnormal return (CAR) for a given time period can be calculate using

$$CAR[t_1, t_2] = \sum_{t=t_1}^{t_2} \overline{A}_t \quad (3)$$

The period of interest for which we conduct the event study is known as event window. The date of announcement is defined as day 0. In practice, the event window often includes day 0 and day 1. By using Formula 3, we calculate the CAR for the event over the event window.

4. Results

Our interest in this paper is to explore whether firm actions toward the breach events will have impacts on the market reactions to the incidents. For each of the 517 events we collected, we calculate the cumulative abnormal returns (CAR) using event window of day 0 and day 1. The CAR results are used as a dependent variable in our analysis. After estimating the CAR, a regression analysis is conducted to investigate the possible factors behind a firm's market value loss. In the regression model, we control firm size, firm industry, and breach time, which are often found by previous research to be associated with abnormal market return [12][18][32]. We also consider several factors that rarely appear in data breach event studies including whether firm initiates the notification to the public, the amount of information disclosed and number of records breached.

We analyze the language used in the event description collected by Privacy Rights Clearinghouse database. According to our observation of the event description data for the 517 events, we believe that the event description can reflect the main information that relates to the event. When measuring whether a firm initiates the notification to the public, we look at whether the description contains "notify", "inform", "announce", "disclose", "release" and similar words. (Table 3) *D_Notify* is 1 if the event description contains these words and without negative vocabulary before them. *D_Notify* is 0 otherwise. For the 517 events, 121 of the events are marked as 1 for D_Notify. We also look at the length of the description; we think that the longer length suggests more information of the events were disclosed. At last, we measure the impact of breached records. In our analysis, the logarithmic transformation is used to measure the length of the description and the number of records breached.

We develop three regression models. The variables we observe and the definitions are listed in Table 4. The results of the regression model are listed in Table 5. In all three models, VIF values for our variables ranged from 1.03 and 1.46, below the VIF value of 10. So our models don't have the concern for multicollinearity. A comparison of Models 1, 2 and 3

suggests that the variables promoted by this paper will better indicate the market reaction toward data breach events.

Table 3: Sample events with or without firm initiated notification

Date public	Company	Keywords	Description
3/2/15	Natural Grocers	Announce	Natural Grocers announced a possible data breach of its customer payment cards. The grocery retailer claims they have not received any reports or complaints…
1/5/15	Morgan Stanley	Notify	An employee of Morgan Stanley stole customer information on 350,000 clients including account numbers…The employee has since been fired and the bank is notifying all of the individuals affected….
9/2/14	The Home Depot	Announce	The Home Depot has announced the data breach they suffered earlier this month has affected approximately 56 million credit and debit cards. This makes this breach the second largest breach ever…
5/24/12	General Communication Inc. (GCI)	Notify	A former customer service representative gathered account information directly from two customers…. GCI decided to notify all other customers who may have been contacted by the dishonest former employee….
6/9/11	Citibank	Release	Hackers have managed to access the information of approximately 1% of Citibank's 21 million users… Citibank released an official statement on the Citigroup website…
9/21/07	Citigroup	/	Three spreadsheets containing 5,200 Social Security numbers and other personal details about customers were inadvertently leaked over an online file-sharing network by a former employee. Tiversa, a company that monitors P2P networks, found Excel spreadsheets from the desktop of a financial analyst at ABN. Although Tiversa found over 10,000 files, deduplication revealed only 5,208 unique Social Security numbers, along with names and what type of mortgage each customer had.
8/12/08	Wells Fargo	Notify	Wells Fargo is notifying customers that hackers have accessed their confidential personal data by illegally using its access codes. Personal information including names, addresses…

The first model we only use the control variables raised by previous studies. The model equation:

$$CAR[t_1,t_2] = \beta_0 + \beta_1 Firm\_Size + \beta_2 Industry\_BSR + \beta_3 Industry\_BSF + \beta_4 Time + \varepsilon \quad (4)$$

The result in Model 1 is very similar to the previous studies. Larger firm size will have significant positive impact on firm's performance after the breach. Negative CAR due to data breach is larger for firm belongs to business, financial and insurance industry. The year 2008 to 2009 is significant negative.

Using Model 2, we evaluate the firm action related variable D_Notify. We tested the statistical significance of firm's action of initiate the notification of data breach. The result indicates the market reactions to data breach after taking into consideration of firm behavior. We control the variables in Model 1. The model equation is:

$$CAR[t_1,t_2] = \beta_0 + \beta_1 D\_Notify + \beta_2 D\_Length + \beta_3 D\_Record + \beta_4 Firm\_Size + \beta_5 Industry\_BSR + \beta_6 Industry\_BSF + \beta_7 Time + \varepsilon \quad (5)$$

Table 5 shows the coefficient estimate for *D_Notify* (0.0029). The significant positive coefficient of *D_Notify* suggests that when the firm initiates the notification to customers or the public, there is a

statistically significant positive market reaction. We measure the amount of event related information disclosed using *D_Length* (-0.0088). The significant negative coefficient of *D_Length* suggests that if too much event related information is disclosed to the public, it will have negative impact on a firm's market reaction. Model 2 adds number of records breached as another variable to test the market reaction. With coefficient at -0.0007 and p-value less than 0.05, the results indicate that the market reaction is significantly negative toward the number of records that was breached in a data breach event. Thus the results support our Hypothesis 1a, 2 and 3.

In Model 3, we add interaction term D_Notify*D_Record to measure whether the interaction between voluntary disclosure and breach record would cause impact on CAR. With coefficient at -0.0013 and p-value less than 0.05, we conclude that larger number of breached records would weaken the positive effect of voluntarily disclosure. We also add D_Length*D_Record to evaluate whether the interaction between the amount of event related information disclosed and the number of records breached have more negative impact on a firm's CAR. With p-value <0.0001, we conclude that the impact of D_Length on abnormal return depends on the level of D_Record significantly. The coefficient estimate (Table 5) for D_Length*D_Record (-0.0028) suggests that D_Length will enhance the negative impact of D_Record and vice versa. We conclude that firms with larger number of records breached and more event related information disclosure will have greater negative CAR. Thus Hypothesis 1b and Hypothesis 4 are supported.

Table 4: Model Variables and Definitions

	Variables	Definition and Calculation
Dependent Variable	*CAR [t1,t2]*	Cumulative abnormal return over [0,1] event window, measured in percentages
Independent Variables	*D_Notify*	Dummy variable equals to 1 if firm initiates the notification of data breach event
	D_Length	The length of the event description, indicating the amount of event information disclosed. Values have been transformed using the logarithm function.
	N_Record	The number of records breached in the data breach event. Values have been transformed using the logarithm function.
	*D_Notify*D_Record*	The interaction term between voluntarily initiates the notification of data breach event and the number of records breached.
	*D_Length*D_Record*	The interaction term between the length of the event description and the number of records breached.
Control Variables	*Firm_Size*	Total assets of the firm. Values have been transformed using the logarithm function.
	Industry_BSF	Dummy variable equals to 1 if the firm belong to Business- financial and insurance service
	Industry_BSR	Dummy variable equals to 1 if firm belong to Business-Retail/Merchant
	Time	Measure whether it is year 2008-2009.

Table 5: CAR Regression Results Given the Characteristics of the Data Breach Events

Variables	Model (1) Coefficient(t-statistic)	Model (2) Coefficient(t-statistic)	Model (3) Coefficient(t-statistic)
Intercept	0.0043(-1.48)	0.0107(2.36)**	0.0046(0.99)
D_Notify		0.0029(1.97)**	0.0033(2.23)**
D_Length		-0.0088(-4.15)***	-0.0051(-2.30)**
N_Record		-0.0007(-2.31)**	-0.0002(-0.73)
*D_Notify*D_Record*			-0.0013(-2.15)**
*D_Length*D_Record*			-0.0028(-3.82)***
Firm_Size	0.0013(1.79)**	0.0015(2.32)**	0.0013(2.22)**
Industry_BSF	-0.0023(-1.55)	-0.0026(-1.74)*	-0.0021(-1.47)
Industry_BSR	0.0011(0.73)	0.0014(0.92)	0.0017(1.15)
Time	0.01(-4.67)***	-0.0101(-4.67)***	-0.0095(-4.54)***
R^2	0.06	0.10	0.15
N Observations	517	517	517

*Significant at 10%, ** significant at 5%, ***significant at 1%

5. Discussions and Future Research

We believe that our study offers a worthwhile contribution to the existed literature. We find new factors that can indicate some types of firm actions toward data breach event. By looking at the result of our investigation, we think that firms can take possible managerial controls on data breaches. Our finding indicates that the market will reward firms that take the action to notify the customers immediately after the breach event. The results show that firms that initiate the notification of data breach event timely will have a positive impact on the market return. However, although voluntary disclosure of data breach events can have a positive effect to CAR, larger number of breach records would weaken the effect. The observation can provide help when firms face the dilemma that disclosure of data breach event may cause damage to the firm's public image. We also investigate the association between the amount of information that was disclosed to the public and market reaction. We believe that greater amount of event related information disclosure will lead to more negative stock reaction. We further find that firms with both larger amount of event related information disclosed and larger breached records will have greater negative market reaction. We find that market tends to punish more for the firms when the amount of event related information and number of records both increased. Although firms may not be able to manipulate the amount of information available to the public related to the data breach event, firms may have some extent of controls over the information that will be disclosed to the public. We believe this result is useful in helping firms design their proper incident response planning strategies. When a larger number of records was breached in the event, firm should disclose less event related information to the public in less regulated industries.

The limitation of our study mainly lies in the data we used. This paper used the event description collected and updated by the Privacy Rights Clearinghouse database. The descriptions are the secondary sources collected from news media, government site or blogs. This may not reflect all the information that investors may take into consideration. Future research may build on our results and perhaps validate our findings through more comprehensive sets of data. Second, the keywords we are using may not reflect all the firm's voluntarily disclosure behavior.

Some actions performed by firms toward data breach event could be missing from our data. In the future, we will improve our categorization scheme and have more comprehensive analyses on the firm actions. Third, when calculating the CAR, we didn't use control firms as a benchmark. We plan to add this in our future work. Fourth, this paper only measures short-term market reaction around the breach date. However, more information regarding to the data breach incidents may be added in follow-up news articles, which we did not consider in this study. This will be addressed in our future work.

6. Acknowledgement

This research was supported by both Center for Business Intelligence and Analytics at Virginia Tech (CBIA) and the Natural Science Foundation of China (Grant# 71531013).

7. References

[1] A. Acquisti, A. Friedman, and R. Telang, "Is There a Cost to Privacy Breaches? An Events Study," *Fifth Work. Econ. Inf. Secur.*, pp. 1--20, 2006.

[2] A. Hovav and J. D'Arcy, "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms," *Risk Manag. Insur. Rev.*, vol. 6, no. 2, pp. 97–121, 2003.

[3] A. Malhotra and C. Kubowicz Malhotra, "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach," *J. Serv. Res.*, vol. 14, no. 1, pp. 44–59, 2011.

[4] D. J. Skinner, "Why Firms Voluntarily Disclose Bad News," *J. Account. Res.*, vol. 32, no. 1, p. 38, 1994.

[5] E. Berglöf and A. Pajuste, "What do firms disclose and why? Enforcing corporate governance and transparency in central and Eastern Europe," *Oxford Rev. Econ. Policy*, vol. 21, no. 2, pp. 178–197, 2005.

[6] E. F. Fama and K. R. French, "Common risk factors in the returns on stocks and bonds," *J. financ. econ.*, vol. 33, no. 1, pp. 3–56, 1993.

[7] F. K. Andoh-Baidoo, K. Amoako-Gyampah, and K. M. Osei-Bryson, "How internet security breaches harm market value," *IEEE Secur. Priv.*, vol. 8, no. 1, pp. 36–42, 2010.

[8] G. Pownall, C. Wasley, and G. Waymire, "The Stock Price Effects of Alternative Types of Management Earnings Forecasts," *Account. Rev.*, vol. 68, no. 4, pp. 896–912, 1993.

[9] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *Int. J. Electron. Commer.*, vol. 9, no. 1, pp. 69–104, 2004.

[10] J. Cardenas, A. S. Coronado, A. Donald, F. Parra, and M. A. Mahmood, "The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation," *18th Am. Conf. Inf. Syst. AMCIS 2012, Seattle, Washingt. August 9-11, 2012*, no. 2004, pp. 1–9, 2012.

[11] J. Goldstein, A. Chernobai, and M. Benaroch, "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories," *J. Assoc. Inf. Syst.*, vol. 12, no. 9, pp. 606–631, 2011.

[12] J. Kwon, J. Rees Ulmer, and T. Wang, "The Association between Top Management Involvement and Compensation and Information Security Breaches," J. Inf. Syst., vol. 27, no. 1, p. 121019083608008, 2012.

[13] J. Lakonishok and S. Smidt, "Volume for Winners and Losers: Taxation and Other Motives for Stock Trading," *J. Finance*, vol. 41, no. 4, pp. 951–974, Sep. 1986.

[14] K. B. Hendricks, "An Empirical Investigation on the Appointments of Supply Chain and Operations Management Executives," *Manage. Sci.*, vol. 61, no. 7, pp. 1562–1583, 2015.

[15] K. Campbell, L. a Gordon, M. P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *J. Comput. Secur.*, vol. 11, no. May 2001, pp. 431–448, 2003.

[16] K. Kannan, J. Rees, and S. Sridhar, "Market Reactions to Information Security Breach Announcements: An Empirical Analysis Literature Review," *Int. J. Electron. Commer.*, vol. 12, no. 1, pp. 69–91, 2007.

[17] K. M. Gatzlaff and K. A. McCullough, "The effect of data breaches on shareholder wealth," *Risk Manag. Insur. Rev.*, vol. 13, no. 1, pp. 61–83, 2010.

[18] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?," *J. Comput. Secur.*, vol. 19, no. 1, pp. 33–56, 2011.

[19] M. Das, Saini; Mukhopadhyay, Arunabha; Anand, "Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics," *J. Inf. Priv. Secur.*, vol. 8, no. September, pp. 27–56, 2012.

[20] M. M. Carhart, "On Persistence in Mutual Fund Performance," *Journal of finance*, vol. 52, no. 1. pp. 57–82, 1997.

[21] O. Hinz, M. Nofer, D. Schiereck, and J. Trillig, "The influence of data theft on the share prices and systematic risk

of consumer electronics companies," *Inf. Manag.*, vol. 52, no. 3, pp. 337–347, 2015.

[22] O. Yosha, "Information Disclosure Costs and the Choice of Financing Source," *J. Financ. Intermediation*, vol. 4, no. 1, pp. 3–20, 1995.

[23] P. C. Tetlock, M. Saar-Tsechansky, and S. MacSkassy, "More than words: Quantifying language to measure firms' fundamentals," *J. Finance*, vol. 63, no. 3, pp. 1437–1467, 2008.

[24] R. Jennings, "Unsystematic Security Price Movements, Management Earnings Forecasts, and Revisions in Consensus Analyst Earnings Forecasts," Journal of Accounting Research 25: 90-110, 1987.

[25] R. Telang and S. Wattal, "An empirical analysis of the impact of software vulnerability announcements on firm stock price," IEEE Trans. Softw. Eng., vol. 33, no. 8, pp. 544–557, 2007.

[26] S. Chai, M. Kim, and H. R. Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decis. Support Syst.*, vol. 50, no. 4, pp. 651–661, 2011.

[27] S. Goel and H. A. Shawky, "Estimating the market impact of security breach announcements on firm values," *Inf. Manag.*, vol. 46, no. 7, pp. 404–410, 2009.

[28] S. J. Grossman, "The Informational Role of Warranties and Private Disclosure about Product Quality," *J. Law Econ.*, vol. 24, no. 3, pp. 461–483, 1981.

[29] S. P. Kothari, S. Shu, and P. D. Wysocki, "Do managers withhold bad news," *J. Account. Res.*, vol. 47, no. 1, pp. 241–276, 2009.

[30] S. Thirumalai and K. K. Sinha, "Product Recalls in the Medical Device Industry: An Empirical Exploration of the Sources and Financial Consequences," *Manage. Sci.*, vol. 57, no. 2, pp. 376–392, 2011.

[31] T. Wang, J. R. Ulmer, and K. Kannan, "The textual contents of media reports of information security breaches and profitable short-term investment opportunities," *J. Organ. Comput. Electron. Commer.*, vol. 23, pp. 200–223, 2013.

[32] T. Wang, K. N. Kannan, and J. R. Ulmer, "The Association Between the Disclosure and the Realization of Information Security Risk Factors The Association Between the Disclosure and the Realization of Information Security Risk Factors," *Inf. Syst. Res.*, no. April 2014, 2013.

[33] X. F. Zhang, "Information Uncertainty and Stock Returns," *J. Finance*, vol. 61, no. 1, pp. 105–137, 2006.