7-1-2023

Data Breach Announcements: Evaluating the Content and Timing of Breach Announcements and Their Effect on Firm Value

Paul Viancourt

Brian Walkup

DATA BREACH ANNOUNCEMENTS: EVALUATING THE CONTENT AND TIMING OF BREACH ANNOUNCEMENTS AND THEIR EFFECT ON FIRM VALUE

Paul Viancourt
Rollins College
PViancourt@rollins.edu

Brian R. Walkup
Rollins College
BWalkup@rollins.edu

ABSTRACT

Cybercrime has significant impacts to firms. One way to measure the significance of cyber events such as data breaches to firm valuation is using event studies. However, the findings of previous event studies in this area have been mixed and need additional research. Additionally, the effect of firm-specific actions contained in the breach announcement, as well as the timeliness of the breach notification itself, have yet to be studied. The current research applied four event study models to data breach announcements over the period 2017-2021, resulting in statistically significant negative cumulative average abnormal returns (CAAR) in days immediately surrounding the breach announcement. A series of cross-sectional regression analyses noted that shareholders reacted more favorably to breach responses including free credit monitoring for those affected and the hiring of a forensic expert. However, investors generally reacted more negatively to breach announcements during periods of high investor uncertainty.

Keywords Data Breach, Event Study, Indirect Cost, Firm Valuation, Abnormal Returns

INTRODUCTION

As firms increasingly leverage information technology in every aspect of their business, the customer data that they collect, store, transmit, and share continues to be a valuable commodity to hackers and organized crime groups who seek to illegally access and exploit this data for financial gain. The likelihood that a firm will experience a data breach is significant and increasing. There were 3,950 data breaches in 2019, which spiked in 2020 by 33.1% to 5,258 before leveling off in 2021 (Basset et al., 2020; Basset et al., 2021).

Loss of customer data via data breach has significant consequences for breached firms, the most immediately impactful of which are the direct costs associated with the breach. Direct costs refer to "unbudgeted, out-of-pocket spending" related to a breach, which includes costs associated with product or service discounts, client notifications, legal fees, administrative fees, call center expenses, and investor relations (Tanimura & Wehrly, 2015). According to The Ponemon Institute (2022), the direct costs to firms of data breaches are significant at $4.3 million per breach in 2022 (p. 5).

As both the likelihood and impact of a data breach are significant, our research questions focus on how the firm's identification and handling of a breach may affect the actions of shareholders. Specifically, does the length of time between when a breach occurs and when it is reported affect shareholder actions? Are the post-breach actions of the firm taken into consideration by shareholders? If so, which actions are seen as most valuable? We are also curious as to the effects of investor distraction. Specifically, will investors act as severely to the announcement of a breach when there is significant market uncertainty?

This research intends to add value to practitioners by allowing firms to properly align their risk mitigation strategies according to the perceived financial risks. We also intend to add value to scholars by furthering the body of knowledge in this area using a research design focused on announcements of data breaches where personally identifiable information was exposed.

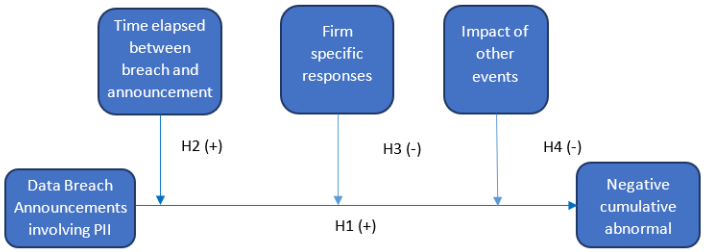

Figure 1. Theoretical Model

LIMITED LITERATURE REVIEW, HYPOTHESES, & METHODOLOGY

While previous research has attempted to measure breach-related costs using event studies to capture abnormal returns in the stock price of breached firms, the results have been mixed. Many have found negative cumulative abnormal returns (CAR) (e.g., Tanimura & Wehrly, 2015, Johnson et al., 2017, Michel et al., 2020 and others), numerous others have found no abnormal returns (e.g., Das et al., 2012, Bolster et al, 2010, Pirounias et al., 2014), and some have even found mixed results among various data subsets (e.g., Kannan et al., 2007; Yayla & Hu, 2011). Based on the findings of previous event studies that focused on breaches of personal identifying information, it is hypothesized that:

H1: Announcements for data breaches where personally identifying information has been compromised will lead to negative abnormal stock price reactions.

While considerable research has been conducted on the overall effects of data breach announcements, the relationship between the timing of a breach announcement and abnormal returns has only been tangentially investigated (Hovav and Gray, 2014; Amir et al., 2018; Muzatko and Bansal, 2018). This is an important area for future research, as it may provide valuable insight into the motivations of investors as they respond to breach announcements. According to the Ponemon Institute, "the faster a data breach can be identified and contained, the lower the costs" (2019). Thus, it is hypothesized that:

H2: The longer the length of time between the occurrence of a breach involving personally identifying information and the associated breach announcement, the more negative the abnormal stock price reaction will be.

Investors may also evaluate the firm's response to a breach and reward or punish firms accordingly. While previous research has identified the importance of firm actions post-breach announcement, none have specifically evaluated the impacts of specific actions contained in the breach announcement and their effect on abnormal returns (Martin et al., 2017; Malhotra and Malhotra, 2011). Based on the repeated calls for an evaluation of the impacts of specific firm responses to a breach, and consistent with previous research focused on data breaches as service failures, the current research hypothesizes that:

H3: Announcements that acknowledge a specific breach response (identity theft protection, credit monitoring, cooperation with law enforcement, or a forensic investigation) will decrease the negative stock price reaction to data breaches.

The current research aims to add originality and value by furthering the findings of Kannan et al. (2007) that investor distraction will affect abnormal returns. We hypothesize that:

H4: Investor distraction is negatively correlated with abnormal stock price reaction, such that negative cumulative abnormal returns following a data breach announcement will be less severe during periods of high market distraction.

This research utilizes four event study methodologies including the market-adjusted model, market model, Fama-French three-factor model (Fama and French, 1992), and Carhart four-factor model (Carhart, 1997) to calculate cumulative abnormal returns (CAR) based on a sample of data breach announcements reported by publicly traded companies. A total of 8,741 records including data breach announcement dates, breach announcements, and other firm-specific data were provided by the Identity Theft Resource Center (ITRC) spanning the five-year period of 2017 to 2021. After excluding breaches that did not occur at publicly traded firms, duplicate entries, breaches occurring prior to a firm's initial stock trading date or within 250 days of the initial trading day of the firm's stock, multiple breaches of the same firm within a single event window, breaches that were not consistent with the definition of a 'data breach' as used in the current research, and apparent errors within the provided data, a final data set of 442 records of all data breaches during the five-year period were under investigation. To further limit potential confounds, FactSet was queried for firm news announcements within each of the event windows.

RESULTS

To assess the impact of a data breach announcement on the stock price of a breached firm, an event study methodology was utilized using www.eventstudytools.com (Schimmer et al., 2015) to calculate AAR and CAR for each breached firm in two event windows, (-1,1) and (-3,3). Firm-specific abnormal returns were then aggregated to determine the cumulative average abnormal returns (CAAR) for all breached firms. parametric tests were then applied to evaluate the statistical significance of the results, including the adjusted Patell's Z (Patell, 1976), the standardized cross-sectional test, and the adjusted cross-sectional test **(**Kolari & Pynnönen, 2010). A series of regression analyses were conducted to test the hypotheses identified in the previous section. Refer to Table 1 for the results of CAAR analyses and related parametric testing.

	All Breaches		PII Breaches Only	
Event Window	**(-1,1)**	**(-3,3)**	**(-1,1)**	**(-3,3)**
n=	397	336	343	288
Market Adjusted Model	-.002**	-.008**	-.001*	-.006**
	(-2.01)	(-2.49)	(-1.71)	(-2.2)
Market Model	-.001*	-.006**	-0.001	-.006**
	(-1.8)	(-2.23)	(-1.6)	(-2.06)
Fama-French	-.008**	-.006**	-.001*	-.006**
Three-Factor Model	(-1.9)	(-2.37)	(-1.91)	(-2.4)
Carhart	-.001*	-.005**	-.001*	-.006**
Four-Factor Model	(-1.66)	(-2.21)	(-1.8)	(-2.21)

Notes: *,**, and *** denote significance at the 10%, 5%, and 1% levels, respectively. Significance calculated using adjusted Patell's Z-test.
The windows (-5,5) and (-10,10) were also examined but untabulated.

Table 1. Cumulative Average Abnormal Returns for All Models

A review of AAR values indicated that data leakage on event day -3 significantly and negatively affected abnormal returns, which was then exacerbated by the market's negative reaction to the announcement on the announcement day. This negative market reaction continued post-announcement, as investors fully digested and responded to new market information. Refer to Figure 2 for a graphical depiction of abnormal returns as they accumulate through the (-3,3) event window for all reported breaches and breaches of PII data, respectively.

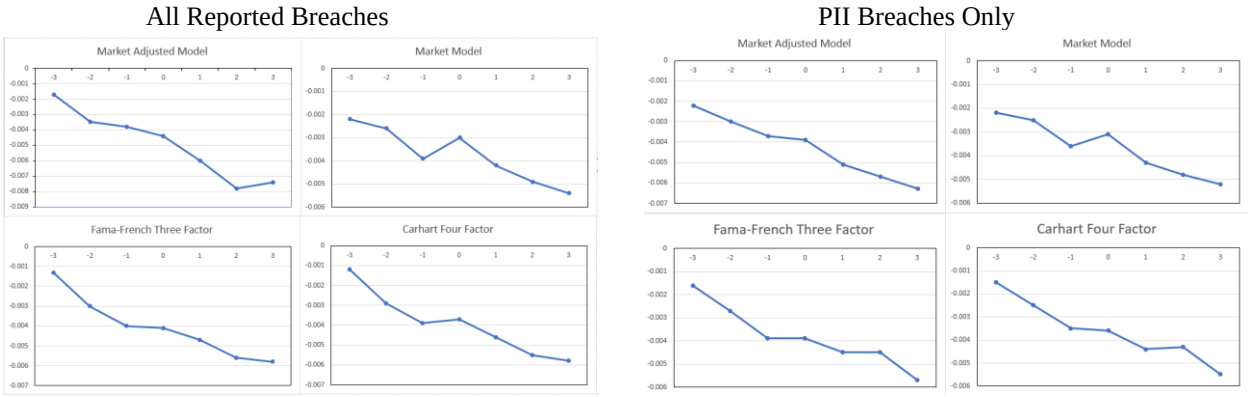

Figure 2. CAAR Output for All Reported Breaches and Breaches of PII Data Only in the (-3,3) Window

While these effect sizes generally appear insignificant in the context of social science research, they become significant in event study research due to the impact that these seemingly insignificant changes in stock price have on a firm. For example, the average market capitalization for all firms included in the CAAR analysis was approximately $59 billion. If the average effect size of -.63% as noted in the CAAR analyses using the market-adjusted model across all event windows is applied to the average market capitalization for all firms included in the analysis, it results in a decline of almost $372 million in valuation for the average firm included in the sample. If the same analysis is conducted using the aggregate market capitalization of all firms included in the sample ($26.4 trillion), the resulting decline in value across all breached firms is $167 billion. Based on an analysis of the CAAR model outputs, there is empirical support for the main effect hypothesized in H1.

A series of regression analyses were then conducted to test H2, H3, and H4. The regression analysis results are shown in Table 2. A total of 8 regression models were evaluated on the (-3,3) window (the (-1,1) was also evaluated, but not tabulated for brevity). Dependent variables in all regressions were CAAR outputs representing each of the four event study models. Separate regressions were run for all breach announcements and breach announcements where PII was exposed during the breach.

The regression analyses included seven dependent variables. The "reporting gap" variable was calculated as the time, in days, between the firm's discovery of the breach and the public announcement and was used to test H2. *Financial Sector* was included as a control variable to test for any potential confounds related to breaches that may disproportionately affect firms in the

financial industry. The variables *Identity Theft*, *Law Enf*, *Forensic Investig*, and *Credit Monitoring* indicated whether a breach announcement included free identity theft protection for those affected, coordinating with law enforcement, hiring external forensics experts or free credit monitoring for those affected, respectively. These variables were used to test H3. The "VIX" variable refers to the Volatility Index and was used to test investor distraction as hypothesized in H4.

	All Breach Announcements				PII Breach Announcements Only			
Event Window	**Mkt. Adj.**	**Mkt.**	**FF3**	**Carhart 4**	**Mkt. Adj.**	**Mkt.**	**FF3**	**Carhart 4**
Reporting Gap	<.001	<.001	>-.001	>-.001	<.001	<.001	<.001	<.001
Financial Sector	.004	.003	<.001	<.001	.004	.004	>-.001	<.001
VIX	-.001 *	-.001 *	<.001	-.001	-.001 **	-.001**	-.001	-.008 *
Identity Theft	-.016	-.017	-.009	-.008	-.017	-.018	-.009	-.008 *
Law Enf.	-.006	-.007	-.008	-.007	-.007	-.008	-.009	-.008
Forensic Inv.	.013 **	.014 **	.012 *	.012 *	.018 **	.019 **	.015 **	.015 **
Credit Monit.	.020 *	.020 *	.019 *	.017	.022 *	.022 *	.024 *	.022 *
Constant	.002	.004	-.001	<.001	.003	.005	-.004	-.003
R^2	.030	.032	.028	.027	.041	.044	.038	.038

Note: *,**, and *** denote significance at the 10%, 5%, and 1% levels, respectively.
All coefficients delineated in unstandardized β values.

Table 2. Regression Model Variable Coefficients for (-3, 3) Event Window

There were no statistically significant results in any of the models for the "reporting gap" variable, indicating that investors are not punishing firms based on the length of time it takes them to report a breach after discovery. As such, H2 is not supported. Conversely, the "VIX" variable was statistically significant at p<.10 in five of the eight models, with two of the models being statistically significant at p<.05 and was negatively related to abnormal returns in all cases. This negative relationship indicates that abnormal returns are more severe during periods when investor distraction is high, contrary to H4.

The firm response variables indicate that shareholders respond more favorably to certain responses than others. Firms including free credit monitoring or hiring external forensic experts were penalized less by market participants. This effect was statistically significant at the p<.10 level or stronger in all eight models for the hiring of external forensic experts, with six being statistically significant at the p<.05 level. For the inclusion of free credit monitoring, the coefficients were statistically significant at the p<.10 level in seven of the eight models. While the findings for coordinating with law enforcement and inclusion of free identity theft were not statistically significant at the p<.10 level, the coefficients were consistently negative indicating that shareholders likely did not see value in these inclusions. H3 is supported for the hiring of external forensic experts and the inclusion of free credit monitoring but is not supported for the inclusion of free identity theft or cooperation with law enforcement.

DISCUSSION

Out of our four hypotheses, only H1 and H3 were supported, while H4 was found to be significant but in the opposite direction as anticipated. Support for H1 indicates investors still react negatively to data breach announcements. A review of the abnormal daily returns in the (-3,3) window indicates that information related to data breaches reaches at least some investors prior to the official announcement date, as is evidenced by negative abnormal returns prior to day (0), consistent with the strong form test of the efficient markets theory (Fama, 1970). Fama's (1970) semi-strong form test of efficient markets theory was also supported, as there were statistically significant findings in both the (-1,1) and (-3,3) windows. Lack of support for H2 seems to indicate that the timeliness of the response does not have bearing on investor decisions.

The mixed results for H3 indicate that shareholders view certain responses by the firm as being more valuable than others. While the impact of the inclusion of identity theft protection and cooperation with law enforcement were not statistically significant, the negative coefficients indicate that, if anything, shareholders view these as destroying value. Conversely, the hiring of external forensic experts and the inclusion of free credit monitoring for those affected were viewed favorably by shareholders with positive and statistically significant coefficients. This implies that companies experiencing a breach should focus on hiring of an external forensic expert and including free credit monitoring over other responses.

While H4 hypothesized that investor distraction would result in less negative reactions to data breaches, the results indicate that investors actually react more negatively during these periods. Given that investor distraction is proxied by the VIX, this

likely indicates that investors penalize the negative news of a data breach with a more negative reaction during periods of market uncertainty. This finding has significant implications for scholars and may form the basis for future research.

CONCLUSION

The current research contributes to the scholarly body of knowledge and provides valuable insight to practitioners in several meaningful areas. Our findings indicate that investors continue to evaluate data breaches as a factor impacting firm valuation and act on this information. This is important for the continued study of data breaches, as it provides empirical support for the position that investors still react to data breach announcements.

Empirical support for H1 also adds value to practitioners, as firms must be aware of the potential short-term erosion to their valuation and proactively select and deploy the appropriate countermeasures to mitigate short-term financial risks to the extent possible. As IT and risk professionals are tasked with making the most efficient use of scarce resources, this knowledge benefits the practitioner by indicating how to best allocate post-breach assets in order to minimize potential negative impacts to share price. As noted above, the CAAR of -.63% may initially seem insignificant. However, this equates to a substantial $372 million average short-term decrease in firm valuation per data breach announcement in the current data set. IT and risk practitioners are constantly evaluating internal controls over IT/cybersecurity/data privacy and are tasked with making effective yet cost-efficient decisions for additional countermeasures. The findings of this research may assist risk cybersecurity professionals as they present a business case to management for additional internal controls to prevent or mitigate the effects of a breach.

This knowledge may also be employed by firms to address strategic risks, with a clearer understanding of how a breach announcement may affect strategy in the short term. Firms may use this knowledge to pursue strategies or engage with vendors or strategic business partners based in part on perceived cybersecurity risks, armed with the foresight that a lapse in cybersecurity may lead to significant consequences if it manifests itself in a data breach.

Similarly, firms may evaluate their reputational risks in the context of these findings. Using negative abnormal returns as a proxy for short-term reputational harm, firms may select and right size countermeasures to protect and preserve their reputation in the event of a data breach. Firms may also use this information to choose vendors and strategic partners more selectively, as there may be shared reputational risks due to a data breach announced by a partner/vendor. Note that breach announcements of vendors were included in the data collection for this research but were ultimately not included in the cross-sectional regression models. Additional research into the impact on a firm of a breach announcement caused by a cybersecurity lapse at a vendor may be warranted to further investigate the possible shared reputational risks between firms, vendors, and/or strategic partners.

The findings regarding the reaction to the inclusion of firm responses (H3) are of high importance to firms. Given shareholders do not respond favorably to the inclusion of free identity theft services or coordinating with law enforcement but do respond favorably to the hiring of a forensic expert and the inclusion of free credit monitoring, this should shape how the firms react both financially and in their public statements.

Contrary to H4, the findings show that data breaches during high VIX periods produce more negative abnormal returns, rather than the predicted less negative abnormal returns. While the prior expectation was that investor distraction may result in less negative abnormal returns, the finding of more negative returns during these periods likely indicates that investors react more strongly during a period of high market uncertainty. This finding appears to have significant benefits for future scholarly research, as it may extend to all types of firm announcements. Future research may expand upon this finding by evaluating how market uncertainty affects myriad other firm news announcements. While not specific to breach announcements, firms may benefit from this research by gaining an understanding of how to appropriately time a significant announcement to the public.

While the current research has significant implications for both practitioners and scholars alike as discussed above, there were inherent limitations. The current research was narrowly focused on breaches of publicly available information (PII) and used a very constricting definition of what type of event constituted a ‘data breach.’ While the scope of the current research was intentionally narrow due to the perceived limitations in the extant literature as discussed in the literature review above, this limits the results to breaches including specific characteristics and exposing a specific type of information. Additional research may be necessary to widen the scope of the research to provide greater generalizability of the results.

REFERENCES

1. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206.

2. Bassett, G., Hylender, C., Langolis, P., Pinto, A., & Widup, S. (2020). Verizon 2020 Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/resources/reports/dbir/
3. Bassett, G., Hylender, C., Langolis, P., Pinto, A., & Widup, S. (2021). Verizon 2021 Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/resources/reports/dbir/
4. Bolster, P., Pantalone, C. & Trahan, E. (2010). Security Breaches and Firm Value. *Journal of Business Valuation and Economic Loss Analysis*, 5(1), 1-11.
5. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.
6. Carhart, M. M. (1997). "On Persistence in Mutual Fund Performance". *Journal of Finance*, 52(1), 57-82.
7. Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security*, *8*(4), 27-55.
8. Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, 25, 383–417.
9. Fama, E. F., & French, K. R. (1992). The cross-section of expected stock returns. *The Journal of Finance*, 47(2), 427-465.
10. Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83.
11. Hovav, A., & Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems*, 34, 893–912.
12. Johnson, M. S., Kang, M. J., & Lawson, T. (2017) Stock Price Reaction To Data Breaches Forthcoming; Journal of Finance Issues.
13. Kannan, K., Rees, J., & Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91.
14. Kolari, J.W., &Pynnönen, S. (2010). Event Study Testing with Cross-sectional Correlation of Abnormal Returns. *Review of Financial Studies*, *23*(11), 3996-4025.
15. Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, *14*(1), 44–59.
16. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58.
17. Michel, A., Oded, J., & Shaked, I. (2020). Do security breaches matter? The shareholder puzzle. *European Financial Management*, *26*(2), 288-315.
18. Muzatko, S., & Bansal, G. (2018). Timing of data breach announcement and E-commerce trust. In *The proceedings of Midwest Association for Information Systems Conference*.
19. Patell, J.M. (1976). Corporate Forecasts of Earnings per Share and Stock Price Behavior: Empirical Tests. *Journal of Accounting Research (Wiley-Blackwell)*, 14(2), 246-276
20. Pirounias, S., Mermigas, D., & 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.
21. Ponemon Institute (2019). Cost of a Data Breach Report 2019. Retrieved from: https://www.ibm.com/security/data-breach
22. Ponemon Institute (2022). Cost of a Data Breach Report 2022. Retrieved from: https://www.ibm.com/security/data-breach
23. Schimmer, M., Levchenko, A., and Müller, S. (2015). EventStudyTools (Research Apps), St.Gallen. Available on: http://www.eventstudytools.com.
24. Tanimura, J. K., & Wehrly, E. W. (2015). The market value and reputational effects from lost confidential information. *International Journal of Financial Management, 5*(4), 18-35
25. Wilcoxon, F. (1945). Individual Comparisons by Ranking Methods. *International Biometric Society*, 1(6), 80-83
26. Yayla, H. H., & 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.