The Impact of Data Breaches on Stock Performance

Riazul Islam

Leonard N. Stern School of Business
Glucksman Institute for Research in Securities Markets
Faculty Advisor: Ingo Walter
April 15, 2020

ABSTRACT

The Impact of Data Breaches on Stock Performance

Riazul Islam

This study focuses on the impact of data breach announcements on stock prices and returns of the affected companies. Data breaches are potentially devastating thefts of data, in many cases personally identifiable, from companies that could be used for a variety of nefarious purposes. While the public discourse suggests that companies are severely punished for becoming data breach targets, the reality is much more mixed, with stock price regressions (using predictions based on widely traded indexes and US Treasury instruments) showing negligible effect on the aggregate, and stock return regressions (using the CAPM model) demonstrating a minor effect on average. However, for companies that have outsized data breaches from both size and severity considerations, the impact on stock price and returns are much more pronounced in the test timeline. With vast quantities of personal data being collected daily by a growing number of companies, and regulators and the public more closely eyeing data protection issues, there is potential for harsher punishment for data breaches in the future.

I. INTRODUCTION

On Monday, July 29th, 2019, Capital One Financial Corporation announced that the company had "suffered a massive data breach, reporting that an outside hacker obtained the personal data of more than 100m customers and applicants for its credit cards."[1] In total, 106 million affected consumers in the United States and Canada were affected, and Capital One, through its partnership with Amazon Web Services in powering its cloud-based systems, became yet another target of a successful data breach that affected a wide swath of the consumer landscape, having the potential to harm nearly the entire US population in some fashion.

Companies large and small are gathering more data on their customers than ever before. In many cases, this data is not being handled with the safety and security that is required to protect against theft by hackers. Hackers are also becoming more sophisticated in their attacks, challenging companies to stay on the cutting-edge of cybersecurity. As a result of incomplete data protections, numerous companies have faced significant data breaches that have collectively exposed billons of data records. While the largest data breach of 2018 hit the Indian government database Aadhar (responsible for storing "citizens' identity and biometric info"), affecting 1.1 billion citizens, most large and known data breaches have afflicted public corporations, ranging from tech giants Google and Facebook to retail conglomerates like Macy's and Nordstrom, financial services companies like CapitalOne and First American, airlines like British Airways and Cathay Pacific, and communications companies like Comcast, (the former) Time Warner Cable, and T-Mobile.[2,3]

[1] https://www.ft.com/content/7c6c6d7a-b269-11e9-8cb2-799a3a8cf37b
[2] https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12
[3] https://www.ft.com/content/5b3046ca-b2d4-11e9-bec9-fdcab53d6959

Hackers typically execute on data breaches for financial gain, taking the data they siphon from companies and monetizing it in various ways.[4] Stolen data is typically aggregated and sold in large bundles on the dark web, often passing through multiple hands to make tracing the chain of exchanges back to the original thief more challenging. The sold data can be quite rewarding for hackers: hacked email accounts can go for $1-15 per account while a full ID package can go for $30-100 per person, according to Symantec's February 2019 Internet Security Threat Report.[5] Many types of data can be monetized this way, such as credit card information, personally identifiable information (PII), and health insurance credentials. Hackers can also hold data ransom, as in the cases of Newark, who paid $30,000 to Iranian hackers to restore their systems, Baltimore, who did not cave to hackers and spent millions of dollars restoring and hardening their systems, and Atlanta, who at various points either paid the ransom or ignored the threat.[6,7,8,9] They could even sell intellectual property, such as research conducted by US companies that is then sold to (typically, foreign) competitor, a significant cybercrime that costs "close to $600 billion, nearly one percent of global GDP," per year, according to the report "Economic Impact of Cybercrime – No Slowing Down" by the Center for Strategic and International Studies (CSIS), in partnership with McAfee.[10] Hackers may also steal data for personal reasons, such as political motivation, ideology, or hacktivism, or to simply show off their skills.[11]

[4] https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/
[5] https://docs.broadcom.com/doc/istr-24-2019-en
[6] https://www.nj.com/essex/2018/11/iranian_hackers_hijacked_newark_city_computers_fed.html
[7] https://www.baltimoresun.com/politics/bs-md-ci-data-lost-20190911-i6feniyk5nd3pereznpdxwsf7a-story.html
[8] https://www.citylab.com/life/2019/10/cyber-security-cities-atlanta-cyberattack-ransomware-data/600982/
[9] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/
[10] https://www.csis.org/analysis/economic-impact-cybercrime
[11] https://blog.trezor.io/trezor-data-privacy-series-why-do-hackers-hack-and-what-happens-to-your-stolen-data-60d93bf351a4

The potential impact severity of data breaches means that there is now a robust market for data breach insurance within the broader context of cybersecurity insurance.[12] Many insurance providers, including AXA, AIG, Beazley, Zurich, Chubb, and Hartford, offer robust cybersecurity insurance policies that will cover data breaches, and offer policyholders specific resources to address breaches, restore service, conduct forensics, and cover potential losses.[13,14] Cybersecurity (and thus, data breach) insurance is not covered by other types of insurance, and must be purchased as a separate policy.

However, even if companies can procure data breach insurance and harden their systems with layers of protection, these data breaches harm consumer privacy and could be considered an externality if companies do not pay for sufficient data security while much of the a data breach's costs are borne by consumers and governments. Stolen data can end up in the hands of various bad actors, and lead to years of essentially disaster management for consumers who must monitor their credit, various bank and credit card accounts, and other personal and financial data to ensure that these are not being used to steal or profit from them.

To better understand the impact of data breaches on the performance of globally traded company stocks, an event study can be conducted using the timing of the announcement of large-scale data breaches for companies whose stocks are publicly traded. This author's hypothesis is that stock prices generally sustain a minor negative impact due to the occurrence of data breaches, but this may vary due to the severity of the data breach, the potential regulatory

[12] https://www.todaysgeneralcounsel.com/find-the-right-cyber-insurance-policy/
[13] https://axaxl.com/insurance/products/cyber-insurance
[14] https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyber-north-america/cyber-and-tech-product-sheet_axa-xl_us.pdf

impacts on the company, the industry in which the company plays, the centrality of the affected business(es) to the company's long-term economic health, and whether investors even care about the data breach with respect to the company. Overall, the stock price change is likely driven by three potential impact groups:

1. Shareholders punish companies for data breaches, since these data breaches represent:
    a. Potential future loss of consumer confidence leading to lower revenues/profits
    b. Lack of investment in IT and data security
2. Fines are levied against the company
    a. These were relatively light in the past, but with regulators in the European Union (relying on the General Data Protection Regulation (GDPR)) and the United States cracking down on data breaches, heavier fines are being levied on companies
3. Class action lawsuits
    a. Brought against companies with data breaches, these are driven by lawyers (primarily) or ordinary citizens who are suing companies for material harm due to personal data that is lost in a data breach

However, even with these impacts, the author believes that the punishment on companies is relatively light compared to the destructive potential of so much stolen personal data. This is in line with some commentators, who believe that investors may not care about the impact of data breaches on corporate performance.[15] In this analysis, the null hypothesis to be tested is that there is no reduction in the stock price due to a data breach announcement, with the alternative

[15] https://www.bloomberg.com/news/articles/2014-05-23/investors-couldnt-care-less-about-data-breaches

hypothesis is that there is some stock price decrease due to a data breach announcement. This simplifies the reality a bit, since there are some key costs that could be expected to arise in most data breaches, including breach assessment, mitigation, new cybersecurity investments to prevent in the future, and fines.

II. PREVIOUS WORK

II.1 Anecdotal

When massive data breaches occur with significant personally identifiable information (PII) stolen by hackers, news reporting will highlight the actual and potential impact of the data breach on stock prices. While these are usually one or two sentence notes in articles that detail the wider impact on consumers, they give a window into what news organizations expect the general public to be interested in with regards to company financial performance. For example, after the Capital One data breach referenced in the introduction, the Financial Times stated in their article on the breach that "The bank's shares fell more than 4 per cent in after-hours trading on the news to $93."[16] Similarly, Yahoo Finance's reporting on Macy's data breach reported in November 2019 included a note that "Macy's stock traded down about 10% to $15.18 per share at time of publication."[17] Education firm Chegg announced a massive data breach of over 40,000,000 exposed records in September 2018; CNBC reported that "Chegg plunged more than

[16] https://www.ft.com/content/7c6c6d7a-b269-11e9-8cb2-799a3a8cf37b
[17] https://finance.yahoo.com/news/macys-acknowledges-data-breach-stock-180858311.html

12 percent Wednesday after disclosing a data breach that could affect customers' user information."[18]

While news reporting will usually avoid mentioning stock price movement if the price does not move appreciably, the fact that many data breaches do include some information regarding stock prices changes points to at least anecdotal evidence that data breaches result in some immediate (if possibly temporary) reduction in value.

II.2 Academic research specific to general IT use and news

There are two clear schools of thought on the impact of IT news on stock price performance: those who think it matters and those who do not think it matters (the IT paradox theory). In the latter camp, Lee and Connolly (2009), in their study "The impact of IT news on hospitality firm value using cumulative abnormal returns (CARs)", find that there is very little impact of IT news on hospitality firm value.

However, other researchers and commentators believe the opposite. Aral, Brynjolfsson, and Van Alstyne (2007) find that "IT use is positively correlated with non-linear drivers of productivity." Byrd, Lewis, and Bryan (2005) write that "that there is a synergistic coupling between strategic alignment and IT investment with firm performance". Nicolas G. Carr, in his article "IT Doesn't Matter" from the May 2003 issue of Harvard Business Review, argued that IT's ubiquity meant that it became a commodity and did not provide a competitive advantage.[19]

[18] https://www.cnbc.com/2018/09/26/ed-tech-company-chegg-plunges-after-disclosing-data-breach.html
[19] https://hbr.org/2003/05/it-doesnt-matter

However, the risks associated with IT were much greater than the potential benefits to IT differentiation.

II.3 Academic research specific to data breaches

Here, we find a distinct lack of research conducted on the impact of data breaches on stock prices. However, the Wharton Research Data Services (WRDS) organization at The Wharton School, University of Pennsylvania conducted an analysis on data breaches as a teaching opportunity regarding event studies.[20] In this, a group of 11 data breaches from 2007 to 2017 were analyzed for impact on stock returns, using abnormal returns and cumulative abnormal returns (similar to the methodology for this research paper). In the WRDS event study, data breaches were shown to have a negative impact on stock price performance, with cumulative abnormal returns (CARs) dropping "by about 5%" on average.[21] However, with a limited sample size and a much longer time frame, this research paper's analysis intends to dive further into the impact of data breaches on stock price performance, with an emphasis on more recent breaches.

III. DATA SELECTION

III.1 Sample Selection

Data breaches occur before, sometimes well before, the public announcement of the breach. Some organizations want to ensure data safety and become a target for hackers, others

[20] https://wrds-www.wharton.upenn.edu/documents/244/investments-event-study-slide-deck.pptx
[21] https://wrds-www.wharton.upenn.edu/documents/244/investments-event-study-slide-deck.pptx

are worried about public reputation or do not find out until a research alerts them to the data breach. Nonetheless, nearly all data breaches have a lag between the actual breach and the public announcement of the breach. Prior to the public announcement, it is considered private information. As private information, the data breach is not reflected in the stock price. It is only after the data breach occurrence is announced and becomes news that it is priced in. Since the timeline of the breach can be vague, even after it has been thoroughly researched, and knowledge of the breach is only widely known at the time of public announcement, this analysis identifies the announcement date as the event date (t=0) for determining whether there is stock price movement due to the data breach.

In order to gather the sample of data breaches that could be used to conduct this analysis, data breach lists were gathered from public sources. While many of these are quite accessible and free for use and review, there are no complete, "one-stop shops" for data breaches and much manual collation is required across the various data sources.

Many news sources provide details regarding these data breaches. The New York Times and Financial Times, for example, provide a great amount of supporting information regarding the largest and most prominent data breaches. In recent years, with journalists wielding greater data and technology expertise, these news sources are becoming increasingly powerful tools for understanding the scope and root causes of data breaches. Technology security companies and bloggers, such as Krebs on Security, provide even greater details on data breaches, both large and small, that may not be highlighted by more general news organizations, while websites like Have I Been Pwned can help consumers identify whether their email addresses or account

information has been compromised in various hacks, though most of these lists are nowhere near exhaustive.[22,23]

Data breach lists on the internet are widely found, especially at year end when top 10 lists of the largest data breaches of the year proliferate. While these are attention grabbers, they do not give a wide view of all data breaches that occurred during the year, especially those that are still large but do not meet a high enough record threshold (usually in the hundreds of thousands or millions) to be part of these types of lists. Websites like Business Insider, which routinely aggregate these types of events into informative listings (some would call these "clickbait"), can help with data gathering, especially for companies in the United States. As a result, many data breaches were captured from year-end lists from these news agencies and aggregators. For example, Business Insider's list of largest data breaches in 2018 helped identify eight large data breaches that could be part of the analysis.[24] For 2019, internet security provider Norton and media websites like CNET provided additional data breaches for analysis.[25,26]

In addition, many privacy and consumer advocacy groups have also begun to gather and provide much longer lists of data breaches to highlight the extraordinary scope of this data protection issue. Thales eSecurity, a data security solutions and services company, releases an annual data threat report that highlights major data breaches, summarizes their impact, and captures the upcoming outlook for data security from industry practitioners.[27] Wikipedia has a list of large data breaches, crowded-sourced from various news agencies.[28] Most helpfully, the

[22] https://krebsonsecurity.com/
[23] https://haveibeenpwned.com/
[24] https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#1-aadhar-11-billion-21
[25] https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html
[26] https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/
[27] https://www.thalesesecurity.com/2019/data-threat-report
[28] https://en.wikipedia.org/wiki/List_of_data_breaches

Identity Theft Resource Center (ITRC) also releases an annual report that also describes various data breaches, with a focus on breaches that affect American consumers and a breadth that reaches over 1,000 breaches per year.[29]

Ultimately, the ITRC reports were the basis of the data breaches examined in this analysis. Using the 2015-2019 reports, a list of all breaches that had above 20,000 data records exposed was collated. Companies identified from these reports were then identified as publicly traded (or not). Added to this list were large data breaches identified in the above listed sources without mention in the ITRC reports, including one in 2020. A summary table of selected breaches and the number of breaches at each step of the funnel is displayed below:

Year	Total Breaches listed	Breaches with over 20,000 records	Public Company	+ Additional Public Data Breaches Identified	= Total
2015	780	55	14	2	**16**
2016	1,093	85	12	1	**13**
2017	1,579	98	13	3	**16**
2018	1,257	118	22	3	**25**
2019	1,473	161	15	6	**21**
2020				1	**1**
Total	**6,182**	**517**	**76**	**16**	**92**

For the complete list of data breaches collected for this analysis, please refer to section VIII.1 List of Data Breaches.

[29] https://www.idtheftcenter.org/2019-data-breaches/

III.2 Data Collection

Many sources were used to gather the information necessary to complete this research paper. These included:

- Stock Prices were gathered from the Wharton Research Data Services
    - US company stock prices were gathered from the Compustat – Capital IQ / North America – Daily / Security – Daily database[30]
    - Ex-US company stock prices were gathered from the Compustat – Capital IQ / Global – Daily / Compustat Global - Security Daily database[31]
- S&P 500, NASDAQ, 10-year bond rates, 3-month T-bill rates were gathered from SAP Capital IQ[32]

From all these data sources, data from January 1, 2014 to April 5, 2020 was gathered to allow for a maximum of data availability.

IV. METHODOLOGY

As described earlier, data breaches typically occur months before companies announce them publicly. Though the data safety issue is resolved prior to the announcement, this paper will use the date of the company's announcement as the trigger event for the decline in stock price.

Since knowledge of a data breach may move from fully private to semi-public prior to a public announcement, the pre-data breach announcement stock performance will be measured in

[30] https://wrds-web.wharton.upenn.edu/wrds/ds/compd/secd/index.cfm?navId=83
[31] https://wrds-web.wharton.upenn.edu/wrds/ds/compd/g_secd/index.cfm?navId=73
[32] https://www.capitaliq.com/

a “pre-contamination” period to avoid any potential impact from an information leak and subsequent trading that could lower the stock price prior to the public announcement. In both analyses to be completed, the contamination period will be considered the 30 days prior to the public data breach announcement. The impact on stock price is expected to be felt in the days and weeks after the data breach announcement. To measure the impact, this paper will look at stock performance 10 days after the data breach announcement; far enough from the announcement date to have the effect fully reflected in the stock price, but not so far out that new information overwhelms the effect of the data breach on the stock price.

In order to estimate the impact of data breaches on stock market performance, two separate analyses will be conducted to create a holistic view of the potential impact of these events. These will be an inductive research approach that will look at individual cases to attempt to identify a generalized pattern of the impact of data breaches, and a yield-based analysis using a Fama-French CAPM model to estimate the cumulative asset returns (CARs) lost due to data breaches.

IV.1 Stock price prediction

The inductive approach is based on regression models aiming to predict daily stock prices prior to the contamination period using various metrics, such as the S&P 500 index, the NASDAQ index, and long- and short-term interest rates. This full version of this formula is:

$$P_{i,t} = \alpha_i + \beta_1 S\&P500_t + \beta_2 NASDAQ_t + \beta_3 10yr\ Bond\ Yield_t + \beta_4 3mo\ TBill\ Yield_t + \varepsilon_{i,t}$$

, where $P_{i,t}$ is the price of security i at time t, α_i is the abnormal return, and the β values are estimated “impacts” of each financial metric on the stock price. For each company, a regression equation will contain anywhere from one to four of these metrics, depending on best fit and

simplicity. A subset of the four metrics will be used so that overfitting is avoided. To determine the best fit without overfitting, all possible combinations of predictors are run as a regression, and the model with the lowest Mallow's Cp will be selected.[33]

Using a data range of t-90 to t-30, regression models were built to attempt to predict those daily stock prices. Based on the above criteria, the estimated betas from the regression can be applied to the post-event period predictor variables to calculate a predicted stock price based on t-90 to t-30 day information. The difference between the predicted stock price and the actual stock price at t+10 days is the estimated total impact of the data breach on the stock price. This, of course, assumes that the company's fundamentals do not appreciably change in the 30-day contamination period. There are also potential fine and class action lawsuit impacts to stock price, which are expected to be built into the post-event stock price.

IV.1 Stock return prediction

The second approach uses cumulative abnormal returns (CARs) calculated from the difference in excess returns expected based on past performance and actual returns. In order to predict CARs, a Fama-French CAPM model will be generated for each stock and used to calculate expected stock returns. These expected stock returns will be compared to actual stock returns by calculating abnormal returns (ARs; actual stock return – expected stock return), which will then be aggregated into CARs.

For this second approach, the Fama-French CAPM model will be used:

[33] Gilmour, Steven G. "The interpretation of Mallows's C_p-statistic." Journal of the Royal Statistical Society. Series D (The Statistician), vol. 45, no. 1, 1996, pp. 49–56. JSTOR, www.jstor.org/stable/2348411. Accessed 15 Apr. 2020.

$$\hat{R}_{i,t} = \alpha_i + \hat{\beta}_i(R_m - R_f) + \varepsilon_{i,t}$$

, based on a similar event study conducted by MacKinlay in 1997.[34] This is the basic Fama-French model, where $\hat{R}_{i,t}$ is the estimated return on stock i at time t, α_i is the abnormal return on stock i (or "alpha"), $\hat{\beta}_i$ is the correlation between the estimated return on stock i at time t and the daily market return (or "beta"), R_m is the daily market return, R_f is the daily risk-free rate (in this case, the 10-year US Treasury bond yield), and $\varepsilon_{i,t}$ is the error term for the predicted stock price, normally distributed around 0 with an estimated error of σ^2. All returns in the above formula are calculated by using the formula:

$$\log(price_t - price_{t-1})$$

, where the natural logarithm is used.

These models will be used to calculate daily ARs, as well as CARs based on the actual and predicted returns. Since there may be evidence of leakage of news prior to an event, the CARs will be aggregated in a t-10 to t+10 period, with t-0 equal to the data breach announcement date. These CARs will also be estimated in the t-0 to t+10 day period (which assumes that there is no news leakage). The CARs would represent the total effect of the data breach on stock performance. As in the earlier approach, the stock price immediately after t=0 should incorporate the market's best guess of both the fine effect and class action lawsuit judgment effect that a firm will face.

[34] MacKinlay, "Event Studies in Economics and Finance"

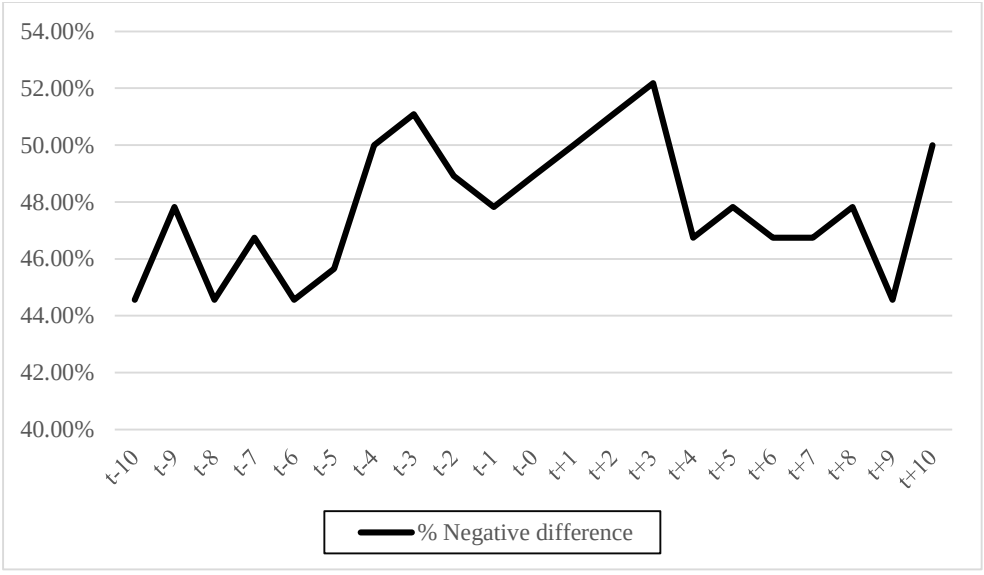
V. RESULTS

V.1 Stock Price Prediction

The results from the stock price prediction analysis point to a lack of impact of data breaches for daily price predictions. In almost every case analyzed, the ability of the t-90 to t-30 regression models to predict stock price in the post-announcement period (t+0 to t+10) is strong, with 70 out of 92 stock price prediction models having R^2 above 50%. The number of companies with a negative difference between the actual stock price and predicted stock price per day is shown in the charts and graph below:

	t-10	t-9	t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1	t-0
Positive difference	51	48	51	49	51	50	46	45	47	48	47
Negative difference	41	44	41	43	41	42	46	47	45	44	45
% Negative difference	44.57%	47.83%	44.57%	46.74%	44.57%	45.65%	50.00%	51.09%	48.91%	47.83%	48.91%

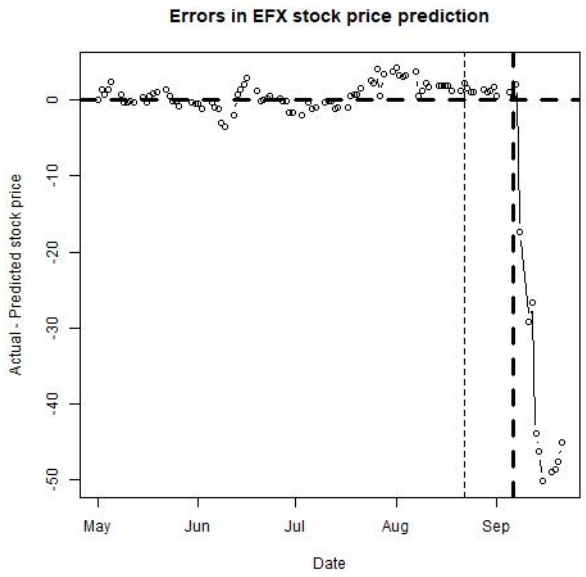
	t-0	t+1	t+2	t+3	t+4	t+5	t+6	t+7	t+8	t+9	t+10
Positive difference	47	46	45	44	49	48	49	49	48	51	46
Negative difference	45	46	47	48	43	44	43	43	44	41	46
% Negative difference	48.91%	50.00%	51.09%	52.17%	46.74%	47.83%	46.74%	46.74%	47.83%	44.57%	50.00%



Based on this, stocks tend to be priced right around where predictors based on t-90 to t-30 performance would have expected them to be in the t-10 to t+10 timeline.

V.2 Specific data breach examples using stock price prediction models

Some of the most egregious and prominent data breaches do have significant price drops compared to the expected price based on their t-90 to t-30 stock price model. One example is of the Equifax data breach, which was announced on September 7, 2017 and exposed over the personally identifiable information of over 150,000,000 people.[35] In this case, Equifax was eventually required by federal and state authorities, including the "Federal Trade Commission, Consumer Financial Protection Bureau, 50 state attorneys-general, and class-action claimants," to pay almost $800 million to various funds and penalties.[36] In this case, the stock price fell dramatically compared to expectations once the data breach was announced:

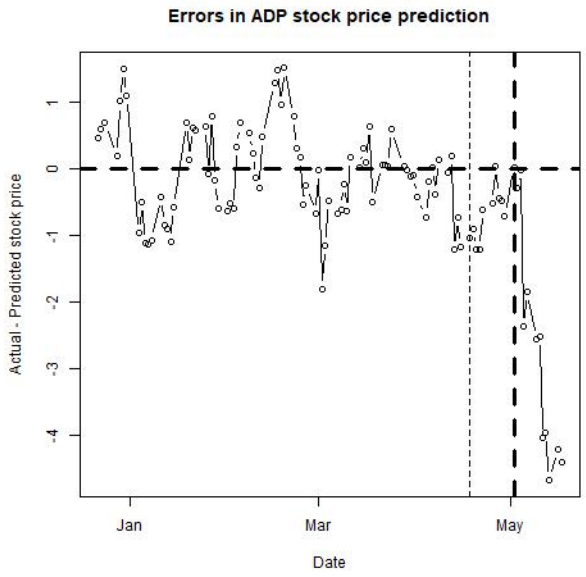


(Note: the heavy dashed line is the t-0 date; the light dashed line is the t-10 date. This is true of the remaining graphs in this paper.)

[35] https://www.ft.com/content/dd98b94e-ac62-11e9-8030-530adfa879c2
[36] Ibid.

On the day after the breach announcement, Equifax's actual stock price was $17.39 (12.39%) below the predicted price and continued to decline against the prediction in the rest of the t+2 to t+10 timeline. This was primarily driven by the stock price dropping over 30% in the t-0 to t+10 timeline and a rising S&P 500, which was the heaviest component of the Equifax price prediction model (74% R^2).

Another example of a company whose stock price did not live up to prediction after a data breach announcement is ADP, who announced their own data breach on May 3, 2016. While the number of records was not made clear, as the payroll, tax, and benefits administrator for over 640,000 companies, any data breach would necessarily be considered a serious issue.[37,38] In this case, the stock price also dropped dramatically upon announcement:



In this case, the actual stock price of $85.35 was $4.39 (5.15%) below the predicted price by t+10. As in the Equifax case, the price dropped almost immediately due to the data breach and

[37] https://krebsonsecurity.com/2016/05/fraudsters-steal-tax-salary-data-from-adp/
[38] https://www.infosecurity-magazine.com/news/adp-w2-breach-a-perfect-example-of/

stayed down. The stock price itself declined $3.46 (3.90%) in the t-0 to t+10 timeframe, but the model (94% R^2) expected the price to stay relatively flat over those 10 days

V.3 Stock Return Prediction using the Fama-French CAPM model

While some stocks suffer from a data breach, many simply do not have an appreciable difference in stock performance. Daily abnormal returns in the t-10 to t+10 range are the following:

	t-10	t-9	t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1	t-0
Positive AR	44	46	46	51	47	45	46	44	46	40	43
Negative AR	48	46	46	41	45	47	46	48	46	52	49
% Negative AR	52.17%	50.00%	50.00%	44.57%	48.91%	51.09%	50.00%	52.17%	50.00%	56.52%	53.26%
Mean AR	-0.13%	0.06%	0.06%	0.07%	0.05%	-0.03%	0.13%	-0.20%	-0.01%	-0.44%	0.02%
Standard Deviation	2.22%	1.80%	1.27%	1.47%	1.60%	1.59%	2.06%	2.05%	1.65%	2.21%	1.70%
Mean AR + 1.96 SD	4.22%	3.60%	2.55%	2.95%	3.18%	3.09%	4.17%	3.82%	3.22%	3.89%	3.35%
Mean AR - 1.96 SD	-4.47%	-3.48%	-2.43%	-2.80%	-3.09%	-3.15%	-3.91%	-4.22%	-3.25%	-4.77%	-3.32%

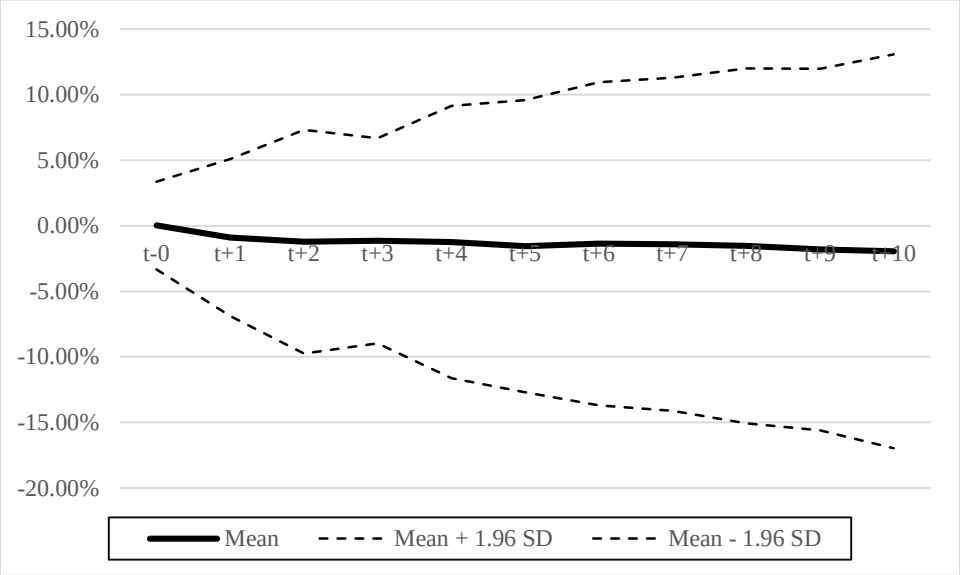
	t-0	t+1	t+2	t+3	t+4	t+5	t+6	t+7	t+8	t+9	t+10
Positive AR	43	40	43	46	50	39	48	46	43	45	42
Negative AR	49	52	49	46	42	53	44	46	49	47	50
% Negative AR	53.26%	56.52%	53.26%	50.00%	45.65%	57.61%	47.83%	50.00%	53.26%	51.09%	54.35%
Mean AR	0.02%	-0.92%	-0.32%	0.08%	-0.09%	-0.32%	0.19%	-0.05%	-0.12%	-0.27%	-0.15%
Standard Deviation	1.70%	2.90%	2.36%	2.12%	2.23%	1.63%	1.99%	1.76%	1.78%	1.77%	2.02%
Mean AR + 1.96 SD	3.35%	4.76%	4.31%	4.23%	4.27%	2.87%	4.10%	3.40%	3.37%	3.21%	3.82%
Mean AR - 1.96 SD	-3.32%	-6.60%	-4.95%	-4.08%	-4.45%	-3.51%	-3.72%	-3.49%	-3.62%	-3.74%	-4.11%

On the day of the breach, only 53% of stocks have a negative abnormal return (AR) compared to the expected return based on CAPM. While this percentage increases on t+1 (56.52% negative AR), it falls on t+2 to t+4. Stocks on average only have slightly below average performance. The average abnormal return is never below -1%, while days t+0, t+3, and t+6 have positive average abnormal return (!).

Abnormal returns in the t-10 to t-0 period, do not seem surprising in either, with average AR close to 0% on most days. However, t-1 does have an average AR of -0.44% and 56.52% of stocks with negative AR, which may be a sign of some pre-announcement news leakage for a select number of stocks.

However, it will be more appropriate to study the cumulative abnormal returns to test whether the stock sustains a negative impact due to the data breach. Here are the CARs starting with the announcement date (t-0):

	t-0	t+1	t+2	t+3	t+4	t+5	t+6	t+7	t+8	t+9	t+10
Positive CAR	43	37	38	38	41	39	40	42	44	43	44
Negative CAR	49	55	54	54	51	53	52	50	48	49	48
% Negative CAR	53.26%	59.78%	58.70%	58.70%	55.43%	57.61%	56.52%	54.35%	52.17%	53.26%	52.17%
Mean	0.02%	-0.90%	-1.22%	-1.15%	-1.24%	-1.56%	-1.37%	-1.41%	-1.54%	-1.81%	-1.96%
Standard Deviation	1.70%	3.06%	4.35%	3.99%	5.29%	5.69%	6.29%	6.48%	6.91%	7.03%	7.66%
Mean + 1.96 SD	3.35%	5.09%	7.30%	6.67%	9.14%	9.59%	10.96%	11.29%	12.00%	11.98%	13.06%
Mean - 1.96 SD	-3.32%	-6.89%	-9.75%	-8.96%	-11.62%	-12.70%	-13.69%	-14.12%	-15.07%	-15.59%	-16.97%



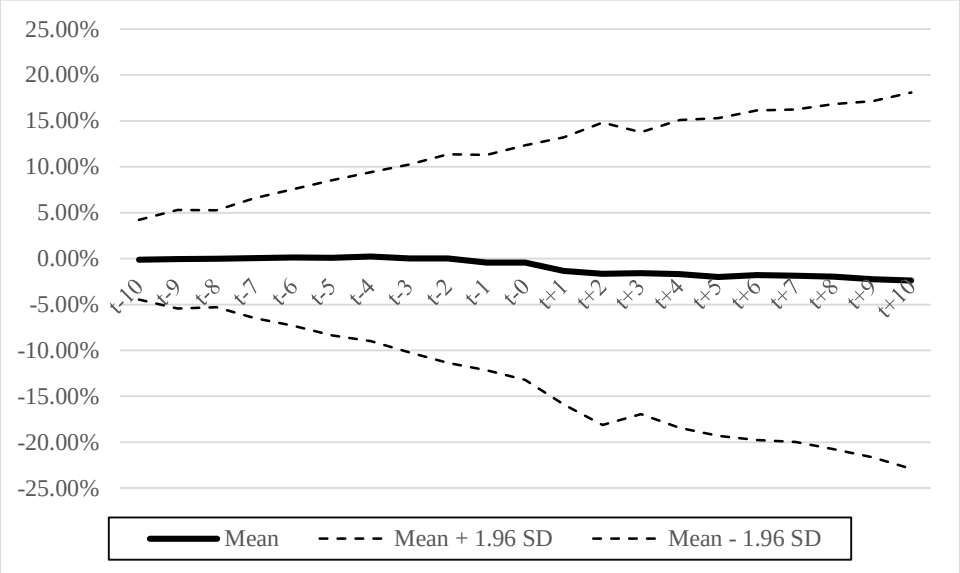
Again, there are more stocks with negative CAR on t=0 (as to be expected with AR at t=0 discussed above) and the mean CAR is slightly positive. Beginning with day t+1, the average CARs remains negative, and trends further negative. However, the CAR at t+10 is -1.96%,

which is not a large difference. More concerning, the entire timeline shows the two standard deviation interval around the average CAR to include 0%, which suggests that the finding is not very strong.

If the CAR window is extended to t-10 to t+10, the following results are generated:

	t-10	t-9	t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1	t-0
Positive CAR	44	46	48	43	44	48	53	51	45	40	40
Negative CAR	48	46	44	49	48	44	39	41	47	52	52
% Negative CAR	52.17%	50.00%	47.83%	53.26%	52.17%	47.83%	42.39%	44.57%	51.09%	56.52%	56.52%
Mean	-0.13%	-0.07%	-0.01%	0.07%	0.11%	0.09%	0.22%	0.02%	0.00%	-0.44%	-0.42%
Standard Deviation	2.22%	2.75%	2.70%	3.33%	3.79%	4.31%	4.70%	5.22%	5.80%	5.98%	6.52%
Mean + 1.96 SD	4.22%	5.32%	5.28%	6.60%	7.55%	8.54%	9.42%	10.25%	11.37%	11.29%	12.36%
Mean - 1.96 SD	-4.47%	-5.45%	-5.29%	-6.46%	-7.32%	-8.36%	-8.98%	-10.21%	-11.36%	-12.16%	-13.20%

	t-0	t+1	t+2	t+3	t+4	t+5	t+6	t+7	t+8	t+9	t+10
Positive CAR	40	34	37	40	41	40	37	38	38	36	37
Negative CAR	52	58	55	52	51	52	55	54	54	56	55
% Negative CAR	56.52%	63.04%	59.78%	56.52%	55.43%	56.52%	59.78%	58.70%	58.70%	60.87%	59.78%
Mean	-0.42%	-1.34%	-1.66%	-1.58%	-1.68%	-1.99%	-1.80%	-1.85%	-1.98%	-2.24%	-2.39%
Standard Deviation	6.52%	7.43%	8.40%	7.84%	8.56%	8.83%	9.16%	9.24%	9.59%	9.90%	10.46%
Mean + 1.96 SD	12.36%	13.21%	14.81%	13.79%	15.09%	15.32%	16.14%	16.25%	16.83%	17.16%	18.10%
Mean - 1.96 SD	-13.20%	-15.89%	-18.12%	-16.95%	-18.44%	-19.31%	-19.75%	-19.95%	-20.78%	-21.65%	-22.89%



With some stocks exhibiting a significant drop on t-1 (as seen in the abnormal returns chart), ~60% of stocks have negative CARs after the event date, and by t+10, companies with

data breaches average -2.39% CAR. This is a stronger result that seen in the t-0 to t+10 timeline and indicates that there is some evidence of a negative impact due to data breaches. However, the 2 standard deviation cone is even wider here that in the previous timeline review.

V.4 Specific data breach examples using the Fama-French CAPM model

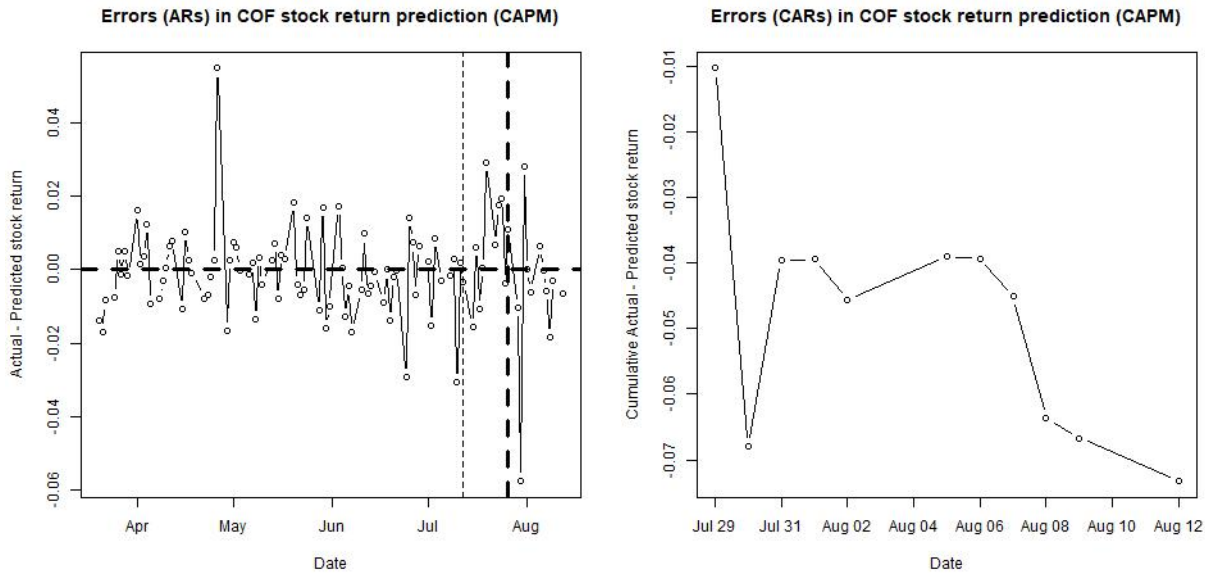
Some companies in the dataset suffered particularly egregious data breaches and should be highlighted separately.

V.4.i. Capital One (NYSE:COF)

Capital One, as highlighted in the introduction, reveals on July 29, 2019 that it had 106 million records containing personally identifiable information stolen.[39] Due to the actions of a single former Amazon Web Services employee, "names, addresses and phone numbers, self-reported income, credit scores and payment history, among other personal information" were lifted from applications for Capital One products. While much finger-pointing between Capital One and Amazon Web Services occurred in week after the data breach, there is no question that this was hugely damaging to American and Canadian citizens.

Reviewing the abnormal returns for the period t-90 to t+10 and the cumulative abnormal returns for the period t-0 to t+10 can help reveal what the market thought of the impact of the breach on Capital One:

[39] https://www.ft.com/content/7c6c6d7a-b269-11e9-8cb2-799a3a8cf37b



(Note: the heavy dashed line is the t-0 date; the light dashed line is the t-10 date. This is true of the remaining graphs in this paper.)

By the tenth day after the data breach announcement, Capital One had a -7.325% CAR over those ten days, signifying a huge expected impact on Capital One. In its news release regarding the data breach, Capital One expected to incur costs of "$100 to $150 million in 2019" due to the event.[40] However, the company also had insurance for cyber risk events with a coverage limit of $400 million after a $10 million deductible, so the company may ultimately suffer much less of an impact than would otherwise have been expected.

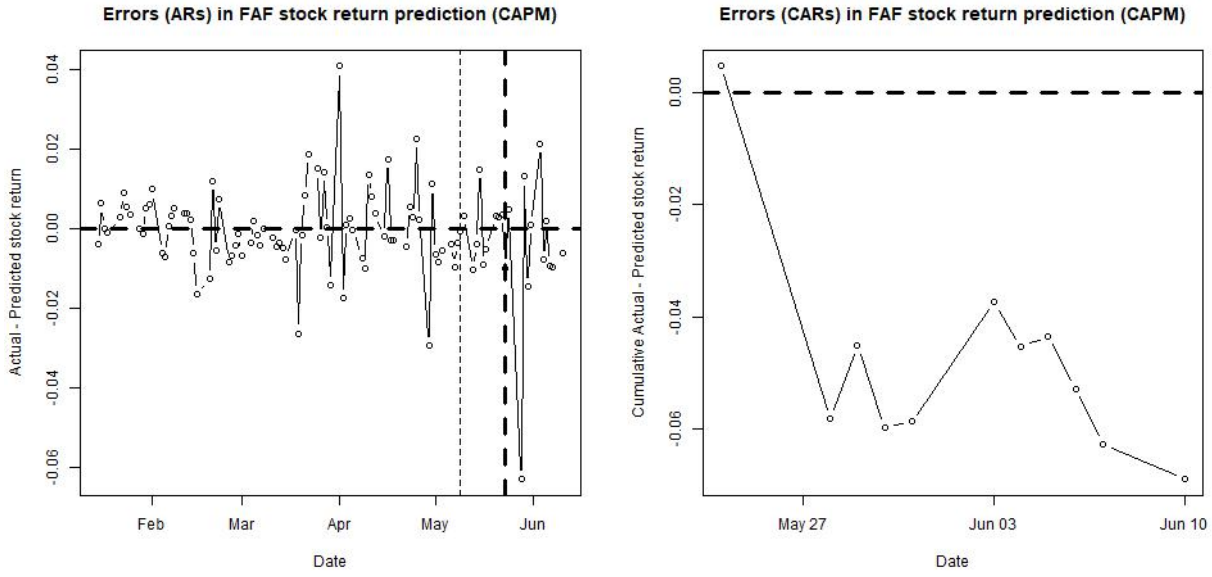
V.4.ii. First American Financial Corporation (NYSE:FAF)

First American, "one of the most widely-used companies for real estate title insurance and for closing real estate deals," exposed up to 885,000,000 records over a web browser without

[40] https://www.prnewswire.com/news-releases/capital-one-announces-data-security-incident-300892738.html

requiring authentication.[41] The data involved included "bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers license images," and though the firm was alerted to this by at least one real estate broker, it required the attention of a top information security writer, Brian Krebs, to gain their attention to the glaring hole in their security. The data breach was announced on May 24, 2019.

Again, it is best to review the abnormal returns from t-90 to t+10 and the cumulative abnormal returns for t-0 to t+10:

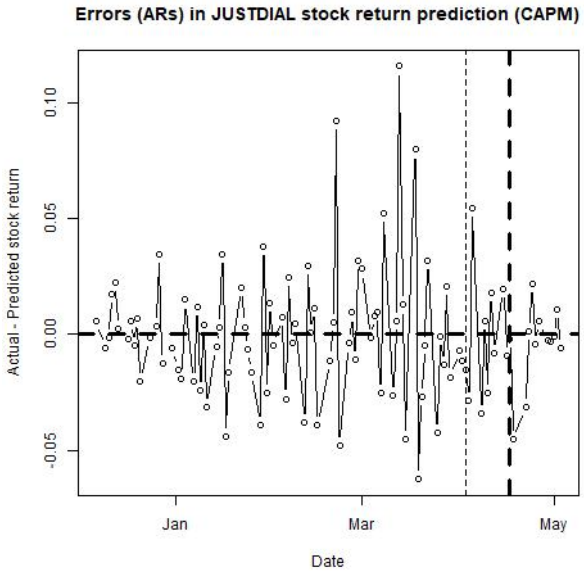


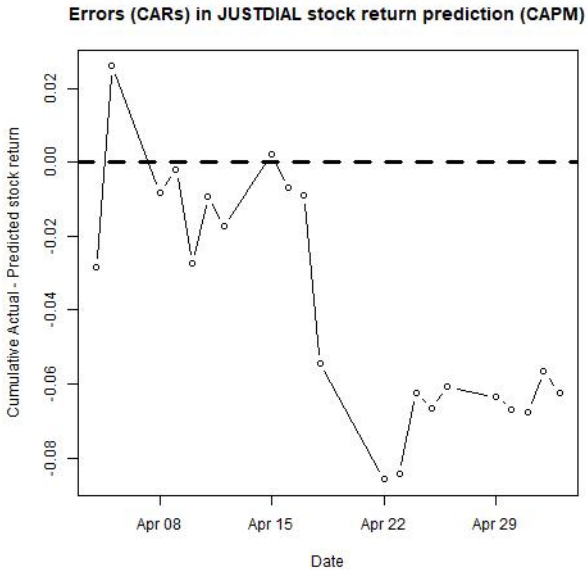
Again, we can see a significant impact on First American's stock price, with a -6.897% CAR in the ten days following the data breach. Nearly the entire impact occurred by the end of trading the day after the announcement, with minor adjustments afterwards.

[41] https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

V.4.iii. Just Dial Limited (NSEI:JUSTDIAL)

Looking outside of the United States, Justdial is an Indian company that offers local search for a variety of services throughout India, over the phone and online. Security researcher Rajshekhar Rajaharia found that four of its application programming interface (APIs), which defines how other systems can access Justdial's data, made personally identifiable information of over 100 million users available.[42] A quick review of the ARs over the full timeline and the CARs over the t-10 to t+10 timeline will show the impact of the data breach on Justdial's stock:



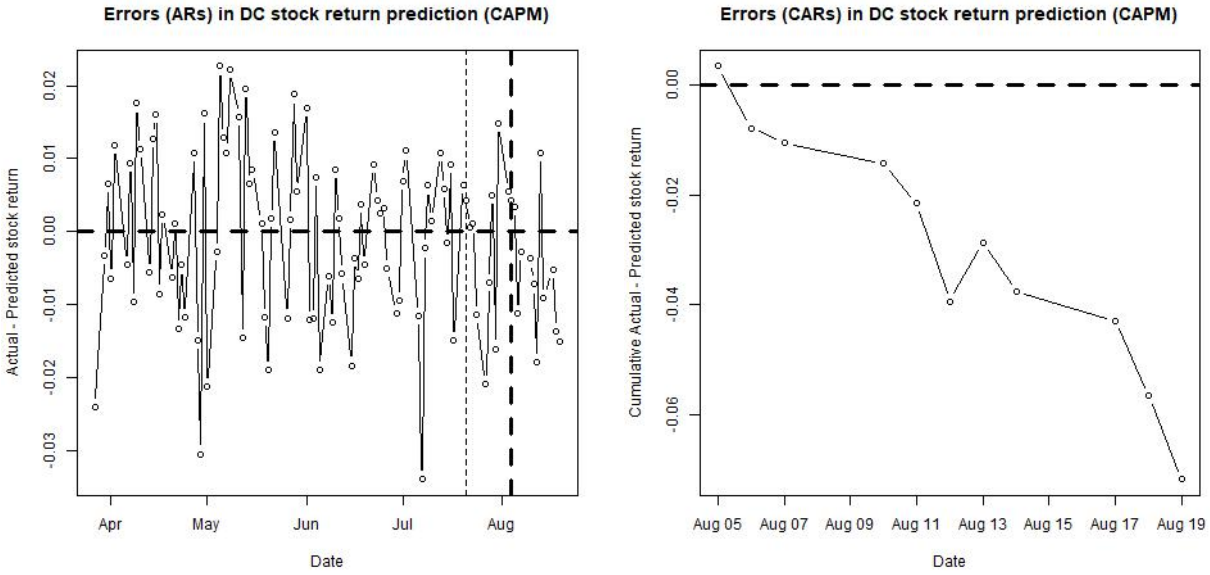


While the stock has significant spikes in the AR graph, the impact of the data breach announcement is immediate, with a 4.5% drop on t=0. In the t-10 to t+10 timeline, the stock has a -6.247% CAR. While this episode may have been expected to lead Just Dial to improve their information security measures, another security researcher, Ehraz Ahmed, discovered a similar flaw in Justdial's Register API that also made over 100 million users' data accessible online.

[42] https://economictimes.indiatimes.com/tech/internet/data-breach-at-justdial-leaks-100-million-user-details/articleshow/68930607.cms

V.4.iv. Dixons Carphone plc (LSE:DC.)

Dixons Carphone plc, a mobile phone carrier based in the United Kingdom and with a presence in other parts of Europe, announced a large data breach affecting more 3,000,000 customers on August 5, 2015 (initial estimates were about 2,400,000 customers).[43,44] While "only" 18,000 customers had "historical payment card details" stolen, "intruders were able to access personal information including the names, addresses, phone numbers, dates of birth, marital status".[45] The severity of the data breach can be seen in the AR and CAR graphs below:



Dixons Carphone ultimately suffered a -7.174% CAR in the t-0 to t+10 timeline. The company was also hit with a £400,000 fine by the United Kingdom's Information Commissioner's Office, a record (tie) at the time of fining in January 2018.[46]

[43] https://www.bbc.com/news/uk-33835185
[44] https://www.ft.com/content/baa7e2d0-82fb-3363-8d3b-170425b8043a
[45] Ibid.
[46] Ibid.

V.5 Summary

Both the stock price and stock return prediction methodologies suggest there is little evidence to reject the null hypothesis of no impact on the stock price due to a data breach announcement in most cases. The stock price prediction analysis sees the sample set of companies at t+10 split evenly between having stock prices above and below the predicted value, suggesting minimal to no impact on stock price due to data breaches.

The stock return prediction analysis shows an average of -1.56% CAR in the t-0 to t+5 range and -1.96% CAR in the t-0 to t+10 range. However, the standard deviations for both ranges are large enough (5.69% for t-0 to t+5, 7.66% for t-0 to t+10) that the null hypothesis of mean = 0.00% is captured by the 95% confidence interval. A similar situation occurs when starting at the t-10 date in CAR calculation.

However, companies which suffer data breaches that deeply affect the core business, such as Equifax and ADP, are much more likely to experience a meaningful negative impact on their stock price due to data breaches. Since their customers, whether they are consumers or businesses, may severely curtail their commerce with them, since regulators may levy substantial fines against them, and since they themselves may be spending hundreds of millions of dollars remedying the root causes and dealing with the aftermath, these companies are more likely to be punished in the markets.

VI. REGULATIONS & SUGGESTED REMEDIES

Data breaches are a growing threat to the safety and security of both consumers and businesses. Though the public has lived with them for years, as data collection increases globally, the potential for personal damage due to breaches expands with it.

The European Union, Federal Trade Commission, and other governments and government agencies around the world are implementing new regulations and penalties for data breaches, and these should continue to be strengthened while leaving room for flexibility given the rapidly changing security environment. The General Data Protection Regulation (GDPR) allows the European Union to fine companies up to 4% of annual revenue for severe data breaches that are not reported on in a reasonable timeframe, and since May 2018, the GDPR has "led to over 160,000 data breach notifications across Europe.[47,48] The potential for severe fines is clear: British Airways, for example, faced a $229 million USD (£183 million) fine from the UK Information Commissioner's Office (ICO, the UK's Data Protection Agency) due to a data breach suffered in 2018, which would be about 1.5% to 2% of annual revenue in recent years and in line with GDPR fines for less severe infringements.[49,50,51] Given that the previous data breach fines levied by the ICO were capped to about $625,000 (£500,000), this could be the start of truly impactful government action against data breaches, possibly leading companies to being more proactive in data management and protection against breaches.

[47] https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf
[48] Corpeleijn, Frederik, 2019. "The Information Hypothesis Revisited: A Further Examination of the Performance of Targets of Failed Takeover Attempts."
https://www.stern.nyu.edu/sites/default/files/assets/documents/Corpeleijn_Glucksman%20paper_1.pdf
[49] https://www.cpomagazine.com/data-protection/british-airways-facing-record-penalty-is-this-the-beginning-of-maximum-gdpr-fines/
[50] https://www.bbc.com/news/business-48905907
[51] https://gdpr.eu/fines/

In addition, new regulations and data privacy rights are being enacted by other governments to help businesses and consumers with data protection challenges. For example, the California Consumer Privacy Act (CCPA), passed in 2018 with an enforcement date of January 1, 2020 and punishment enforcement date of July 1, 2020, allows consumers to ask for their personal data held by companies to be delivered for review or even deleted.[52] While this may not directly impact data protection and the prevention of breaches, CCPA requirements and punishments for noncompliance are severe enough to require companies to automate request processing, which means companies will be required to manage their data better, while consumers will be able to proactively protect their data and avoid the potential impact of a company's data breach. In addition, New York State passed the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") in July 2019, with data security requirements taking effect on March 21, 2020

However, two big questions remain. First, how vigilantly will these new laws be enforced? If companies see that governments are unwilling or unable to punish companies for data breaches, they will be lax in building the data protections that should be in place to prevent breaches. There is already evidence of companies that are playing the "wait-and-see" game with the many new regulations coming online. Second, many countries around the world simply do not have data breach protections in place, so when will (or even, just will) companies located in those nations be subject to regulations that punish them that suffer data breaches? DLA Piper's Data Protection Laws of the World Handbook, an extensive repository of data protection requirements from around the world, suggests that there are only 116 countries in the world that

[52] https://www.oag.ca.gov/privacy/ccpa

have data protection laws on the books.[53] With 193 member states of the United Nations, this means that only 60% of internationally recognized countries have some sort of data protection laws, a disappointingly low number.[54]

In addition, while companies are sometimes and should be punished for leaking data, there may also be insufficient punishment for those who actually commit the crime of stealing, or enable the theft of, data. A lack of resources, ability, or willpower (that determination is beyond the scope of this paper) on the part of government and private investigators to find the perpetrators of data breach crimes results in those who are stealing data to not fear criminal prosecution. This situation is akin to a hypothetical situation: person A steals person B's diary from person C's house; person C is punished but person A gets away without ever being discovered. Perhaps increased visible and tangible enforcement is required, though over policing may be more harmful than helpful (again, outside the scope of this paper).

Companies, large and small, may also spend more effort in adhering to well-known cybersecurity frameworks. Governmental agencies, such as National Institute of Standards and Technology (NIST), and non-governmental organization (NGOs), such as International Organization for Standardization (ISO), Information Systems Audit and Control Association (ISACA, creator of the Control Objectives for Information and Related Technologies (COBIT) framework), and the International Society of Automation (ISA), publish references that can help organizations mature their cybersecurity policies. Firms that do offer strong data protections should also signal that they have invested in these functions, without giving away too much information and weakening their protections to hackers in the process. For smaller organizations,

[53] https://www.dlapiperdataprotection.com/index.html?t=about&c=BA&c2=AR
[54] https://www.un.org/en/member-states/

as hackers become more sophisticated, the cost of cybersecurity may continue to increase over time, leaving them with the difficult choice of investing in their business or spending money on data security, which is not a standalone revenue-generating action.

Finally, consumers and businesses can and should punish organizations that do not offer sufficient cybersecurity protections, putting their data at risk. While a vast number of companies have suffered severe data breaches, one of the very few that has truly suffered the ultimate consequence of a data breach and folded as a result is American Medical Collection Agency (AMCA), which filed for Chapter 11 bankruptcy due to the fallout from its data breach.[55] After exposing "the personal information on nearly 20 million Americans," the parent company of AMCA was forced to fold due to the expenses related to the data breach and loss of its four largest customers. While this was an enormous price to pay for AMCA, it should be a lesson that consumers, businesses, and governments will punish companies for a lack of data security.

VII. SUGGESTIONS FOR FUTURE RESEARCH

A great continuation of this research would be to identify company sectors or groups which are particularly susceptible to negative stock performance after the disclosure of a data breach. While this analysis did identify companies like Equifax, ADP, and First American Financial Corporation as particularly hard hit after data breach announcements, stocks of companies such as Facebook and Google do not nearly fall as much when a data breach is announced, even though personal data is also core to their business. Perhaps it is financial or personally identifiable data that can be directly translated to profit, such as credit card

[55] https://www.bloomberg.com/news/articles/2019-06-17/american-medical-collection-agency-parent-files-for-bankruptcy

information, credit data, or social security numbers, that need to be exposed for investors to punish these companies.

Another extension of this research would be to better understand whether the reduced stock prices, where companies which suffer data breaches also have stock price drops, are caused by lower revenues / profits, fines / penalties from government agencies, or class action lawsuits brought by citizens or governments. This may be hard to estimate but could be done using discounted actual fines and lawsuit settlements, when made available after two to three years of winding through the courts and government reviews, and applying those values to the change in a firm's market valuation.

Finally, further research could be done into whether investor punishments of data breaches is increasing over time. With more powerful regulations and higher consumer awareness of the potential impact of data breaches, it is certainly possible that investors reflect this in their post-breach company valuations.

VIII. CONCLUSION

In this study, I analyzed the stock market's short-term response to large-scale data breaches; in this case, 92 data breaches affecting publicly traded companies from 2015-2019 (and one in 2020). These breaches ranged in size from 20,000 Air Canada mobile app records compromised during August 22-24, 2018 (announced on August 29, 2018) to 1 billion Yahoo records compromised in 2013 and reported in 2016.[56,57] The mean cumulative abnormal return

[56] https://www.cbc.ca/news/business/air-canada-mobile-app-1.4802879
[57] https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

(CAR), measure from the day of a data breach announcement to the day after a data breach is disclosed is -0.90%, rising to -1.96% 10 days after the disclosure. The largest drops in cumulative abnormal returns were measured from -13.65% 1 day after disclosure to -38.42% 10 days after disclosure. 31 of the 92 data breaches (33.70%) had a negligible CAR (between -2% and 2%) 10 days after the breach announcement, while only five had a negative CAR below -17%.

Last year, the Identity Theft Resource Center (ITRC) identified 1,473 data breaches that affected American consumers, with over 850 million records exposed.[58] While these can have sometimes devastating effects on those whose data is stolen, firms typically only experienced a small punishment, at best, in their stock price performance. Though there has been increased scrutiny on data privacy in recent years, the loud dialogue around data protection and privacy concerns appears to have much less impact on companies than would otherwise be expected.

[58] https://www.idtheftcenter.org/2019-data-breaches/

References

Aral, Sinan, Erik Brynjolfsson, Marshall W. Van Alstyne. "Information, Technology and Information Worker Productivity: Task Level Evidence." (June 2007). NBER Working Paper No. w13172. Available at SSRN: https://ssrn.com/abstract=993403

Brown, Stephen J. and Jerold B. Warner, 1984. "Using Daily Stock Returns: The Case of Event Studies." *Journal of Financial Economics*, Vol. 14 (1985), pp. 3-31.

Byrd, Terry Anthony, Bruce R. Lewis, Robert W. Bryan, 2005. "The leveraging influence of strategic alignment on IT investment: An empirical examination." *Information & Management*, Volume 43, Issue 3 (April 2006), pp. 308-321.

Carpenter, Jennifer N., Robert F. Whitelaw, and Dongchen Zou, 2020. "The A-H Premium and Implications for Global Investing in Chinese Stocks." http://people.stern.nyu.edu/jcarpen0/pdfs/A-H.pdf. Accessed 15 Apr. 2020.

Corpeleijn, Frederik, 2019. "The Information Hypothesis Revisited: A Further Examination of the Performance of Targets of Failed Takeover Attempts." https://www.stern.nyu.edu/sites/default/files/assets/documents/Corpeleijn_Glucksman%20paper_1.pdf. Accessed 15 Apr. 2020.

Gilmour, Steven G. "The Interpretation of Mallows's C_p-Statistic." *Journal of the Royal Statistical Society. Series D (The Statistician)*, vol. 45, no. 1, 1996, pp. 49–56. JSTOR, www.jstor.org/stable/2348411. Accessed 15 Apr. 2020.

Im, Kun Shin, Kevin E. Dow, Varun Grover. "Research Report: A Reexamination of IT Investment and the Market Value of the Firm—An Event Study Methodology." Information Systems Research, vol. 12, no. 1, 2001, pp. 103–117. JSTOR, www.jstor.org/stable/23011102. Accessed 16 Apr. 2020.

Karpoff, Jonathan M, D. Scott Lee, Gerald S. Martin, 2008. "The Cost to Firms of Cooking the Books." *Journal of Financial and Quantitative Analysis*, Vol. 43, No. 3 (September 2008), pp. 581-612.

Lee, Seoki, and Daniel Connolly, 2009. "The impact of IT news on hospitality firm value using cumulative abnormal returns (CARs)." *International Journal of Hospitality Management*, Vol. 29 (2010), pp. 354-362.

MacKinlay, A. Craig. 1997. "Event Studies in Economics and Finance." *Journal of Economic Literature*, Vol. 35, No. 1 (March 1997), pp. 13-39.

APPENDIX

A. List of Data Breaches

#	Company	Ticker	Industry	Announcement Date
1	MGM Resorts International	NYSE:MGM	Hotel/Gaming	February 19, 2020
2	Microsoft	NasdaqGS:MSFT	Software (System & Application)	December 29, 2019
3	Facebook	NasdaqGS:FB	Software (Entertainment)	December 14, 2019
4	Microsoft	NasdaqGS:MSFT	Software (System & Application)	December 06, 2019
5	T-Mobile US	NasdaqGS:TMUS	Telecom (Wireless)	November 23, 2019
6	Macy's	NYSE:M	Retail (General)	November 14, 2019
7	Adobe	NasdaqGS:ADBE	Software (System & Application)	October 25, 2019
8	EyeBuyDirect	ENXTPA:EL	Apparel	October 17, 2019
9	Zynga	NasdaqGS:ZNGA	Entertainment	September 12, 2019
10	Choice Hotels	NYSE:CHH	Hotel/Gaming	August 13, 2019
11	Pearson plc	LSE:PSON	Publishing & Newspapers	July 31, 2019
12	Capital One	NYSE:COF	Financial Svcs. (Non-bank & Insurance)	July 29, 2019
13	Sprint	NYSE:S	Telecom (Wireless)	July 16, 2019
14	Quest Diagnostics	NYSE:DGX	Healthcare Support Services	May 31, 2019
15	First American	NYSE:FAF	Insurance (Prop/Cas.)	May 24, 2019

16	Justdial	NSEI:JUSTDIAL	Software (Entertainment)	April 18, 2019
17	Hartford Financial Services Group	NYSE:HIG	Insurance (General)	April 12, 2019
18	Toyota Motor Corporation	TSE:7203	Auto & Truck	March 29, 2019
19	Facebook	NasdaqGS:FB	Software (Entertainment)	March 21, 2019
20	HauteLook	NYSE:JWN	Retail (General)	March 21, 2019
21	Westpac	ASX:WBC	Bank (Money Center)	February 19, 2019
22	Don Best Sports Corporation	NasdaqGS:SGMS	Hotel/Gaming	February 06, 2019
23	Alphabet (Google)	NasdaqGS:GOOG.L	Software (Entertainment)	December 10, 2018
24	Marriott International	NasdaqGS:MAR	Hotel/Gaming	December 01, 2018
25	Bankers Life	NYSE:CNO	Insurance (Life)	October 25, 2018
26	Cathay Pacific Airways	SEHK:293	Air Transport	October 24, 2018
27	Alphabet (Google)	NasdaqGS:GOOG.L	Software (Entertainment)	October 08, 2018
28	Navionics	NasdaqGS:GRMN	Electronics (Consumer & Office)	October 08, 2018
29	Facebook	NasdaqGS:FB	Software (Entertainment)	September 28, 2018
30	Chegg	NYSE:CHGG	Education	September 25, 2018
31	British Airways	LSE:IAG	Air Transport	September 06, 2018
32	Air Canada	TSX:AC	Air Transport	August 29, 2018

33	Cheddar's Scratch Kitchen	NYSE:DRI	Restaurant/Dining	August 22, 2018
34	T-Mobile US	NasdaqGS:TMUS	Telecom (Wireless)	August 20, 2018
35	Lifelock	NasdaqGS:NLOK	Software (System & Application)	July 25, 2018
36	BMO	TSX:BMO	Bank (Money Center)	May 28, 2018
37	Comcast Corporation	NasdaqGS:CMCS.A	Cable TV	May 22, 2018
38	Nuance Communications	NasdaqGS:NUAN	Software (System & Application)	May 11, 2018
39	SunTrust Banks, Inc.	NYSE:STI	Banks (Regional)	April 21, 2018
40	Inogen	NasdaqGS:INGN	Healthcare Products	April 13, 2018
41	Delta Airlines Inc	NYSE:DAL	Air Transport	April 04, 2018
42	Hudson’s Bay Company	TSX:HBC	Retail (General)	April 01, 2018
43	UnderArmour	NYSE:UAA	Apparel	March 29, 2018
44	Orbitz	NasdaqGS:EXPE	Retail (Online)	March 19, 2018
45	FedEx (Bongo)	NYSE:FDX	Transportation	February 15, 2018
46	Royal Bank of Canada	TSX:RY	Bank (Money Center)	January 26, 2018
47	Bell Canada	TSX:BCE	Telecom. Services	January 23, 2018
48	TIO Networks	NasdaqGS:PYPL	Information Services	December 01, 2017
49	Pizza Hut	NYSE:YUM	Restaurant/Dining	October 14, 2017

50	Hyatt Hotels	NYSE:H	Hotel/Gaming	October 12, 2017
51	FlexShopper, LLC	NasdaqCM:FPAY	Financial Svcs. (Non-bank & Insurance)	October 03, 2017
52	Equifax	NYSE:EFX	Business & Consumer Services	September 07, 2017
53	UniCredit SpA	BIT:UCG	Bank (Money Center)	July 26, 2017
54	Wells Fargo	NYSE:WFC	Bank (Money Center)	July 24, 2017
55	Dow Jones & Company	NasdaqGS:NWSA	Publishing & Newspapers	July 17, 2017
56	Verizon	NYSE:VZ	Telecom. Services	July 12, 2017
57	World Wrestling Entertainment, Inc. (WWE)	NYSE:WWE	Entertainment	July 07, 2017
58	Kmart / Sears Holding Company	OTCPK:SHLD.Q	Retail (General)	June 01, 2017
59	Bell Canada	TSX:BCE	Telecom. Services	May 15, 2017
60	Sabre Corporation	NasdaqGS:SABR	Information Services	May 04, 2017
61	Rite Aid	NYSE:RAD	Retail (Special Lines)	April 11, 2017
62	Gamestop	NYSE:GME	Retail (Special Lines)	April 07, 2017
63	Verifone	NYSE:PAY	Information Services	March 09, 2017
64	InterContinental Hotels Group PLC	LSE:IHG	Hotel/Gaming	December 28, 2016
65	Yahoo! Inc.	NasdaqGS:YHOO	Software (Entertainment)	December 14, 2016
66	Quest Diagnostics	NYSE:DGX	Healthcare Support Services	December 12, 2016

67	Disney Consumer Products / Playdom Forum	NYSE:DIS	Entertainment	July 30, 2016
68	Acer Service Corporation	TSEC:2353	Computers/Peripherals	June 14, 2016
69	Southern Michigan Bank & Trust	OTCPK:SOMC	Banks (Regional)	May 13, 2016
70	Kroger (or Equifax?)	NYSE:KR	Retail (Grocery and Food)	May 05, 2016
71	ADP	NasdaqGS:ADP	Information Services	May 03, 2016
72	Verizon Enterprise Solutions	NYSE:VZ	Telecom. Services	March 24, 2016
73	Taobao	NYSE:BABA	Retail (Online)	February 04, 2016
74	Wendy's	NasdaqGS:WEN	Restaurant/Dining	January 27, 2016
75	Centene Corporation	NYSE:CNC	Healthcare Support Services	January 26, 2016
76	Time Warner Cable	NYSE:TWC	Cable TV	January 08, 2016
77	Hyatt Hotels	NYSE:H	Hotel/Gaming	December 23, 2015
78	SanrioTown.com	TSE:8136	Retail (Special Lines)	December 19, 2015
79	Vtech	SEHK:303	Telecom. Equipment	November 30, 2015
80	Starwood	NYSE:HOT	Hotel/Gaming	November 20, 2015
81	Comcast Corporation	NasdaqGS:CMCS.A	Cable TV	November 09, 2015
82	TalkTalk	LSE:TALK	Telecom. Services	October 22, 2015
83	T-Mobile	NasdaqGS:TMUS	Telecom (Wireless)	October 01, 2015

84	Hilton	NYSE:HLT	Hotel/Gaming	September 25, 2015
85	Molina Healthcare	NYSE:MOH	Healthcare Support Services	September 17, 2015
86	AutoZonePro.com	NYSE:AZO	Retail (Automotive)	August 23, 2015
87	Dixons Carphone	LSE:DC.	Retail (Special Lines)	August 05, 2015
88	Akorn, Inc.	NasdaqGS:AKRX	Drugs (Pharmaceutical)	June 04, 2015
89	Sally Beauty Holdings	NYSE:SBH	Retail (Special Lines)	May 04, 2015
90	Natural Grocers by Vitamin Cottage	NYSE:NGVC	Retail (Grocery and Food)	March 02, 2015
91	Anthem	NYSE:ANTM	Healthcare Support Services	February 04, 2015
92	Morgan Stanley	NYSE:MS	Brokerage & Investment Banking	January 05, 2015