Stock Impact of Data Breaches

Sijia “Lily” Liu
Advisor: Professor Teitel
Economics and Accounting Honors Thesis
College of the Holy Cross
April 5, 2019

Abstract

This study conducts first an OLS regression to study how stock prices of public companies in the U.S. react to data breach announcements, and subsequently, a cross-section analysis to study how different breach and firm characteristics might affect the magnitude and direction of the impact. This study includes an additional variable, “timing”, into the existing pool of firm characteristics, which measures the timing difference between breach start date and breach disclosure date. This study includes breach events from 2008 to July of 2018, a wider and more recent time period than existing studies. It is found that the overall impact of data breach announcements around disclosure date on companies’ stock prices is not significantly different from zero. The timing difference is not significant, due to the lack of sufficient disclosure of breach events. However, it is found that the size of the breached firms negatively impacts companies’ stock reactions, as well as when the breached data involved electronic user login information. It is also found that a repeated breach event somehow has a positive impact on breached firms’ stock price change from data breach disclosure.

Acknowledgements

I would like to thank professors in the Economics and Accounting Department for your help along the way. Special thanks to my thesis advisor, Professor Teitel, for your knowledge and support throughout. I would also like to mention my family and friends, who have encouraged me.

Introduction

As technology has become an integral part of people's lives, investors, capital markets, and the general public in the U.S. are increasingly vulnerable to the risk of security breaches (Cohn, 2018). Large-scale breaches of cybersecurity have been rated as one of the five most serious risks facing the world today by the World Economic Forum (World Economic Forum, 2017). A recent quote from the Securities and Exchange Commission (SEC) summarizes the broad impact and severe consequences of a security breach: "Cybersecurity risks pose great threats to investors, our capital markets, and our country...The investing public and the U.S. economy depend on the security and reliability of information (Cohn, 2018)." With the recognition that all economic parties heavily rely on information, which is increasingly electronic, in making economic decisions, the SEC voted unanimously to approve guidance to encourage public companies to provide disclosures about cybersecurity incidents they encounter and the risks they face (Cohn, 2018). Furthermore, because the economy is becoming more globalized, one incident of security breach can lead to a wide-ranging impact over the company, its investors, the local market, and even the international market.

The public has slowly begun to recognize the risks associated with cyber-attacks. Within a one-year period, starting from April 2017, the question "How can an identity thief access your personal information?" has increased its Google search popularity by 1850% (Google, 2017). This is an indication of the general public's increased awareness of the importance to protect their personal information. However, firms are often slow in implementing preventive controls on cyber security, as it is costly for them to maintain and update their cyber systems. Therefore, firms have to weigh the financial outcome of data breaches and the cost of obtaining preventive controls against cyber risks. When companies are breached, some of the potential costs include remediation costs (liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack), increased cybersecurity protection costs (these costs may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants), lost revenues resulting from the attack or failure to retain or attract customers following an attack, litigation and legal risks, increased insurance premiums, and reputational damage (SEC, 2018). These changes in risks, based on the efficient market theory, are to be captured by a stock price change of the company, as the stock price is a perfect reflection of market reaction towards one economic event—company's stock price fluctuates on a daily basis and is considered to react the fastest to news like data breach disclosures. Therefore, when companies evaluate the financial consequences of data breaches, they often turn to the evaluation of their stock price.

This study conducts first an OLS regression to study how stock prices of public companies in the U.S. react to data breach announcements. Additionally, a cross-section analysis is conducted to study how different factors, related to either breach events or breached firms, might affect the magnitude and direction of the impact. This study includes an additional variable, "timing", into the existing pool of firm characteristics, which measures the timing difference between breach start date and breach disclosure date. The timing difference is increasingly noted in media reports, especially after the Equifax incident, but has been disregarded by existing literature. This study attempts to study how breached firms' system and reaction, reflected as the days breached firms take to discover and disclose breach events, affects their stock prices. It is found that the overall impact of data breach announcements around disclosure date on companies' stock prices is not significantly different from zero. The timing difference is not significant, due to the lack of sufficient disclosure of breach events.

Review of Previous Literature

The majority of existing literature on the impact of data breaches on firms' stock prices find that data breach announcements have a significant and negative impact on firms' short-term stock prices, though the size of the impact varies among studies (Gatzlaff, 2010; Das, 2014; Cavusoglu, 2004; Goel, 2009). Others, on the other hand, find no significant relationship between data breach announcements and breached firms' stock price (Kannan, 2007; Patel, 2010; Cardenas, 2012). The disparity among studies on whether data breach announcements affect company's stock price probably results from the lack of agreed upon categorizations and definitions of data breaches. The market reacts differently towards data breach announcements that involve confidential data because such data is valuable to the general public, investors, and identity thieves, while operational data may only be valuable to investors, the firms, and their competitors. When a data breach involves confidential data of customers and employees, studies consistently find that data breach announcements significantly and negatively impact the breached firms' stock price (Gordon, Loeb, and Zhou, 2003; Acquisti, et al., 2006; Gatzlaff, 2010).

It is therefore crucial to examine what factors contribute to the negative impact of data breach announcements for firms to best evaluate its risk in being subject to the negative impact of data breach announcements. Most existing literature also perform a cross-sectional analysis on how different factors influence the magnitude and direction of the stock price change. The factors studied can be categorized into two groups, which are firm characteristics (some examples include the size of the firm, whether the firm is expected to better protect customer data, growth potential of the firm, etc.) and breach characteristics (for example, the number of records leaked). Their findings include that smaller firms are impacted more by data breach announcements (Cavusoglu 2004, Gatzlaff 2010), internet firms are more negatively impacted by breaches (Cavusoglu 2004), and that parent companies are somewhat insulated from their subsidiary's data breach announcements (Das 2014, Gatzlaff 2010).

Other than evaluating firms' risk and the magnitude of their potential financial loss from a data breach announcement, finding out about how firms can best react to data breaches more directly addresses the problem and provides firms with specific suggestions when it comes to the manner and timing of data breach disclosures. However, few have studied how firms' actions towards the public announcement of the data-breach impact the magnitude and direction stock price change. Among the few studies that focused on the aggravating or mitigating impact of certain firm actions on company's stock price change, Gatzlaff and McCullough (2010) examined whether directly addressing inquiries about the breach from the public impacted the magnitude and direction of the stock price change. Specifically, they looked at relevant news articles and descriptions of firms' data breach disclosures. They found that the more directly firms addressed to data breach events, the less negatively impacted company's stock price was (Gatzlaff, 2010). Similarly, Song, Wang, and Fan (2017) also concluded that the more voluntary the disclosure was, the less negatively impacted breached firms were. It their study, they looked at news articles on data breaches of public companies and looked at the verbs news reporters used when describing firms' actions of data breach announcements. They found that if there was a negative vocabulary (such as "admit") that described firms' announcements, the magnitude of the decrease in stock price was greater, probably because the negative vocabulary was an indication of firms' unwillingness to disclose (Song, 2017). However, in the same study, it was also found that if firms disclosed too much details of how the breach happened, they were more negatively impacted. It seemed that the public would lose confidence in firms' operations and security system if firms disclosed too much about how they failed to protect customer data.

The problem with existing studies on the impact of firms' actions on the stock price change is that their analysis of descriptions in news reports are subjective and prone to errors. Additionally, since all firms are required by SEC rules and local state legislations to disclose material data breaches, news descriptions of data breach announcements might not truly reflect firms' willingness in protecting the confidentiality of customers and employees and their efficiency in doing so. That is why this study turns to the timeliness of the data breach disclosure, which not only is objective and thus more reliable, but also is more representative of breached firms' willingness to disclose the breaches and the efficiency in existing controls around cyber security.

The timeliness of data breach disclosures as an indication of firms' control efficiency is often overlooked by the public. Oftentimes, when firms are breached, they excuse themselves from reporting the breach to the public or their investors by claiming that they need time to investigate what exactly caused the data breaches and how they happened. However, if the breached firms have greater detective controls around cyber security and proper systems around access authorizations, they would not take as long to find out what exactly went wrong in the system and subsequently disclose the data breach to the public sooner.

I hypothesize that the more quickly firms react to data breaches and disclose them to the public, the more confident they are in resolving relevant issues, which is a good indication of its internal controls. As a result, the firms are more voluntary to disclosure data breaches to the public, leading to a more positive reaction among stockholders. On the other hand, the longer breached firms wait to disclose data breaches, the more negatively impacted their stock prices are because of shareholders' declining trust in their system and management integrity.

The impact of the timeliness of data breach announcements can be exemplified by the Equifax breach event in 2017. Equifax discovered the breach in May of 2017, however, the firm did not disclose the incident to the public until September 7, 2017. Their failure to disclose the breach timely might have contributed to the steep drop in its stock price. Four days after the data breach announcement, the stock of Equifax dropped 18.4% (Nusca, 2017). By adding the variable of the timeliness of data breach disclosures into the cross-sectional analysis, this study will contribute to and further the line of studies that examine the impact of firms' actions on the change in company's stock price and aims to provide investors, firms managements, and the public a better understanding of the impact of firm actions' and management decisions on firms' performance and stock returns.

Question

This study aims to study the overall impact of data breach announcements on breached companies' stock price. Furthermore, it examines how different factors, especially the timing difference between breach start date and breach disclosure date, affect the magnitude and direction of such impact. The hypotheses of this study, therefore, are:

H1: The overall impact of data breach announcements on breached firms' stock price is negative and statistically significant.

H2: The larger the timing difference between breach start date and breach disclosure date, the bigger the negative impact on breached firms' stock price.

Methodology

The vast majority of relevant studies employ an event study methodology where the impact of data breach announcements is measured as the cumulative abnormal returns (CARs) on company's stock market exchange (Acquisti, 2006; Cavusoglu, 2004; Cardenas, 2012; Kannan, 2007; Campbell, 2003; Gatzlaff, 2010; Patel, 2010; Das, 2014). This measurement is based on the efficient market theory which assumes that changes in stock price reflect all known information of a firm. As a result, the effect of an unusual economic event (such as a data breach announcement) is perfectly reflected as the abnormal returns of company's stock price.

Abnormal returns are measured as the difference between the actual returns and the expected returns. Actual returns are the stock price of the breached firm at a given date, and the expected returns for company j at time t are estimated using the market model outlined in Brown and Warner (1985) and adopted by Gatzlaff and McCullough (2010). The expected returns using the one-factor model is calculated as follows:

$$R_{jt} = \propto_j + \beta_j R_{mt} + \varepsilon_{jt}$$

Here, $R_{jt}$and R_{mt} are the returns of company j and of the market (measured by average return of the S&P 500) for day t. On the event date (t=0), ε_{jt}represents the abnormal return, which is calculated by subtracting the expected return from the actual return for that day. The parameters of the market model are estimated using ordinary least squares (OLS) methods over the estimation window (-250, -5). The estimation window of around 250 days was adopted from Gatzlaff and McCullough. This window captures market returns from one year (about 250 trading days) before the event date to 5 trading days (1 week) before the event date. This measures the returns of company j over the event window. And estimation of the expected return of company j on the event date is based on 1 year's data.

However, while Gatzlaff used the data breach announcement date as the event date for their study, a key issue for my study specifically was the choice of the date around which to estimate the expected returns. Gatzlaff and other past researchers mostly established their models around the announcement date and estimated expected returns using returns for up to one year before the announcement date. However, because this study aims to measure the timing effect of the breach announcement, the selection of the event date for stock return estimation is crucial and therefore must be given consideration. Theoretically, it is the best to establish event windows around the breach date, as the breach event might have an impact on firm’s financial performance. Therefore, the study originally aimed to use the breach start date as the event date of the study; however, during the process of data collection, it was found that specific dates of when the breaches started and ended are largely undisclosed. This is probably due to the fact that companies are not required by the state law to disclose such information. Generally, a notification letter includes some information about the breach--though details of such information vary from company to company—, how private data was breached, if the company has taken any measures to further prevent future breaches, and resources breached individuals can resort to in order to figure out whether there has been damage to their credit records, etc.

However, because companies can choose not to disclose any of the above information if they choose not to or if the information is not available to them. For example, companies might not disclose the date of the breach because they cannot determine when exactly the breach happened, due to the nature of a cyber-attack. Companies might not disclose the type of breach because they choose to send out the notification letter before the investigation is over. Companies might even choose not to disclose too much information in fear of bad publicity and repercussions from customers and clients. As a result, specific breach dates of when the breaches start and end are largely undisclosed in companies’ breach letters, and thus makes it not practical to use start date as the event date in this study. Therefore, this study resorts to the discovery date and the disclosure date, which are the date when companies find out about the security breach events and the date of breach announcement. An estimation window of (-250, -10) is used for both estimation around discovery date and estimation around disclosure date. Estimation around discovery date yields a better result; additionally, estimating expected market returns around discovery dates avoids potential leakage effect, which is the potential for company management might leak the breach information out and cause stock price of the breached firm to behave abnormally. As a result, discovery dates are used for the market model estimation over the estimation window of (-250, -10).

After the calculation of expected returns, the abnormal return, which is the difference between the actual return and the expected return, for company j on day t is calculated as follows:

$$\square\square\square\square = \square_{\square\square} + [\hat{\alpha}_{\square} + \hat{\beta}_j R_{\square\square}]$$

Based on the efficient market theory, the stock market should capture the effect of the data breach disclosures when they are made, however, it might not be the case in real world. Ideally, different event windows should be used to fully measure the full abnormal returns. Therefore, this study measures abnormal returns for several different event windows as well: (0, 1), (-1, 1), (-5, 5), and (-10, 10). The results from all event windows are not significant, however, the result of event window (0, 1) is the most significant, which is used in the final dataset.

Additionally, both the discovery date and disclosure date

Lastly and most importantly, this study conducts a cross-sectional analysis using the following model to measure what factors contribute to the variation in stock market reactions towards data breach announcements:

$$
\begin{aligned}
CAR_j \;=\; \square \;+\; \beta_1(\square\square\square\square) + \beta_2(\square\square\square\square\square h) + \beta_3(Hightech) + \beta_4(Financial) \\
+ \beta_5(Healthcare) + \; \beta_6(Personal) + \beta_7(Electronic) + \beta_8(Identity) \\
+ \beta_9(Bank) + \beta_{10}(Healthandemploy) + \beta_{11}(Repeat) + \beta_{12}(Timing) + \varepsilon_{\square}
\end{aligned}
$$

To measure the timing effect of breach announcements, an additional variable is added to the regression. The timeliness of data breach disclosures is defined here as the timing difference between the date when the breach event starts and the date when firms disclose the breach to the public or to its clients. The “timing” variable is the number of days between the breach start date and the disclosure date, measured by subtracting breach start date from disclosure date. The decision to define “timing” variable as the timing difference between breach start date and disclosure date was due to the fact that most news articles and media sources report the start date of the breach instead of the discovery date of the breach, as the discovery date is mostly undisclosed by breached firms. The assumption here is that the investing public sees the timing gap between breach start date and disclosure date as evidence for both a lack of sufficient controls and measures to prevent or detect breaches and an unwillingness to admit wrongdoing and put customers and employees’ interest before their own.

This study also examines the impact of factors such as the industry of the breached companies based on their SIC codes and the type of data breached based on the description of breach events.

Data

Like the study conducted by Gatzlaff and McCullough (2010), this study also uses Privacy Rights Clearinghouse's database[1] to obtain a list of breach events that are dated from January 1, 2008 to July 31, 2018. The Privacy Rights Clearinghouse database has, if available, the breached firm's name in non-standard forms, breach announcement dates, number of records involved, the city and state of breached firms' location, the type of the breach, the type of the breached firm, total records breached, a brief description of the breach from media sources, and the source of the information. However, it did not have any information on when the breach started, when the breach ended, when the breach was discovered by the firm, and when the firm decided to disclose the breach, which were key pieces of information for this study's purpose of examining the timing effect of breach disclosures.

Therefore, this study uses state-level databases established by attorney general offices in states that have data breach disclosure laws and regulations. These databases are usually available for public access and contain a variety of information. However, the start date, end date, discovery date, and disclosure date of the breach could be found in detailed breach notification letters attached, which the state regulations often require to include in firms' disclosure. Additionally, even though not all states have such databases established or allow public access to the databases, because many states require all data breach events impacting residents in that state to be disclosed and because a lot of public companies have employees and customers from different states, presumably, there is a lot of overlap between breach events reported on these state-level searchable databases and breaches in other states not requiring disclosure. Therefore, the Attorney general's websites that had more information compared to the others were used to

[1] More information on Privacy Rights Clearinghouse and its database can be found on its website: https://www.privacyrights.org/ .

collect relevant dates. Used databases include websites established for California, New Hampshire, Maryland, and Washington.[2]

Since this study only concerns breach events involving publicly traded companies in the U.S., after the collection of relevant dates, existing dataset was imported into ResearchInsight, a finance software that keeps up-to-date data of public companies. As a result, 298 breach events involving 195 public companies were kept afterwards. Also obtained from ResearchInsight were daily closing prices of all 195 companies from January 1, 2008 to July 31, 2018, company's ticker symbol (which is an acronym of company's registered name), SIC code (to get companies' industry information), companies' market value of the year prior to disclosure (which represents the size of the breached firm), and companies' book-to-market ratio of the year prior to disclosure (which represents breached firms' growth potential).

Control variables related to the breaches themselves or the breached firms are also collected. Breach characteristics include the type of data breached and whether the breach was a repeat. Firm characteristics include the size of the breached firm, measured as the natural log of the market value of the firm in the year prior to the breach, its growth potential, measured as the firm's book-to-market ratio in the year prior to the breach, and the firm industry. Finally, this study aims to broaden the realm of firm-related variables by adding an additional variable that measures the timing difference between the date of disclosure and the start date of the breach.

[2] More information could be found on respective websites of state attorney generals' offices. Overlapping breach events from different websites are omitted.

Standard Industrial Classification (SIC) is used to classify firms into three groups based on their SIC codes: high-tech, financial, and healthcare. According to Cavusoglu et al. (2000), high-tech companies are expected to better protect customer data due to their improved ability to put in technical controls in the system. Financial companies, which include banks, handle more banking information of customers. Healthcare companies generally hold more personal information of patients and employees, including social security numbers, birthdates, treatment information, etc. Therefore, these companies might be subject to more scrutiny by regulators and their customers, and thus are hypothesized to be have stock prices that react more to data breach announcements.

Information on the types of data involved in the breach is collected through searches on different databases and websites including the Privacy Rights Clearinghouse, Google, and state attorney generals' websites. The Privacy Rights Clearinghouse includes a short description of the breach event, usually through a news source, and has information on the type of data breached. However, since the short descriptions are generally vague and the categorizations of breached data were too many, extensive Google searches and reviews of notification letters on state attorney generals' websites were conducted. Since this study is concerned with breach events that involve only customer and employee information, as privacy breaches were found to have a more negative impact on companies' stock prices, the private information of customers and employees are categorized into five groups:

1. Personal: breached information contains general information about the employee and/or the customer. For example, dates of birth, gender, addresses, etc.

2. Electronic: breached information contains account login information.
3. Identity: breached information contains social security number, tax identification number.
4. Bank: breached information contains banking information. For example, bank accounts, routing numbers, CVV codes for credit cards, credit card numbers, etc.
5. Healthandemploy: breached information contains information about one's health conditions and employment conditions. For example, doctors' diagnoses, salary information, one's position at the firm, etc.

Finally, the timing variable, which measures the timing of data breach announcements compared to when the breach event started, is measured as the timing difference between breach start date and breach disclosure dates, in days.

Results

Summary statistics are displayed in Table 1 in the attached. Approximately 27% of the observations are in the high-tech industry and 19% are financial institutions. However, only one observation is coded as healthcare, as a result this variable is dropped in the final analyses. As indicated in breach type variables, each breach may result in multiple types of information being at risk. The most common type of breaches involves banking, personal information and identity data, representing, 72%, 71% and 63% of the observations, respectively. Not only are multiple types of information breached, but 48% of the observations are firms with more than one data breach in the data period.[3] Finally, the average time between the breach start date and breach disclosure is 69 days.

The overall impact of data breach on breached firms' stock price is a mean cumulative abnormal return of -0.0018. While the mean is negative, it is not statistically different from zero and does not support the hypothesis that the mean CAR is negative. This might be due to the lack of disclosures on data breaches with negative cumulative abnormal returns. Additionally, the number and type of reporting companies are limited in this study. In the final dataset of 66 breach events from52 breached firms, breach events were mostly listed on the attorney generals' websites. These breach events are only the tip of the iceberg of all breach events that are disclosed or undisclosed from 2008 to 2018. This study started with 6,663 breaches that were identified by Private Rights Clearinghouse, involving both private and public companies. After narrowing the dataset to public companies only, the dataset consisted of 298 breach events from 195 unique companies. However, because of the difficulties in finding detailed information about the breach event, especially around the relevant dates of the breaches, the final dataset is significantly smaller than the initial dataset.

The lack of breach disclosures and the insufficient information provided to customers, employees, and the public regarding the breach events are further confirmed by an analysis by the Wall Street Journal, summarized in an article*, Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts*—despite the new guidance on security breach disclosures by the SEC, about 90% of known cyber incidents remained undisclosed. Though an increase in disclosures

[3] The repeat variable, which is a dummy variable, is coded as "1" if the larger dataset with 298 breach events has at least one breach event beforehand that involves the same firm, and "0" otherwise.

from 2017, when 97% of cyber incidents went undisclosed, the vast majority of public companies still choose to not report securities breaches, which could have a negative impact on their stock price. Therefore, it makes one wonder whether the lack of statistically significant result is due to the lack of disclosure by breached firms.

Cross-Sectional Analysis Results

A cross-sectional analysis is conducted to examine the potential relation of firm and breach characteristics to the magnitude and direction of the stock market response to data breach announcements. The results are summarized in Table 2.

The size of the breached firms, measured by the market value of breached firms the year prior to the disclosure date, has a negative and significant impact on breached firms' stock price. This could be due to more publicity for larger firms and higher expectations from the investing public of larger firms—larger firms might be expected to have better systems, better accountability structures, etc. This finding is contrary to Gatzlaff and McCullough's findings that the larger the breached firms are, the less of an impact breach announcements have on firms (2010). This is probably resulted from the difference in time periods between studies—Gatzlaff and McCullough and other prior research study time periods prior to 2006, whereas this study used much more recent data consisting of breach events from 2008 to July of 2018. The public's expectations of larger firms might have changed with the most recent incidents of data breaches, holding larger corporations more responsible.

If the breached data was “electronic”, which means that it involved user names, passwords, website account information, etc., the breached firms are more susceptible to a more negative impact on their stock price. This could be explained by the increasing use of the internet and online forums. If usernames or passwords get leaked, customers and employees would have to respond immediately to the breach event by changing their login information, making them more aware of the breach event.

Additionally, whether the breach event was a repeat was found to be significant and positively impacting stock price of breached firms. Among the 66 breach events, 32 are repeated breach events. Therefore, it might help explain the repeated nature of breach events and how the public can potentially get numbed by all data breach events that have been disclosed by the same company. Another explanation could be that the investing public is aware of the proliferation of data breach events. Therefore, the public might see data breach disclosures by the firm as a showcase of the firms’ responsibility and business ethics, and on the other hand see firms that only report one incident or no incident at all as ones that refuse to take measures against breaches. However, this could also result from the fact that 90% of data breaches remain undisclosed, according to the Wall Street Journal article. Therefore, the market might be unaware of a repeated breach event of the same public company.

The timing difference between breach start date and breach disclosure date is not significant. This could be explained by the lack of publicity of many breaches in the final dataset, which are listed on attorney generals’ websites but not necessarily reported to the public through news and media. Additionally, the lack of data on specific dates might have prevented this study to capture the full picture. In the future, when more data is made available through the enaction of state level laws or potentially SEC regulations, it would be interesting to see the results from continuing studies.

However, the addition of the timing variable still helps us understand the more detailed information in regard to the timeline of the breaches. As shown in Table 1, the mean of timing is 69, which means that it takes a firm an average of 69 days to discover and disclose a breach, and the timing difference ranges from 3 to 214 days. Please see the Appendix for a full list of breached firms in the final dataset, along with their ticker symbol, breach start date, breach end date, discovery date, and disclosure date, if available. The timing measure is consistent with the new report, *Trends in Cybersecurity Breach Disclosures* (2019), by Audit Analytics, where it was found that it takes on average 35 days between the date of breach and discovery of breach, and another on average 26 days between discovery of breach and disclosure of breach, which makes it a total of 61 days between the date of breach and disclosure of breach.

However, the maximum timing difference found by Audit Analytics was 1,537 days between date of breach and discovery of breach, and 367 days between discovery date of breach and disclosure date of breach. Had data been more available, those breach events would be interesting to be included in the sample. This also indicates that the timing of disclosure is still a problem that poses a threat to customers and employees, as the bigger the timing difference is, the bigger chance that their private information is used against them. Furthermore, the timing of discovery could be another area to look into for future research, as big gaps between breach date and discovery date might suggest poor internal system maintenance and the lack of detection measures within the breached firms.

Conclusion

This event study does not find the overall impact of data breach disclosures to be significantly different than zero, which is contrary to what most existing literature studying privacy breaches. However, this study examines a much broader and more recent time period of 2008 and 2018. This result could be better explained through more researched in the future with longer and more recent time periods. The lack of significant results could also result from the lack of access to breach data. Due to the fact that little is known about specific timelines and dates of breach events, this study's sample is limited. Therefore, future studies with fuller datasets might also help explain the results of this study, as data breaches continue and state and federal legislators change laws regarding data breach disclosures.

Additionally, prior studies on the impact of data breach announcements primarily obtain data from LexisNexis, which contains the largest, more egregious or more publicly known breach events. As a result, breach events in these studies might have had a more negative impact on breached firms' stock prices due to public exposure and media reports. Media coverage is a factor that could potentially be added in as a breach characteristic to control media's impact on breached firms' stock prices in the future.

The univariate test of the overall negative impact of data breach announcements is not significant in this study. However, prior research indicates that market reactions differ depending on firm and breach characteristics. Therefore, a cross-sectional analysis is also performed. This study finds that the size of the breached firm negatively impacts the impact of breach disclosures on stock price. This study also finds evidence that when username, password, and login information are breached, the breached firm's stock price is more negatively impacted by breach disclosures. Furthermore, a repeated breach is found to somehow positively impact breach disclosures on stock price.

Table 1: Descriptive Statistics of Final Dataset

Model:

$$\square\square\square\square = \square_{\square\square} + [\hat{\alpha}_{\square} + \hat{\beta}_j R_{\square\square}]$$

Variable	N	Mean	25%	Median	75%	S.D.	Min	Max
CAR	66	-0.0018*	-0.0089	-0.0019*	0.0089	0.0248	-0.1303	0.0684
Size	66	9.1827*	8.0588	9.0171*	10.4386	1.8128	4.5930	12.4726
Growth	66	2.2913*	1.4765	2.0700*	5.2409	54.8296	-398.9367	138.2623
Hightech	66	0.2727*	0.0000	0.0000*	1.0000	0.4488	0.0000	1.0000
Financial	66	0.1970*	0.0000	0.0000*	0.0000	0.4008	0.0000	1.0000
Healthcare	66	0.0152	0.0000	0.0000	0.0000	0.1231	0.0000	1.0000
Personal	66	0.7121*	0.0000	1.0000*	1.0000	0.4562	0.0000	1.0000
Electronic	66	0.1667*	0.0000	0.0000*	0.0000	0.3755	0.0000	1.0000
Identity	66	0.6364*	0.0000	1.0000*	1.0000	0.4847	0.0000	1.0000
Bank	66	0.7273*	0.0000	1.0000*	1.0000	0.4488	0.0000	1.0000
Healthandemploy	66	0.0303	0.0000	0.0000	0.0000	0.1727	0.0000	1.0000
Repeat	66	0.4848*	0.0000	0.0000*	1.0000	0.5036	0.0000	1.0000
Timing	66	69.1364*	21.0000	54.5000*	107.0000	57.4282	3.0000	214.0000

* The mean/median is significantly different from zero with P-value<0.05.

Definitions of Variables:

Size: The size of the breached firm, measured as the market value of the breached firm the year before disclosure year;

Growth: The growth potential of the breached firm, measured as the book-to-market ratio of the breached firm the year before disclosure year;

Hightech: A dummy variable. Value equals 1 if the breached firm is a high-tech company.

Financial: A dummy variable. Value equals 1 if the breached firm is a financial services company, such as banks.

Healthcare: A dummy variable. Value equals 1 if the breached firm is a health insurance company or a hospital.

Personal: A dummy variable. Value equals 1 if breached information contains general information about the employee and/or the customer. For example, dates of birth, gender, addresses, etc.;

Electronic: A dummy variable. Value equals 1 if breached information contains account login information;

Identity: A dummy variable. Value equals 1 if breached information contains social security number, tax identification number;

Bank: A dummy variable. Value equals 1 if breached information contains banking information. For example, bank accounts, routing numbers, CVV codes for credit cards, credit card numbers, etc.;

Healthandemploy: A dummy variable. Value equals 1 if breached information contains information about one’s health conditions and employment conditions.

Repeat: A dummy variable. Value equals 1 if the larger dataset with 298 breach events has at least one breach event beforehand that involves the same firm.

Timing: The timing difference between breach start date and breach disclosure date, in days.

Table 2: Cross-Sectional Regression with Breach and Firm Characteristics

Model:

$$\begin{aligned} CAR_j \;=\; \square \;+\; & \beta_1(\square\square\square\square) + \beta_2(\square\square\square\square\square h) + \beta_3(Hightech) + \beta_4(Financial) \\ & + \beta_5(Healthcare) + \beta_6(Personal) + \beta_7(Electronic) + \beta_8(Identity) \\ & + \beta_9(Bank) + \beta_{10}(Healthandemploy) + \beta_{11}(Repeat) + \beta_{12}(Timing) + \varepsilon_{\square} \end{aligned}$$

Variable	Estimate	T-Statistic	Probability Value
Intercept	0.0457**	2.29	0.026
Size	-0.0043**	-2.21	0.031
Growth	-0.0001	-1.61	0.113
Hightech	-0.0029	-0.41	0.686
Financial	-0.0089	-1.11	0.270
Personal	-0.0117	-1.35	0.182
Electronic	-0.0173**	-2.10	0.041
Identity	0.0091	1.18	0.245
Bank	-0.0126*	-1.68	0.098
Healthandemploy	0.0061	0.34	0.734
Repeat	0.0168**	2.33	0.023
Timing	0.0000	0.31	0.758

Sample size	66
F-Statistic	2.20
R-squared	0.3097
Adjusted R-squared	0.1691

*,** The variable is statistically significant at the 90%, 95% confidence level.

Definitions of Variables:

Size: The size of the breached firm, measured as the market value of the breached firm the year before disclosure year;

Growth: The growth potential of the breached firm, measured as the book-to-market ratio of the breached firm the year before disclosure year;

Hightech: A dummy variable. Value equals 1 if the breached firm is a high-tech company.

Financial: A dummy variable. Value equals 1 if the breached firm is a financial services company, such as banks.

Healthcare: A dummy variable. Value equals 1 if the breached firm is a health insurance company or a hospital.

Personal: A dummy variable. Value equals 1 if breached information contains general information about the employee and/or the customer. For example, dates of birth, gender, addresses, etc.;

Electronic: A dummy variable. Value equals 1 if breached information contains account login information;

Identity: A dummy variable. Value equals 1 if breached information contains social security number, tax identification number;

Bank: A dummy variable. Value equals 1 if breached information contains banking information. For example, bank accounts, routing numbers, CVV codes for credit cards, credit card numbers, etc.;

Healthandemploy: A dummy variable. Value equals 1 if breached information contains information about one's health conditions and employment conditions.

Repeat: A dummy variable. Value equals 1 if the larger dataset with 298 breach events has at least one breach event beforehand that involves the same firm.

Timing: The timing difference between breach start date and breach disclosure date, in days.

Appendix A: Final Dataset—A List of Breached Firms and Breach Dates

tickersymbol	companyname	breachstart	breachend	discovery	disclosure
FLWS	1-800-FLOWERS.COM	2016/2/15	2016/2/17	2016/2/15	2016/3/8
ABM	ABM INDUSTRIES INC	2017/7/7		2017/8/1	2017/11/14
ACM	AECOM	2014/6/15		2014/7/1	2014/7/8
AET	AETNA INC3	2016/9/9	2016/9/9	2016/9/9	2016/12/29
ALSK	ALASKA COMMUNICATIONS SYS GP2	2017/10/1	2017/12/22	2018/3/19	2018/5/3
AXP	AMERICAN EXPRESS CO	2018/7/5	2018/7/9	2018/7/23	2018/7/31
ARW	ARROW ELECTRONICS IN	2010/2/18	2010/2/18	2010/2/19	2010/3/3
T	AT&T INC	2017/1/25	2017/4/20	2017/5/5	2017/5/19
T	AT&T INC3	2014/8/11	2014/8/25	2014/9/23	2014/10/3
T	AT&T INC4	2014/4/9	2014/4/21	2014/5/20	2014/6/10
AN	AUTONATION INC	2014/3/5	2014/5/2	2014/5/6	2014/5/20
BJ.1	BJ'S WHOLESALE CLUB INC2	2007/12/31		2008/1/3	2008/1/15
BA	BOEING CO	2016/11/21	2016/11/21	2017/1/9	2017/2/8
BC	BRUNSWICK CORP	2016/4/29	2016/4/29	2016/4/29	2016/5/2
CAH	CARDINAL HEALTH INC	2010/6/15		2010/6/15	2010/9/7
CTL	CENTURYLINK INC	2017/1/30	2017/2/1	2017/2/1	2017/2/24
CVX	CHEVRON CORP	2016/6/4	2016/6/4	2016/7/1	2016/8/18
DAL	DELTA AIR LINES INC	2017/9/26	2017/10/12	2018/3/28	2018/4/13
EBAY	EBAY INC	2014/2/28	2014/3/1	2014/5/7	2014/5/21
EXEL	EXELIXIS INC	2013/7/30	2013/7/30	2013/7/30	2013/8/16
FRC	FIRST REPUBLIC BANK	2012/8/2	2012/8/2	2012/8/2	2012/8/14
FRC	FIRST REPUBLIC BANK2	2012/1/21	2012/2/25	2012/2/25	2012/5/16
FRED	FREDS INC	2015/3/23	2015/4/24	2015/4/24	2015/8/10
HNT	HEALTH NET INC	2013/4/1	2013/5/3	2013/5/3	2013/7/2
HQY	HEALTHEQUITY INC	2018/4/11	2018/4/13	2018/4/13	2018/6/13
HD	HOME DEPOT INC	2014/4/15		2014/9/2	2014/9/8
HD	HOME DEPOT INC3	2014/3/7	2014/5/21	2014/5/21	2014/5/27
HUM	HUMANA INC2	2012/7/12	2012/11/28	2012/11/28	2012/12/17
HUM	HUMANA INC4	2018/6/3	2018/6/4	2018/6/3	2018/6/22
H	HYATT HOTELS CORP	2017/3/18	2017/7/2	2017/7/7	2017/10/12
INTU	INTUIT INC10	2016/10/17		2016/10/17	2016/11/4
INTU	INTUIT INC11	2016/4/12	2016/4/12	2016/4/12	2016/10/17
INTU	INTUIT INC12	2016/8/22	2016/8/22	2016/8/22	2016/9/15
INTU	INTUIT INC14	2017/2/13	2017/2/13	2017/2/13	2017/2/21
INTU	INTUIT INC15	2016/11/22	2016/11/22	2016/11/22	2016/12/2
INTU	INTUIT INC16	2017/2/26	2017/2/26	2017/2/26	2017/3/10
JLL	JONES LANG LASALLE I	2009/12/17	2009/12/23	2009/12/23	2010/1/7
JPM	JPMORGAN CHASE & CO2	2013/7/15	2013/9/15	2013/9/15	2013/12/5

KMB	KIMBERLY-CLARK CORP	2017/10/18		2017/10/20	2017/10/30
M	MACY'S INC	2018/4/26	2018/6/12	2018/6/11	2018/7/1
NFLX	NETFLIX INC	2011/2/15	2018/4/11	2011/4/4	2011/4/20
JWN	NORDSTROM INC	2013/8/14	2013/10/5	2013/10/5	2013/11/7
JWN	NORDSTROM INC2	2012/6/15	2018/7/12	2012/6/7	2012/8/1
NUAN	NUANCE COMMUNICATION	2014/12/10		2015/1/27	2015/3/20
NVDA	NVIDIA CORP	2014/10/8		2014/12/1	2014/12/17
OCR	OMNICARE INC	2011/1/19	2011/1/19	2011/1/19	2011/3/8
OMCL	OMNICELL INC	2012/11/14	2012/11/14	2012/11/15	2012/12/21
PKI	PERKINELMER INC	2016/2/24	2016/2/24	2016/2/24	2016/3/16
PFE	PFIZER INC	2011/4/22	2011/4/22	2011/4/22	2011/6/10
PFE	PFIZER INC3	2008/2/7	2008/2/7	2008/2/7	2008/3/19
PRI	PRIMERICA INC	2017/4/5	2017/4/5	2017/4/5	2017/4/14
DGX	QUEST DIAGNOSTICS IN	2014/11/17	2014/11/17	2014/11/17	2014/12/22
RCII	RENT-A-CENTER INC	2012/4/1	2012/4/1	2012/4/2	2012/4/25
RSG	REPUBLIC SERVICES IN	2013/8/10	2013/8/10	2013/8/11	2013/8/26
RAD	RITE AID CORP	2017/1/30	2017/4/11	2017/4/11	2017/5/17
RAD	RITE AID CORP2	2015/1/15	2015/2/15	2015/4/30	2015/6/5
ROL	ROLLINS INC	2013/3/4	2013/3/12	2013/3/12	2013/3/27
SFM	SPROUTS FARMERS MARK	2016/3/14	2016/3/17	2016/3/17	2016/3/28
SPLS	STAPLES INC	2014/8/10	2014/9/16	2014/9/15	2014/12/19
SMMF	SUMMIT FINANCIAL GRO	2015/1/1	2015/2/15	2015/4/15	2015/6/22
RUN	SUNRUN INC	2017/1/20	2017/1/20	2017/1/20	2017/2/2
TMUS	T-MOBILE US INC	2015/9/15	2015/9/15	2015/9/15	2015/9/21
TXT	TEXTRON INC	2009/10/15		2009/11/3	2009/12/3
VRA	VERA BRADLEY INC	2016/7/25	2016/9/23	2016/9/15	2016/10/12
WU	WESTERN UNION CO	2013/9/3	2013/9/5	2013/9/5	2013/10/29

References

Alessandro Acquisti, Allan Friedman. 2006. "Is There a Cost to Privacy Breaches? An Event Study." *Twenty Seventh International Conference on Information Systems.* Milwaukee.

Atiya Avery, C Ranganathan. 2016. "Financial Performance Impacts of Information Security Breaches." *the 11th Pre-ICIS Workshop on Information Security and Privacy*. Dublin: Association for Information Systems. 1-16.

Audit Analytics. 2019. "Trends in Cybersecurity Breach Disclosures." 2019.

Cohn, Michael. 2018. "SEC wants cybersecurity disclosures." *Accounting Today*, February 26. https://www.accountingtoday.com/news/sec-wants-cybersecurity-disclosures.

Dean, Christos Makridis and Benjamin. 2017. "The Economic Effects of Cyber Security Failures on Firms: Evidence from Publicly Reported Data Breaches."

Google. 2017. Information Security: Interest Over Time. Accessed May 1, 2018. https://trends.google.com/trends/explore?q=information%20security.

Huseyin Cavusoglu, Birendra Mishra, & Srinivasan Raghunathan. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers." *International Journal of Electronic Commerce* 69-104.

Jengchung V. Chen, Hung-Chih Li, David C. Yen, Kenneth Vincent Bata. 2012. "Did IT consulting firms gain when theri clients were breaches?" *Computers in Human Behavior* 456-464.

Jesus Cardenas, Adolfo Coronado, Aurelia Donald, Fernando Parra, & M. Adam Mahmood. 2012. "The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation." *the Eighth Americas Conference on Information Systems.* Seattle: Association for Information Systems. 1-8.

Karthik Kannan, Jackie Rees & Sanjay Sridhar. 2007. "Market Reactions to Information Security Breach Anno an Empirical Analysis." *International Journal of Electronic Commerce* 60-90.

Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou. 2003. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market." *Journal of Computer Security* 431-448.

Kevin M. Gatzlaff, Kathleen A. McCullough. 2010. "The Effect of Data Breaches on Shareholder Wealth." *Risk Management and Insurance Review* 61-83.

Myung Ko, Kweku-Muata Osei-Bryson, & Carlos Dorantes. 2009. "Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms." *Information Resources Management Journal* 1-21.

Nusca, Andrew. 2017. "Equifax Stock Has Plunged 18.4% Since It Revealed Massive Breach." Fortune, September 11. http://fortune.com/2017/09/11/equifax-stock-cyberse curity-breach/.

Patel, Nishant. 2010. "The Effect of IT Hack Announcements on the Market Value of Publicly Traded Corporations." Durham, North Carolina: Duke University, April.

Rubin, Gabriel. 2019. "Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts." The Wall Street Journal, February 26.

Saini Das, Arunabha Mukhopadhyay, & Manoj Anand. 2014. "Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics." *Journal of Information Privacy and Security* 27-55.

Sanjay Goel, Hany A. Shawky. 2009. "Estimating the market impact of security breach announcements on firm values." *Information & Management* 404-410.

Securities and Exchange Commission. 2018. “Commission Statement and Guidance on Public Company Cybersecurity Disclosures.”

Spanos Georgios, Angelis Lefteris. 2014. “The impact of information security events to the stock market: A systematic literature review.” *Computers & Security*.

World Economic Forum. 2017. "Global Risks Report 2017."

Ziqian Song, G. Alan Wang, Weiguo Fan. 2017. "Firm Actions Toward Data Breach Incidents and Firm Equity Value: An Empirical Study." *the 50th Hawaii International Conference on System Sciences*. 4957-4966.