S

Introduction

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. A 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 price finds 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 (Gatzlaf et al., 2010; Das, 2014; Cavusoglu, 2004; Goel, 2009). Others, on the other hand, find insignificant relationship between data breach announcements and breached firms' stock price (Kannan, 2007; Pan, 2010; Cardenas

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 (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 matter 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

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.

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 a delayed 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

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, 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 disclosure.

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 in California, New Hampshire, Maryland, and Washington.[2]

Since this study only concerns breach events involving publicly traded companies in the U.S.,

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.

breach in the data period.[3]

from 2017, when 97% of cyber incidents went undisclosed, the vast majority of public companies still chose to not report security breaches, which could have a negative impact on their stock price. Therefore, it makes one wonder whether the lack of statistically significant result isdue 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 (2010). This is probably resulted from the difference in time periods between studies Gatzlaff and McCullough and other prior research stud. I (m) Tc 0 T-5 ((m)-28.8 -2.3 Td [(0 T0Tc -06,Tc -0.011)-12

0(c)-6 (C)-314 (ed)6 (t)3.9

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 increase 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 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,

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 come to light 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 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:

$$= \quad + [\quad + \quad]$$

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:

$$= + {}_1( ) + {}_2( ) + {}_3( ) + {}_4( ) + {}_5( ) + {}_6( ) + ( ) + ( ) + ( ) + ( ) + ( ) + ( ) +$$

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	

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 corr

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	

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. 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-cybersecod D(c)-6P <</MC4 0 Td [(T Tc 0.022 T0E