The Effect of a Public Announcement of a Company Data Breach over Time

Honors Undergraduate Thesis

Presented in Partial Fulfillment of the Requirements for the Degree with Honors Research Distinction in Finance in the Fisher College of Business of The Ohio State University

By

Jordan Hepperle

Undergraduate Degree in Business Administration with an Accounting Specialization

The Ohio State University

2019

Thesis Committee:

Dr. Roger Bailey

Dr. Justin Birru

Abstract

Public announcements of data breaches do not affect all companies the same. Data security and hacking and their effect on companies have become popular subjects to study since the start of the 2000s. By measuring the cumulative abnormal return (CAR) of stocks, it has been found in previous studies that announcements of a data breach do negatively affect the stock's return after the public announcement. The cumulative abnormal return is a finance term used to measure the impact of an event on a stock. To expand on past research, and to examine to see if there is any correlation between the year of the public announcement of a company data breach and the cumulative abnormal return, this paper measures the cumulative abnormal return of stocks that announced a data breach for the years 2005-2018. The data set consists of over 300 incidents of publicly traded companies that suffer data breaches from 2005-2018. The cumulative abnormal return for the year is plotted on a timeline and examined for any patterns. This paper examines how the effect of a data breach has affected companies' stock returns over the fourteen years of data. In order to help determine if there has been a trend regarding investors' opinions about data security over the years as it has become more prominent in everyday lives. It appeared that the year the data breach was announced did not have a significant effect over the timeline.

Acknowledgements

I would like to thank Justin Birru for all of his support and mentorship with my project. Without his patience and guidance I would not have been able to graduate with Research Distinction. I could not have asked for a better advisor to have the opportunity to work with throughout this program. I would also like to thank Dr. Roger Bailey for his commitment to our Honors Contract Program. Dr. Bailey has taught us the value of research and solving problems, which are lessons we will take onto our future endeavors. Lastly, I would like to thank my family, for their love and support, and shaping me into the person I am today.

Vita

June 2015 ……...Issaquah High School

May 2019 ……BSBA Accounting, The Ohio State University

Fields of Study

Major Field: Business Administration: Accounting

Minor Field: Economics

Table of Contents

List of Tables

List of Figures

Introduction

Any company that stores customer or employee information is at risk for a security breach of this private information. It seems fairly common now to hear about "data breaches", "security hacks", and "cyber-attacks" in the news whether it be business, government, or personal information. Data security has turned into a buzz phrase. Since the internet boom, essentially everyone is vulnerable to identity theft due to the increased amount of online shopping, online banking, and online account information storage. After highlighting the major cyberattacks of 2017, CNN quotes Mark Nunnihoven, vice president of cloud research at the security company Trend Micro, saying there is more to come, "as we do more and more of our business online, and as criminals realize the value of data that organizations are protecting, we're seeing more big-name breaches, more high profile breaches" (Larson 2017). Many companies don't put enough resources toward research and security to know the trends of the reactions to a data breach or fully protect themselves from hackers. The effects of such events can be so complex that research is just scratching the surface of the trends of a data breach. The 2000s have been a huge time period of growth and change in the way that we go about our daily lives. This has led to a new data security epidemic that society is trying to understand. To end, the year 2018 was a big year for data security legislation. It was the first year that all 50 States and territories of the United States had data breach notification laws. It has been proven that companies are impacted negatively from a data breach, but has the same negative impact stayed consistent over the years? It seems that investor reactions each year regarding data security breaches are worth examining for future predictions as more companies are being put under more pressure to disclose and provide a greater degree of transparency.

My study aims to investigate the relationship between the year that a company publicly announced a data breach and the cumulative abnormal return for the day before, day of, and day after the announcement CAR (-1,1). The cumulative abnormal return is a common measurement used to examine how events impact stock returns. By comparing the cumulative abnormal return over the 14 year period of the study, 2005-2018, I investigate to see if the CAR (-1,1) is consistent year after year, and if the average CAR (-1,1) for the first 7 years in the study is different from the average CAR (-1,1) of the second half of time period. This will provide information about security breach events trends and will be able to give some insight on any reaction trends over the years. I also separate out the data breaches that are classified as "hacks" to examine for more trends. By examining the cumulative abnormal return (CAR), and analyzing how the year effects the breach, the CAR (-1,1) can be used as a measure to interpret how investor reactions may have changed over the time period.

Literature Review

A current research study, *What is the Impact of Successful Cyberattacks on Target Firms,* investigates firms, and analyzes which firms are more likely to be a victim of a cyberattack, and how these firms that do suffer attack are affected. Their research covers extensive variables to examine which companies are the most susceptible to a data breach. The findings include "that the more visible firms such as larger firms and firms included in the *Fortune 500* list, more highly valued firms, firms with more intangible assets, and firms with less board attention to risk management are more likely to be attacked." (Kamiya, Kang, Kim, Stulz, 2018) There are many studies that shows the possible negative effects of a public announcement of a company data breach. Previous event studies have been conducted to explore the impact of a public

announcement of a company data breach especially in the earlier 2000s. “Such announcements have often – but not always – had a significant negative impact”. (Acquisti, Friedman, Telang 2006). It is frequently noted in many studies that it can be hard to accurately quantify the price that companies pay as a result for a security breach event. However, it has been stated that a useful measure used throughout studies is to measure the stock price changes after a company faces a significant event, like a public announcement of a data breach is measuring the cumulative abnormal return. A decline in a company’s stock price is an indicator that the event had an adverse consequence to the company. There are a great number of costs, such as security upgrades, litigation costs, and fines on top of damaged brand reputation that a company could face when dealing with the aftermath, and a stock market assessment helps bring all these costs into one comparable measurement. Researchers have found that “the more recent instances in their sample are associated with a stronger negative stock market response, which they attribute to investors’ changing perceptions of security breaches over time” (Gatzlaff, McCullough 2010). In general, the studies discuss in some capacity that the loss in market value that companies experience as a result of a security breach type event needs more analysis. In addition, these previous studies that were conducted used the cumulative abnormal return (CAR) to measure the effect of the event. The abnormal returns compare the stock return of the day to the market return of the day to examine expected returns if the event did not occur. It is important to note that the CAR is a summation of the abnormal returns over the time period of the event window. For my study I will calculate the annual CAR, meaning I will take the average of the breach CARs in that year. Past event studies have all noted that there is a need for more research, and that this is a very complex issue that

companies and the public have to deal with. There are many variables that can affect a company's outcome or consequences when it announces a data security breach.

Hypothesis

- Dependent Variable = CAR (-1, 1)

- Independent Variable = Date of the Public announcement of the company data hack

Predictions:

This research supposed that as the time periods increase, it will result in a more negative CAR. As the time period increases closer to 2018 the trend is that companies will have an increasingly negative market returns after the announcement of a company data breach. It appears as though society is becoming more aware and fearful to the idea that their information is vulnerable; therefore, this research predicts that compared to the later 2000s of the 14 year stretch that there is a stronger negative statistically significant reaction to a company's CAR, after a public announcement to a company data breach in the earlier 2000s. These effects are compounded since news is continually breaking that even companies that are in the market of protecting private information are vulnerable to such security breaches.

Methodology

The data for this project was collected from companies that suffered a data breach from 2005-2018. The cases used in the sample regarding company data hacks came from the website www.privacyrights.org/data-breach. Privacyrights.org is a nonprofit organization that focuses on privacy and consumer protection. The website gives a list of types of businesses that were attacked, and the categories selected for this study were Business-Financial + Insurance

services (BSF), Business - other (BO), Businesses - retail/merchant + including online retail (BSR), and Unknown (UNKN). The list of security breaches from 2005-2018 was downloaded, the number of data breaches that occurred in each year was counted to see how the number of breaches reported over the years have changed. The companies that were not public at the time of the breach, and companies that did not suffer loss of personal data were eliminated from the data set. Once the private companies at the time of their data breach announcement were eliminated from the data set, a second count of the number of data breaches that happened each year was completed to compare the number of announcements each year of companies that were public at the time, and then compared the public count to the original total count. The study used the CAR event window of (-1, 1), one day before the date of announcement, day of the announcement, and one day after the announcement.

The study used Bloomberg functions in excel to obtain the ending stock price of the days before, day of, day after, and the S&P 500 return for the same dates for each separate security breach to calculate the abnormal return for each company that suffered a data breach. The study used the S&P 500 return as the market measure in order to have a singular consistent measurement. Next, the historical ending price data points were obtained by using the Bloomberg historical cost lookup formula in excel by using the company's ticker symbol and date that used for the calculation programmed into the formula. Once all the data points for each company's stock and the market of the days were obtained, the calculations were started. . The first step to calculating the cumulative abnormal return was to find the abnormal return for the date before, the day of, and the day after for each data breach that a company announced. The abnormal return was found by subtracting the S&P 500 market return from the

stock return from each particular day. After all the abnormal returns were calculated, the next step was to find the cumulative abnormal return for each year that is included in the study. To calculate the CAR, first the average abnormal return from each year for each the day before, the day of, and the day after the public announcement of a data breach was found, then the average abnormal return from the day before, the day of, and day after an announcement of each year was added up to give the CAR (-1,1) for each year 2005-2018. Then a histogram with the year on the horizontal axis and the annual CAR (-1,1) on the vertical axis was made to get a visual representation of the data. The cumulative abnormal return calculation for each year helped to compare how the year affected the returns on the stocks after a public announcement of a data breach, to help prove if the hypothesis is correct.

Next, the steps above are repeated for a smaller data set by just looking at the data breaches from the total list of companies that were classified as a "hack". To do this, the list of data breaches from privacyrights.org with all the same requirements from above was downloaded again, but instead this time only selected "hack" from the type of breach section. The study used the same procedures mentioned above to calculate the annual CAR (-1,1) for 2005-2018 for "hack" data set. Next, a histogram with the year on the horizontal axis and the annual CAR (-1,1) on the vertical axis was made to get a visual representation of the data.

A chi square analysis for both the total data set, and the "hack" data set was made that will be used to indicate if there is a significant difference between the cumulative abnormal return for each year. To do this, the sum of all the annual CARs (-1,1) was taken and divided by 14, which is the number of years used in this study. This was the expected return value. Then

the expected value was subtracted from the observed value, and then squared to find each year's contribution to the chi-square. The chi square statistic was compared to the chi square chart to determine if it is a significant value. To show a significant relationship between the year that the breach occurred and the CAR (-1,1), statistically significant p value with an alpha value of .05 and 13 degrees of freedom. The chi square analysis was used show how the general investor reaction and the stock market may have changed over the time period, and that the responses are not the same each year if there is a significant chi square statistic. The goal was to show if the year of the announcement could affect the CAR of a company's stock value.

To further analyze any trends, the mean annual CAR (-1,1) was calculated for the total data set, and the "hack" data set. First, each mean was compared to zero using a *t* test to confirm a better understanding of the overall effect of a public announcement of a data breach over all the years. Then, a difference of means test was used to analyze how the two means compare to each other, to help compare the two different data sets. For each of the two data sets the mean for the first half (2005-2011) and the second half (2012-2018) was calculated. For each of the data sets another difference of means test was conducted for each data set to see if the mean annual CAR (-1,1) from the first 7 years in the study is statistically significant from the mean annual CAR (-1,1) from the second 7 years in the study. The difference of means test provided some more evidence of potential trends in the investor's reactions over the years.

Next, the same method from above was used to do two more CAR calculations using the total data set, one from the day before and day of the announcement of a data breach CAR(-1,0), and the CAR (1) of the day after the announcement of a data breach. Again a histogram

was made for the annual CAR (-1,0) and annual CAR (1) with the year on the horizontal axis and the CAR on the vertical axis. These two calculations were used to compare how investors may have reacted differently before/day of and after the date of announcement. The study compared the 2005 annual CAR (-1,0) to the 2005 annual CAR (1), until each of the two CAR calculations are compared for each year. The study looked to see if the annual CARs flipped signs, indicating a reaction and a market correction. This helped draw some conclusions about over reactions and under reactions that investors may have had.

Results

The primary hypothesis is that the year that a data breach was announced did have an effect on the annual CAR (-1,1). It was predicted that the annual CAR (-1.1) of the later years would have more of an effect on the company's stock than the annual CAR (-1,1) of the earlier years included in the study. While it was proven that the average annual CAR (-1,1) does have a negative effect on the company's stock. There were no clear trends found in the annual CAR (-1,1) over the years of 2005-2018.

Figure 1

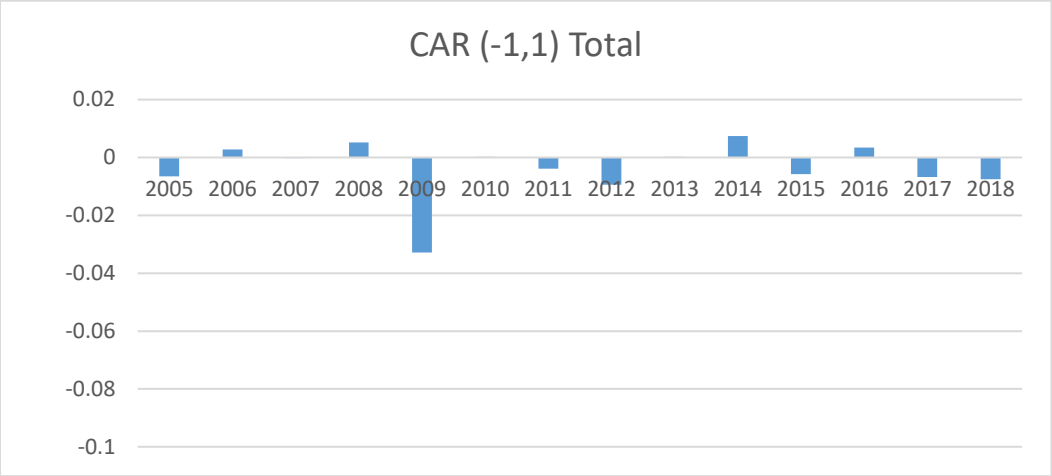


Table 1

t-Test: Two-Sample Assuming Equal Variances		
	1st half of CAR	2nd half of CAR
	Variable 1	*Variable 2*
Mean	-0.001917064	-0.004135278
Variance	0.001289454	0.000779326
Observations	189	189
Pooled Variance	0.00103439	
Hypothesized Mean Difference	0	
df	376	
t Stat	0.670466661	
P(T<=t) one-tail	0.251485973	
t Critical one-tail	1.648916269	
P(T<=t) two-tail	0.502971947	
t Critical two-tail	1.966293229	

Figure 1 shows the average annual CAR plotted for each year. It was seen that on average the annual CAR (-1,1) is negative for the total data set. The total data set consisted of 378 data breach announcements in the years included in the study. It is important to note that list of data breach announcements originally consisted of over 1,000 data breach announcements, before the companies

that were not public at the time of their data breach announcement were eliminated from the data set. The mean annual CAR (-1,1) was -.30%, and a *t*-test showed that it is statistically significant at the 10% level. The mean annual CAR (-1,1) for the first half of the data was -.19% and the mean annual CAR (-1,1) for the second half was -.40%. After conducting a difference of means test seen in table 1 above, the mean CAR (-1,1) of the first half, was not statistically different from each other. This indicated that it cannot be concluded that investors acted in a different way in the earlier years in the study compared to the later years in the study. It may be relevant to note that 2009 may have been a result of a very pessimistic investment market at the time of the great recession, which is why its cumulative abnormal return CAR (-1,1) appeared to be more of an outlier in the data. A robustness check was conducted to examine what happens when the year 2009 is excluded from the data. A difference of means test was run for the first half of the data compared to the second half of the data, excluding the breaches that were announced in 2009, and found a t-stat of 1.68. This is significant at the 10% level, meaning that 2009 could be a bit of an outlier in this case. The difference of means in Table 7 listed in the appendix.

Figure 2

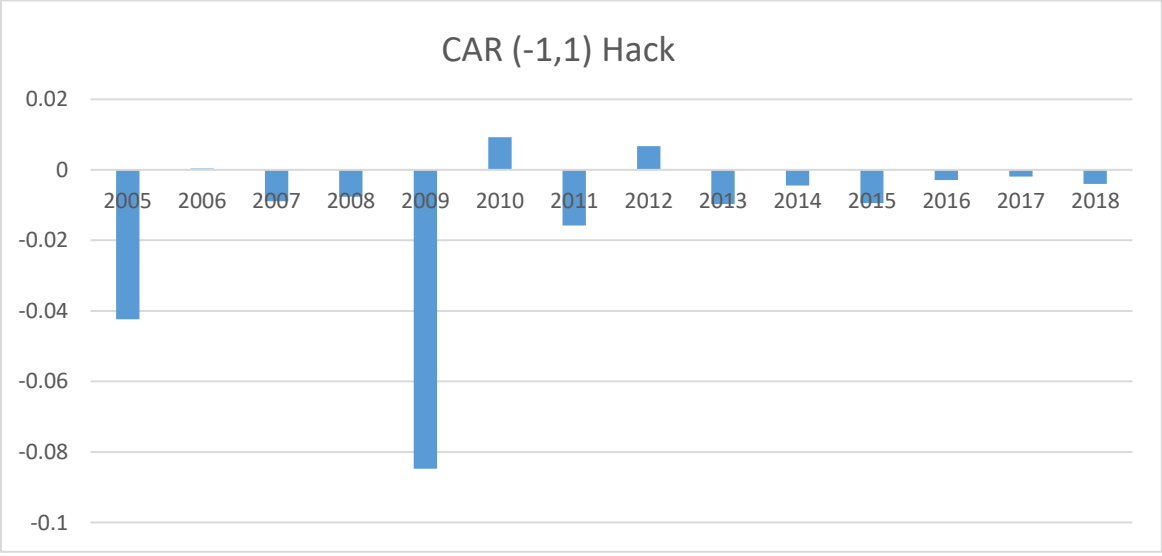


Table 2

t-Test: Two-Sample Assuming Equal Variances		
	1st half of CAR	2nd half of CAR
	Variable 1	*Variable 2*
Mean	-0.007570421	-0.005420874
Variance	0.001493015	0.001368476
Observations	96	97
Pooled Variance	0.001430419	
Hypothesized Mean Difference	0	
df	191	
t Stat	-0.394782605	
P(T<=t) one-tail	0.346721914	
t Critical one-tail	1.652870547	
P(T<=t) two-tail	0.693443827	
t Critical two-tail	1.97246199	

Figure 2 shown above showed the annual CAR (-1,1) for the companies that announced a data breach that are categorized as a "hack" on privacyrights.org. This data set consisted of 193 public announcements of a data breach that were categorized as "hacks". The mean annual CAR (-1,1) of this data set was -.65%, and after running a *t* test it was proven to be statistically significant at the 5% level. After conducting a difference of means test, the mean of the total dataset CAR (-1,1) is not statistically different than the mean of the "hack" dataset. However, the magnitude for the negative returns was much larger for the "hack" dataset. One potential theory for the insignificance between the two means was that the much smaller number of data breaches in the "hack" dataset versus the total dataset. The mean annual CAR (-1,1) for the first half was -.76% and the mean annual CAR (-1,1) for the second half was -.54%. The difference in the means from each half was not statistically significant. This indicated that it cannot be concluded that investors acted in a different way in the earlier years in the study compared to the later years in the study for the "hack" data set either. It may be relevant to note again that 2009 may have been a result of a very pessimistic investment market at the time of the great

recession. As a robustness check to examine what happens when the year 2009 is exclude from the data, a difference of means test was run for the first half of the data compared to the second half of the data, excluding the breaches that were announced in 2009, and found a *t*-stat of 0.53. The test results indicated that this is insignificant. The difference of means in Table 8 listed in the appendix.

Table 3

	Date	CAR (-1,1)
2	2005	-0.006522134
3	2006	0.002804396
4	2007	-0.000182286
5	2008	0.005231736
6	2009	-0.032902119
7	2010	0.000232218
8	2011	-0.003870377
9	2012	-0.009375147
10	2013	0.000231532
11	2014	0.007366591
12	2015	-0.005759332
13	2016	0.003445538
14	2017	-0.006755843
15	2018	-0.007478909

observed	expected value	contribution to chi square			
-0.00652	-0.003823867	-0.001904			
0.002804	-0.003823867	-0.011489		Critical chi square value	
-0.00018	-0.003823867	-0.003468		13 degrees of freedom k-1	
0.005232	-0.003823867	-0.021445	alpha	0.01	
-0.0329	-0.003823867	-0.221123		27.69	
0.000232	-0.003823867	-0.004302		no significance	
-0.00387	-0.003823867	-0.000001			
-0.00938	-0.003823867	-0.008059			
0.000232	-0.003823867	-0.004301			
0.007367	-0.003823867	-0.032749			
-0.00576	-0.003823867	-0.000980			
0.003446	-0.003823867	-0.013820			
-0.00676	-0.003823867	-0.002248			
-0.00748	-0.003823867	-0.003494			
	chi square statistic	-0.32938			

After running a chi square analysis to further investigate for a relationship, the p value was calculated to be insignificant, seen above in Table 3. This meant that there is no significant relationship between the year that the data breach was announced and the CAR (-1,1). There were no conclusive trends with this test.

Figure 3

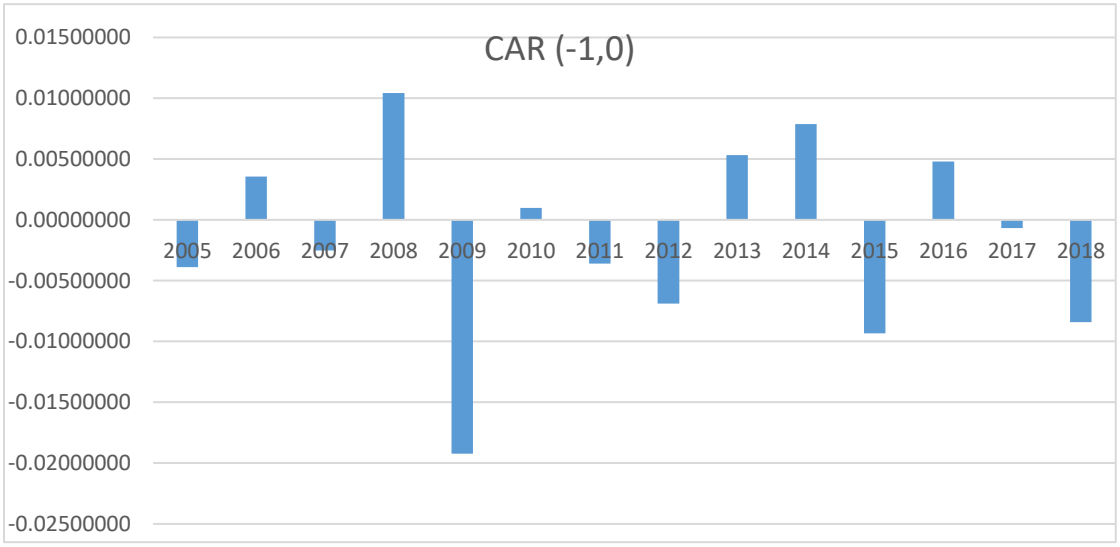
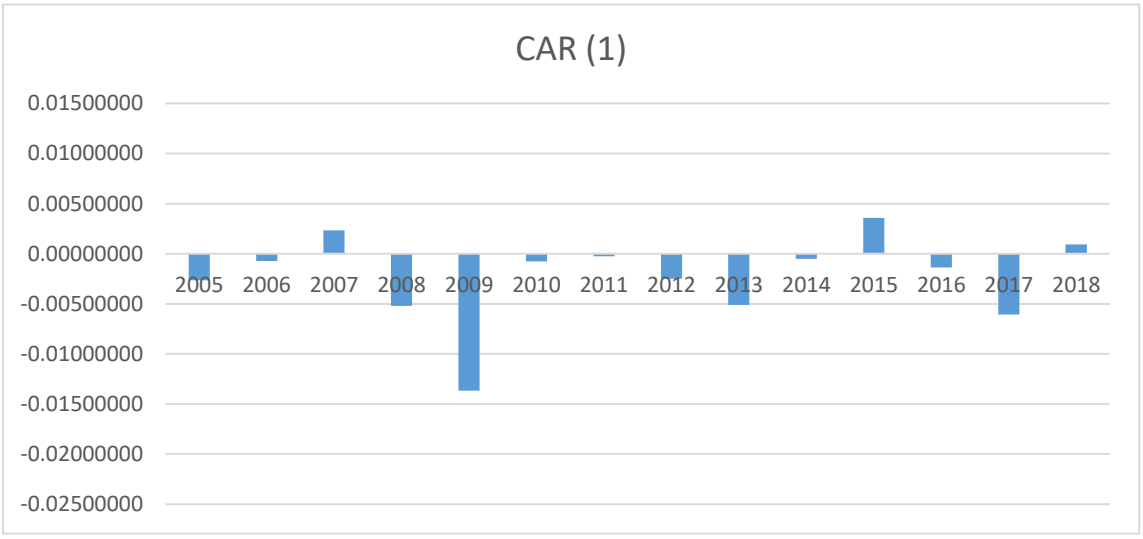


Figure 4



To further investigate for trends in investors reactions. Each year's annual CAR (-1,0), seen in figure 3, and the corresponding year's annual CAR (1), seen in figure 4 was examined. Returns on day (-1,0) that go in the opposite direction of returns for (1) would be consistent with overreaction in that the market moves too much initially, and then moves back in the opposite direction to correct itself. After

comparing the two different CAR calculations for each year, it was found that 9 out of the 14 years there were signs of overreaction with investors after a public announcement of a data breach, due to movements in the opposite direction. This indicated that investors about 66% of the time investors are more likely to initially overreact at reacting to the news of a data breach.

Table 4

CAR (-1,0)					
observed	expected value	contribution to chi square			
-0.00388604	-0.00154127	-0.003567173			
0.00355141	-0.00154127	-0.016827311		Critical chi square value	
-0.00252213	-0.00154127	-0.000624216		13 degrees of freedom k-1	
0.01042873	-0.00154127	-0.09296303	alpha	0.01	
-0.01922877	-0.00154127	-0.202980731		27.69	
0.00099002	-0.00154127	-0.004157226		no significance	
-0.00360835	-0.00154127	-0.002772285			
-0.00689418	-0.00154127	-0.01859101			
0.00533315	-0.00154127	-0.030661529			
0.00787426	-0.00154127	-0.057518995			
-0.00933344	-0.00154127	-0.039394793			
0.00480360	-0.00154127	-0.026119676			
-0.00068461	-0.00154127	-0.000476138			
-0.00840140	-0.00154127	-0.030534237			
	chi square statistic	-0.527188351			

Table 5

CAR 1					
observed	expected value	contribution to chi square			
-0.00263609	-0.00228260	-0.0000547434			
-0.00074702	-0.00228260	-0.0010330391		Critical chi square value	
0.00233984	-0.00228260	-0.0093607969		13 degrees of freedom k-1	
-0.00519700	-0.00228260	-0.0037210695	alpha	0.01	
-0.01367335	-0.00228260	-0.0568427710		27.69	
-0.00075780	-0.00228260	-0.0010185838		no significance	
-0.00026203	-0.00228260	-0.0017886261			
-0.00248096	-0.00228260	-0.0000172383			
-0.00510162	-0.00228260	-0.0034814980			
-0.00050767	-0.00228260	-0.0013801712			
0.00357411	-0.00228260	-0.0150271630			
-0.00135807	-0.00228260	-0.0003744683			
-0.00607123	-0.00228260	-0.0062883213			
0.00092249	-0.00228260	-0.0045003992			
	chi square statistic	-0.1048888892			

After running a chi square analysis for each broken down CAR, CAR(-1,0) and CAR (1), the p value was calculated to be insignificant. This meant that there is no significant relationship between the year that the data breach was announced and the CAR (-1,0) or CAR (1). Unexplained variation could play a role in the effect in the reaction after a public announcement. There were no conclusive trends with this test.

Table 6

Date	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
# of breaches 1	11	43	44	25	11	35	30	26	20	14	15	13	15	75
# of breaches 2	30	141	121	68	30	100	117	118	53	45	30	48	45	330

After examining the count of the number of breaches each year for just the public companies, next to the number of private and public companies, the public companies made up roughly a third of the data breaches reported for the categories of businesses chosen. Note that neither of these counts include educational institutions, government and military, healthcare providers/institutions, and non-profits which would have added an even greater number of reported data breach; however, for these types of companies and institutions it would be extremely difficult to measure their loss. Also note the jump in the count for the year of 2018. One explanation for the large jump could be attributed to the new legislation that was enacted in 2018. 2018 was the first year that all fifty states and the U.S. territories had legislation of data breach disclosure to the public.

Discussion

While there may not be a clear trend in the cumulative abnormal return after a data breach over time, it is clear to see by the number of attacks that this is a persistent problem that society is facing today, and that the magnitude of the CAR for companies that suffered a "hack" is more negative. While the year that the announcement is made and the CAR are independent of each other, the number attacks being reported is on the rise due to new laws and regulations. The absence of trends indicates that data security is an issue that is ongoing. With the new laws regarding data security implemented in 2018, it appeared that the new laws had an impact on the count given the rise of the count recorded in 2018. It would be interesting to investigate in more detail in the future to examine how the legislation continues to change and affect how and when companies are required to make an announcement and report when they suffer a data breach. It would be interesting to look more in detail about the differences in data legislation between the states. Would data regulation and disclosure be more effective for the victims if it was nationally regulated? Even though all fifty states and the U.S. territories now have legislation as of 2018, society still has a long way to go regarding data regulation and disclosure.

Implications/Future Research

There is much more research to be done regarding data breaches and the implications that face companies after a public announcement. It has been proven that on average companies suffer negative consequences at the initial reaction to the event, but how do investors react over a longer period? It would be worthwhile to investigate the CAR for a longer term. All the information regarding the initial announcement of the data breach might not have been fully incorporated by the end of day 1. For this reason, it would be interesting to examine a longer term CAR for evidence of a differential effect. The key would be to find a longer term time period that allows for the information of a data breach be fully

incorporated to the investors and public knowledge, but not too long that there could be more conflicting factors influencing the CAR other than the public announcement of a data breach.

It would also be interesting to investigate trends in reaction to the announcement of data breaches in the future, providing additional data that can strengthen the statistical analysis. Additionally, this would allow an investigation of whether there is any change or development in trends in reaction after 2018 when all fifty states and the U.S. have data breach disclosure regulation. How will investors react differently as they hear about data breaches in a timelier manner? It would also be interesting to also calculate longer term CARs in a few years to compare how the new data breach legislation could affect the longer term investor reaction. How long does it take stocks to rebound after a disclosure? Data security is a realm where we will see a lot of change and development in our life time, and it is important for companies to be conscientious about how they handle their data to prevent these attracts.

References

Acquisti, Alessandro; Friedman, Allan; and Telang, Rahul, "Is There a Cost to Privacy Breaches? An Event Study" (2006). *ICIS 2006. Proceedings*. 94.

Andoh-Baidoo, F.K, K Amoako-Gyampah, and K.-M Osei-Bryson. "How Internet Security Breaches Harm Market Value." *Security Costs; Privacy*. 8.1 (2010). Print.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "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*. 9.1 (2004): 70-104. Print.

Gatzlaff, Kevin M, and Kathleen A. McCullough. "The Effect of Data Breaches on Shareholder Wealth." *Risk Management & Insurance Review*. 13.1 (2010): 61-83. Print.

Kamiya, Shinichi and Kang , Jun-Koo and Kim, Jungmin and Milidonis, Andreas and Stulz, René M., What is the Impact of Successful Cyberattacks on Target Firms? (March 6, 2018). Fisher College of Business Working Paper No. 2018-03-004. Available at SSRN: https://ssrn.com/abstract=3135514 or http://dx.doi.org/10.2139/ssrn.3135514

Larson, Selena. “10 Biggest Hacks of 2017.” *CNNMoney*, Cable News Network, 20 Dec. 2017, money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

Appendix

Table 7

t-Test: Two-Sample Assuming Equal Variances		
	1st half of CAR	2nd half of CAR
	Variable 1	*Variable 2*
Mean	-0.003244543	-0.005572954
Variance	0.000426103	0.00139796
Observations	94	94
Pooled Variance	0.000912031	
Hypothesized Mean Difference	0	
df	186	
t Stat	0.528571422	
P(T<=t) one-tail	0.298866461	
t Critical one-tail	1.653087138	
P(T<=t) two-tail	0.597732922	
t Critical two-tail	1.972800114	

Table 8

t-Test: Two-Sample Assuming Equal Variances		
	1st half of CAR	2nd half of CAR
	Variable 1	*Variable 2*
Mean	0.000191818	-0.004439971
Variance	0.000615819	0.000768271
Observations	183	184
Pooled Variance	0.000692254	
Hypothesized Mean Difference	0	
df	365	
t Stat	1.686232402	
P(T<=t) one-tail	0.046302782	
t Critical one-tail	1.649039017	
P(T<=t) two-tail	0.092605564	
t Critical two-tail	1.966484596	