Journal of Finance and Investment Analysis, vol. 8, no. 4, 2019, 19-36
ISSN: 2241-0998 (print version), 2241-0996(online)
Scientific Press International Limited

Cyberterrorism and its Dramatic Impact on Insurance and Security Companies

Joshua Afshani[1]

Abstract

Cyberterrorism has come to be one of the most threatening forms of terrorism in 2019. In the face of the negative implications cyberattacks can have on affected firms and consumers, this article focuses on the flip side of the coin: I hypothesize that cyberattacks can produce abnormal positive returns for the stock prices of insurance and security companies. Heretofore practically ignored by most businesses, companies that specialize in insurance and security dealing with cyberterrorism are experiencing increased positive interest and attention. I conducted an event study analysis to investigate how the stock prices of insurance and security companies changed one day and one week after major cyberattacks on large firms. Such cyberattacks investigated range from the 2013 Yahoo attack to the globally destructive Petya Ransomware attack. Using the P-value as a measure of significance, I found that, on average, the companies realized a consistent, positive abnormal return in 11 of the 15 events one day after an attack. This evidence supported my hypothesis as investors understand that increased cyber activity results in increased cyber-awareness. Both insurance and security companies will likely increase premiums and experience higher quarterly revenues. Moreover, it was found that security companies experienced more positive, abnormal returns than insurance companies, as consumers gravitate towards security in hopes of greater protection.

JEL classification numbers: G22
Keywords: cyberterrorism, cyber awareness, cybersecurity, stock market, empirical analysis, abnormal returns, P-value

[1] University of Michigan, Ross School of Business.

Article Info: *Received*: July 24, 2019. *Revised:* August 6, 2019.
Published online: November 1, 2019

1. Introduction

Cyber-attacks are becoming one of the most threatening forms of terrorism possible. An estimated 556 million people fall victim to cybercrime annually or 12 people every second [4]. No longer are companies worried about their data being stolen physically. In this new age of the internet, companies (and everyday consumers) are now worried about their software being compromised by hackers offline. In the past decade, hackers from around the world have managed to break into the security systems of the government, hospitals, schools, and even the world's largest companies such as Yahoo, Amazon, and Microsoft. Even with the highest-leveled security systems available, companies are at risk of interrupted online service and stolen confidential information. These attacks have severe implications on the stock prices of these companies. Many researchers have found that the average loss by an affected firm is about 2% [6]. These losses are catastrophic and can lead to "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm" [7]. Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021 [7]. This could mean a 100% increase from the 3 trillion dollars in cost which occurred in 2015. Companies can lose millions from lost revenue and worker productivity, but the most threatening losses can be from the intangible costs a firm suffers with its reputation and brand. Building trust with consumers is a priority many companies rank highly. Also, direct losses can involve the loss of information that are stolen during an attack. These intangible costs are exactly why firms have underestimated the costs of security breaches in the past [6]. There is no return on investment that can be calculated. Firms must simply acquire top level security if they do not want to suffer the consequences later. Before, security was an issue that companies addressed after the fact. But now, security is something executives have to build on from the start because of the effect it has had on other companies [18].

These losses can even be life threatening. In February 2016, a California hospital was forced to pay a ransom of $17,000 in Bitcoin to retrieve stolen patient records after a hacker compromised their security system [26]. The 2016: Current State of Cybercrime Survey by RSA stated that "due to the sensitivity, level of accessibility required for patient care, and ultimately, the potential to directly threaten human life, health care systems will be particularly impacted by ransomware" [16].

Table 1: Putting Malicious Cyber Activity in Context

Criminal Action	Estimated Cost	Percent of GDP	Source
Global			
Piracy	$1B - $16B	0.008% - 0.02%	IMB
Drug Trafficking	$600B	5%	UNODC
Global Cyber Activity	$300B - $1000B	.04% to 1.4%	Various
US Only			
Car Crashes	$99B - $168B	.7% - 1.2%	CDC, AAA
Pilferage	$70B - $280B	0.5% - 2%	NRF
US Cyber Activity	$24B - $120B	0.2% - 0.8%	Various

Table 1 demonstrates the extent to which cyber-crime harms society in comparison to many of the most damaging crimes known to date. Percent of GDP impacted and estimated cost are used as metrics to calculate approximate damage to society.

Recently, the worldwide "Wanna Cry" ransomware attack affected 150 countries including factories and hospitals. This attack, occurring in May of 2017, was a sobering moment for the world on the severity of cyber-crimes. Beazley, a leading provider of data breach response insurance, found that these attacks will only increase in number in the next coming years. In their "Beazley Breach Insights" report in January 2017, they determined that ransomware attacks were four times higher in 2016 than in 2015. They also project that these attacks will double by 2017 [3]. Another Ransomware attack, Petya, affected airplanes in Ukraine, FedEx courier deliveries in Europe, and Maersk container ships in late June of 2017 [20]. New York Department of Financial Services Superintendent Maria T. Vullo, in a statement said, “Attacks such as these reinforce the critical need for regulatory minimum standards and robust cybersecurity programs, such as outlined in DFS’s cybersecurity regulation" [21]. Attacks like these only highlight the need for security programs.

According to ISACA's State of Cybersecurity Implications for 2016 survey, 461 cybersecurity managers and practitioners confirmed that the current state of cybersecurity remains chaotic. In the survey, 75% of respondents believe they will be victims of an attack and have since increased security budget for cybersecurity related technologies and training. But, most significant, is the fact that 24% of respondents "did not know which threat actors exploited their organizations" [16]. This survey illustrated the lack of global cyber awareness.

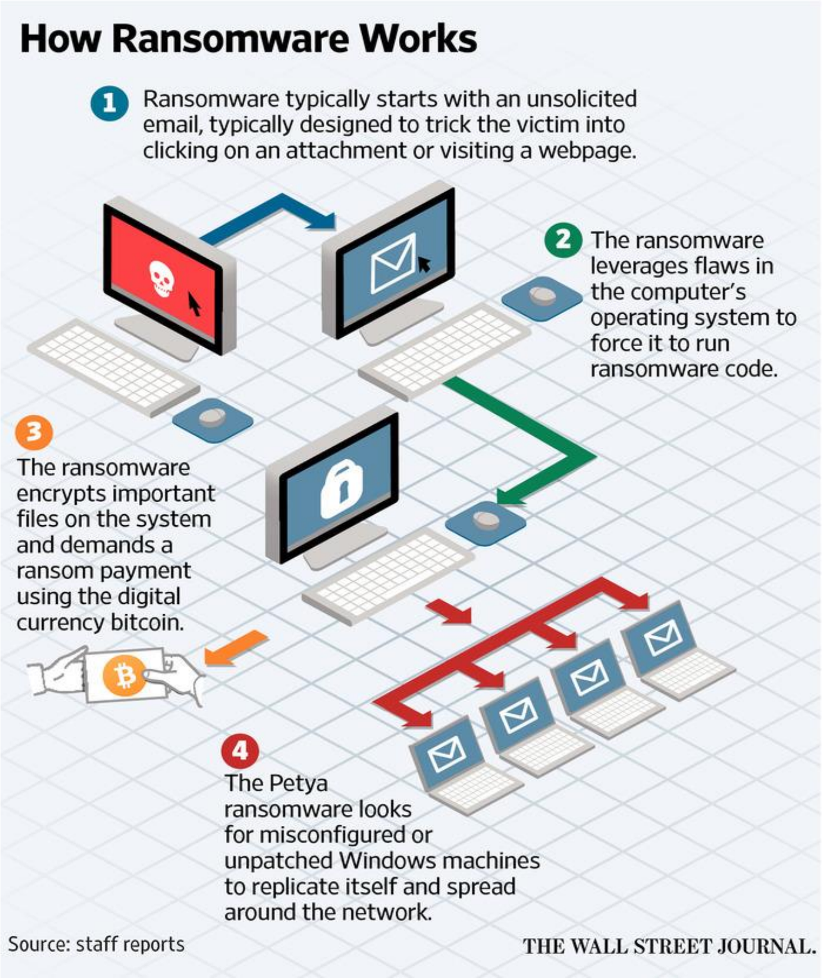

How Ransomware Works
1 Ransomware typically starts with an unsolicited email, typically designed to trick the victim into clicking on an attachment or visiting a webpage.
2 The ransomware leverages flaws in the computer's operating system to force it to run ransomware code.
3 The ransomware encrypts important files on the system and demands a ransom payment using the digital currency bitcoin.
4 The Petya ransomware looks for misconfigured or unpatched Windows machines to replicate itself and spread around the network.
Source: staff reports
THE WALL STREET JOURNAL.

Figure 1:How Ransomware Works.
Uses the Petya ransomware attack to illustrate how a ransomware attack occurs and infiltrates computer systems.

The plethora of attacks are no doubt damaging to the economy and the nation as a whole. However, two industries have been affected positively by these attacks: the cyber-insurance industry and the cyber-security industry. These include companies which insure against cyber-crimes or companies which protect against similar incidents. Before cyber-crimes had become as frequent as they are today, companies did not see a direct need for security or insurance. There was no direct payoff for companies who bought insurance and many companies did not feel a need to insure or protect against an incident which has not yet occurred. There was nothing tangible about insurance. But, now that companies are being maliciously hacked every month, insurance and security companies are now seeing the payoff and firms are buying insurance and security in fear [13]. Cyber-Insurance is the fastest-growing insurance product in the world. PricewaterhouseCoopers forecasts that the cyber-security market will increase from 3 Billion to 7.5 Billion in premiums in 2020 [22]. Global spending for cybersecurity is projected to reach 1 Trillion over the next 5 cumulative years from 2017 to 2021 [9].

The response of these cyberattacks is affecting the cybersecurity market tremendously. This paper looks specifically into the stock prices of the top cybersecurity companies before and after a major cyber breach of large corporations. With increasing and inventive cyberattacks hitting companies, CEOs and directors are forced to change their security strategies. Forbes conducted a survey with 308 executives with a range of corporations making more than 100M in annual revenue. They found that 69% of executives surveyed believe that digital transformation is forcing them to rethink their cybersecurity strategies [17]. Additionally, 64% of those executives will boost spending to protect against known security threats, and most saw that operations teams are seeing heightened accountability for security breaches. This increased need for security will aid security companies tremendously, both in revenue and in demand. More executives will need higher level security, which will in turn increase the revenue flow of security companies in the future. The cyber-security industry is changing dramatically as cyber breaches are becoming more frequent and more destructive to the economy.

2. Literature Review

There has been abundant research published by economists on the impact of cyberattacks on the targeted firm. Campbell, Katherine, et al. was one of the first articles published in 2003, which investigated 43 attacks between 1995 to 2000 looking at the targeted companies' stock price over a three-day period. Interestingly, however, they found that there was no concrete evidence that the market would have a negative reaction to a cyberattack. But, they did find that there was a stronger market reaction from attacks which specifically involved confidential information. The study concluded that investors did not consider Denial-of-Service attacks to be significant, as they are only short-term incidents which do not affect long-run profitability [5]. Nonetheless, many articles which have come out more recently have found that any cyberattack has a strong negative influence on the stock price of affected firms. It is suggested that in the late 1990s, investors did not understand the severity of cyber-crimes as they did in the later 2000s or as they do today.

Articles from Yayla, Ali Alper, and Qing Hu., using similar event methodology as Campbell, Katherine, et al. found that companies who had been hit by a cyberattack experienced negative market reactions. They investigated a number of factors including business type and type of breach, and the authors concluded that pure internet firms, such as companies like Amazon or Google, experienced higher negative market reactions than brick and mortar firms in the case of a cyber-crime. They also found that DOS attacks had a higher negative impact than other types of attacks [27]. Ettredge and Richardson also concluded that firms that had a higher dependence on the internet suffered 5% greater losses in market value than non-internet firms. [10].

Garg, et. al., investigated 22 events that occurred between 1996 and 2002. They found that, on average, the affected firms experienced a 2.7% decline in their stock price one day after the attack and 4.5% decline three days after the attack [14]. But, contrary to Yayla, et al., they found that attacks including chiefly credit card data and financial information caused the largest decline.

Perhaps the most influential paper was from Cavusoglu, Huseyin, et al. They determined that compromised firms who experienced a cyberattack lost, on average, 2.1% of their market value within two days of the event. This translates into a 1.65% average loss in market value per incident. Additionally, they found that net firms, on average, experienced additional 2.83% negative abnormal returns. This loss of market value was due to the fact that a cyberattack can lead to lost consumer confidence, lost business, and exposure to third-party liability. This could also illustrate a vulnerability within a company which also decreases investor confidence. Also, their research found that smaller firms lose more than larger firms in the event of a security breach because, usually, smaller firms have less capable security systems. But, what is most significant about this article is that this was the first paper to look into the effects of internet security breach announcements on the market value of Internet Security Developers. They found that in the two-day period after the announcement, the security developers realized a total average gain of $1.06 billion [6]. They concluded that this response was most likely due to the fact that the internet developers expected future gains from the aftershock of such incidents.

3. Hypothesis Development

After research done by many, it is almost certain that firms hit by a cyberattack realize a huge loss to their stock value. Much more interesting is how security and insurance firms are affected by these frequent security breaches. The future of security lies directly in the software capabilities these security companies have to offer. As stated earlier, in 2017, 69% of executives surveyed believe that digital transformation is forcing them to rethink their cybersecurity strategies [17]. With an increased need for innovative securities, the security companies will be seeing an increase in their revenue and possibly an increase in their premiums. Conclusively, cyber-security companies are increasing in value. With increased premiums and an increased need by corporations and people, it is apparent that cyber-security companies will have increased revenue [19]. This paper looks to find correlation between the stock prices of security companies at the time of a major cyberattack.

Also, in the incident of a cyberattack, more people and companies will feel the need to become insured. After the Wanna Cry Ransomware attack, the demand for coverage increased [23]. As these types of cyber-attacks are more widely broadcasted by the media, more people are realizing the sensibility in insuring their data. Before these attacks became global, many people and companies did not see the need for coverage. But, since major companies and even governments were compromised, people now see a need for insurance as they do not want to suffer the consequences others have endured [24]. It is logical to assume that investors will see the increased need for cyber-insurance. For the first hypothesis, I decided to look at the combined impact of both the insurance and security companies. I found a combined P-value for the 8 Insurance companies and the 11 security companies. Thus, the first hypothesis of this paper is as follows:

Hypothesis 1: The stock value of cyber-insurance and cyber-security companies increase one business day after the announcement of a cyber-breach.

This paper looks to see the immediate reaction of the market after these announcements. The stock market reaction to the news of a firm's cyber-incident is a result of the perceived impact it will make on the insurance sector in the future. But, most importantly, this paper looks to investigate the long-term effects of cyberattacks on cyber-insurance companies after the data breach as well. Unlike previous articles which only looked at the stock value immediately after a breach, this paper investigates stock prices one week after a data breach. I choose to set the limit at one week rather than one month or three months due to the fact that there are many factors which can affect the price of a stock. In a month-long period, unlimited occurrences can happen which could affect the price of the stock. Also, the fact that cyber-crimes are increasing in frequency, these chronic incidents can affect the stock price. Nonetheless, I assume that there will be no abnormal stock return a week after an announcement. My assumptions were based on that fact that after the immediate reaction from the market after a few days, the insurance companies' stock price will be ambiguous as usual. It is nearly impossible for a single event to affect a company's stock price for more than a couple of trading days. This does not mean, however, that this event is not significant. This simply means that the event will not consistently affect the stock of an insurance company a week after the announcement. But, the effects are illustrated in the growing value of the insurance industry. A study done by Markets and Markets found that the cyber-security and cyber-insurance sector is estimated to grow from USD 122.45 Billion in 2016 to USD 202.36 Billion by 2021 with a Compound Annual Growth Rate (CAGR) of 10.6% during the forecast period [8].
Furthermore, the second hypothesis is as follows:

Hypothesis 2: The stock value of insurance and security companies will be ambiguous one week after the announcement of a cyber-breach.

I decided to find the P-value of the combined security and insurance companies as I wanted to see the overall impact of the two fields as they both benefit from world-wide security breaches. But, I do realize that it is important to look at both fields individually for the purpose of clarity and precision in the results. I predict that security companies will yield higher abnormal stock returns than insurance companies because of the immediate response CEOs will have after a breach to their company. It seems that CEOs will likely look to strengthen their security after a breach rather than to pay for better insurance. I believe that investors will have the same logic and thus, the third hypothesis is as follows:

Hypothesis 3: The stock value of security companies will yield higher positive, abnormal stock returns than insurance companies after the announcement of a cyber-breach.

4. Methodology

For the purpose of this research, I define an "event" as a cyber-security breach which has been announced to the public by the companies through the media. This investigation covers cyber-crimes from October 2, 2013 to June 27, 2017. With the growing threat of cyber-crime each year, it is necessary that this paper covers the most recent crimes to get the most relevant data to investors. I first started by researching the biggest insurance companies in the world. I then started searching for the biggest insurance companies and security companies which specifically deal with cyber incidents. After finding these companies, I checked to see if they were public. Next I started to search for events that fit that categorization. I looked for incidents that were either DOS attacks or breaches which include confidential information and were involved with large corporations. With the lack of data available to me and the inaccessibility to news sources such as Lexis/Nexis, CNET, and ZDNET, I had trouble finding the largest data breaches in the past 5 years. But, using reliable news sites such as Forbes, the Wall Street Journal, CNN, and CSO Online, I found the data breaches I needed (Armerding, Taylor; Hardekopf, Bill). I only selected 15 events because, in reality, cyberattacks happen almost every week. I only wanted to demonstrate the fluctuations in stock price after a huge company such as Neiman Marcus or Home Depot were attacked. After finding when these data attacks occurred, I looked at the Public Relations website of the particular company or a major news source to see if the information was widespread. The sources are listed in the Bibliography under "Press Releases." Then, I found the exact date and announcement the company issued the information to the public.

I then matched these announcement dates with each of the security and insurance company's IPO dates to see if the company went public before the breach occurred. After, using Yahoo Finance's "Quote Lookup," I determined the stock prices a trading day before, a trading day after, and a week after the event. See Appendix A for example of data collection with data attacks against T-Mobile and The Office of Personnel Management. I decided to list the stock price before the announcement occurred to set a constant and determine if there were any abnormal returns based on the starting stock price. Unfortunately, some of the data breaches occurred on weekends or holidays. This resulted in there being no trading information on the day before, the day after, or the exact week after the breach. Thus, I had to take the stock price on the next trading day. I subsequently copied down the stock prices of the insurance companies on the three intervals for each event. After listing the stock prices of each company for each event, I found the P-value of the specific interval.

A P-Value is a statistical value which measures the significance of a certain set of data. For the purposes of this paper, I considered any value under 5% to be extremely significant and any value less than 10% to be significant.
For example, if I determined a stock price to be 63.5 the day before, and the stock price a day after was 63.7, I would determine through the P-value that there was no abnormal return. This is because the deviation from what was expected (63.5) to what occurred (63.7) was so small compared to the overall number. When looking for abnormal occurrences, economists generally only accept values under 5%. Thus, with a P-value that is so high, it is evident that there was no abnormal change in that circumstance.

To test H1, I found the P-Value associated with the day before and the day after the announcement.

To test H2, I found the P-Value associated with the day before the announcement and a week after the announcement.

To test H3, I found the P-value associated with the day before and the day after the announcement, but, I determined two values. I found the P-Value for security companies and the P-Value for insurance companies.

Lastly, it is imperative that our results reflects abnormal changes solely from that of the cyberattacks and not from standard fluctuations in the market. First, companies were checked against other confounding factors, such as mergers, acquisitions, earnings, and other significant public announcements, during an event that may affect the stock price realized by the firm. Second, and most importantly, we regressed the realized gains against the stock market. After finding the p-values, we took the significant events (exhibiting p-values of less than 5%) and did a cross analysis using another methodology known as the Ordinary Least Squares (OLS) to regress against gains made from the overall fluctuations of the market. OLS assumes that the error terms from regressions are independent and identically distributed, have a mean of zero and are homoscedastic. The Capital Asset Pricing Model (CAPM) was used to estimate the market model of each firm in the timeframe of the event, calculating what the firm would have gained or lost in the absence of a massive cyberattack. The model is calculated as follows:

$$R_{et} = R_{rf} + B_a (R_{mt}-R_{rf}) \tag{1}$$

Where: R_{et} is the expected return for firm A on date T; R_{rf} is the risk-free rate on date T, usually determined by the US Treasury Rate; R_m is the market return on date T; B_{af} is the beta or market model intercept for company A on date T. For market returns, we look at the Dow Jones, as security and insurance firms are most represented in this index.

After finding the expected return for each company at the date of the event, we correlated compared the expected returns with the real returns, finding the complete abnormal return for the company at each event. We used the Alternative Asset Pricing Model (AAPM) to compare these values. The model is calculated as follows:

$$AR_{at} = R_{rt} - (R_{rf} + B_a (R_{mt}-R_{rf})), \tag{2}$$

Where: AR_{at} is the abnormal returns for company A at time T; R_{rat} is the real return of company A at time T that was determined earlier. The abnormal return represents extent to which realized returns deviate from the returns that would expected based on the firm-specific parameters estimated for the market model on that specific date.

Thus, after regressing the potential gains and losses realized from the market, the new values were used to find the p-value of the firms from before the cyberattack was announced to one day after the attack.

5. Results

Using the daily closing stock prices of both security and insurance firms in the time-window of the event, I calculated any abnormal change through the P-value. Setting the day before the event as the basis or constant, I determined if there was a positive market reaction on the day after the attack and if the positive market reaction continued a week after. Of the 15 events I analyzed between December 2013 and July 2017, many demonstrated significance and detailed possible conclusions about the cybersecurity/insurance industry and the stock market. As stated in the Data and Methodology section, most economists use the P-Value to determine significance of an event after one day and after one week. After finding the P-Value for the events in the one-day interval, I found that, on average, *the companies listed experienced positive, abnormal market reactions in 11 out of 15 cases*. I only accepted P-Values at 5% or lower, as this is the acceptable number for abnormalcy in economics. In 11 out of 15 events, on average, the P-value for 10 of the events were under 5%, and there were 6 out of the 15 events with P-values under 1%.

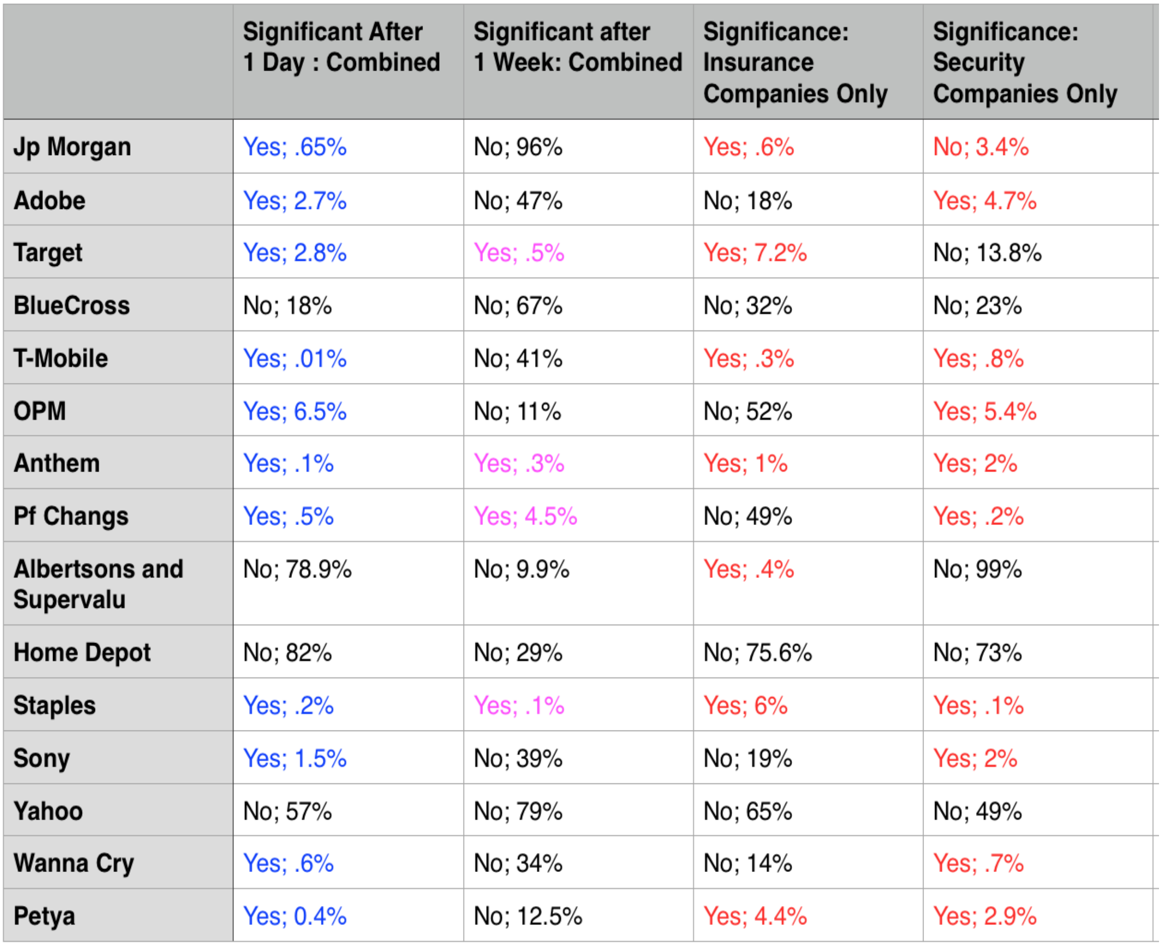
Furthermore, I used the CAPM (Capital Asset Pricing Model) to find the actual value of what each company was expected to receive based on the market (Shown in Appendix B). I therefore subtracted the real returns with the theoretical expected returns to develop the abnormal returns, and with these values, I calculated the P-Values of those 11 abnormally significant companies, and it was true that, *after regressing the returns against the market*, there were still *11/15 cases in which events received P-Values of less than 5%*. This regression technique, on average, lowered the value of significance but further demonstrates the abnormality and significance of cyberattacks on insurance and security companies.

These values illustrate very abnormal and significant results regarding the value of insurance companies after a cyberattack. I found these values to investigate the first hypothesis which states that "The stock value of cyber-insurance companies increases one business day after the announcement of a cyber-security breach." *After finding the P-Values for these different events, I find that Hypothesis 1 is supported.* The investigation was continued when I checked the stock price of the listed companies and computed the P-value a week after the attack. The results found a week after the attack and a day after the attack were vastly different. For 11 of the 15 events, there was no abnormal change in the stock price a week after the attack. For most of the events I studied, the initial abnormal change experienced by the company was quickly dissipated. But, for 4 of the events, the companies, on average, experienced positive returns even after a week. It may be that during that specific week, the market had positive gains for most of its companies or possibly because those attacks had created different reactions from investors.

Furthermore, Hypothesis two was based on the fact that the cyberattack would not consistently result in abnormal returns a week after the attack. I suggested this because, as stated earlier, the effects would not consistently show up in the stock price a week after but in the long run with reference to earnings reports and price changes. Despite a special few instances, the results found illustrate that cyber-attacks usually do not consistently increase the stock prices of insurance and security companies a week after an attack. *The P-values found a week after the events I examined support Hypothesis 2*.

Additionally, I looked at the stock prices of both security and insurance companies individually. I assumed that security companies would yield higher abnormal returns because it seems as though investors would feel more confident the security field, which is much more important to companies that insurance in the case of a cyberattack. However, my data did not find solid evidence for this hypothesis. Out of the 15 events I examined, 9 of the events found that the security companies, on average, experienced more positive, abnormal market returns in comparison with insurance companies. I took the stock of the two sets of companies and looked to find the P-Value one day after the attack to see which type of company experienced higher returns. I found that, on average, the security companies experienced positive, abnormal returns in 10 of the 15 events; however, on average, the insurance companies experienced positive, abnormal returns in 7 of the 15 events. *Thus, because of my results, I found that Hypothesis 3 is supported and that security companies yielded higher, more consistent positive abnormal returns than insurance companies.*

Table 2: Date Set



	Significant After 1 Day : Combined	Significant after 1 Week: Combined	Significance: Insurance Companies Only	Significance: Security Companies Only
Jp Morgan	Yes; .65%	No; 96%	Yes; .6%	No; 3.4%
Adobe	Yes; 2.7%	No; 47%	No; 18%	Yes; 4.7%
Target	Yes; 2.8%	Yes; .5%	Yes; 7.2%	No; 13.8%
BlueCross	No; 18%	No; 67%	No; 32%	No; 23%
T-Mobile	Yes; .01%	No; 41%	Yes; .3%	Yes; .8%
OPM	Yes; 6.5%	No; 11%	No; 52%	Yes; 5.4%
Anthem	Yes; .1%	Yes; .3%	Yes; 1%	Yes; 2%
Pf Changs	Yes; .5%	Yes; 4.5%	No; 49%	Yes; .2%
Albertsons and Supervalu	No; 78.9%	No; 9.9%	Yes; .4%	No; 99%
Home Depot	No; 82%	No; 29%	No; 75.6%	No; 73%
Staples	Yes; .2%	Yes; .1%	Yes; 6%	Yes; .1%
Sony	Yes; 1.5%	No; 39%	No; 19%	Yes; 2%
Yahoo	No; 57%	No; 79%	No; 65%	No; 49%
Wanna Cry	Yes; .6%	No; 34%	No; 14%	Yes; .7%
Petya	Yes; 0.4%	No; 12.5%	Yes; 4.4%	Yes; 2.9%

This table set illustrates the approximate P-values, or measure of abnormality and significance, for each major cyber-attack investigated. The values considered “significant” are colored in blue/pink while the “non-significant” values are left black. Also pictured is the comparison between cyber-insurance companies who yielded significant stock returns and that of cyber-security companies.

6. Conclusion and Implications

The main goal of this paper is to discuss the business implications of cyber terrorism in regards to insurance and security companies. However, another point illustrated through the findings and investigation from this paper is the importance of security for firms holding confidential information within their databases and even the everyday consumer with valued information on a laptop. There is a high vulnerability for consumers and firms alike, and their vulnerability will only increase without proper security and protection.

The findings of this article detail the impact that that will occur economically, but it also points out the change in e-commerce. As described before, with an increased awareness of cyber-crime, more companies will be paying for cyber-security. Centuries ago, no brick and mortar business was safe without locks and physical security on its store doors. In the next few years, it will be imperative that every company enlists some type of cyber-security or that company could be the victim of severe losses. With more CEOs understanding the risks of cyberterrorism, it is becoming more common knowledge cyber-security and e-commerce go hand in hand. Thus, the market is reacting as investors have been more willing to invest in security technologies. Perhaps a good extension of this paper would be to estimate the costs associated with a cyberattack on a firm, or the change in revenue and premiums that cybersecurity firms have yielded over the past years. This would involve investigation into quarterly revenues of attacked firms and security companies.

The risk of cyberterrorism is high, but it will only increase. Microsoft predicts that "By 2020 the world will need to cyber-defend 50 times more data than it does today" [7]. They estimate that by 2020 four billion people will be online - a significant increase from 2014. They predict 50 billion devices will be connected to the internet by 2020, and data volumes online will be 50 times greater than today. David Bray, columnist at the Huffington Post, reinforces Microsoft's findings when he adds that the Chief Information Officer (CIO) at the Federal Communications Commission (FCC) has said that "today there are 7 billion people, about 850 million web servers online, and about 4 billion zetabytes of digital content worldwide. By 2022 there will be 8 billion people, 75-300 billion networked devices globally and 96 zetabytes of digital content is estimated to exist" [7]. This increase in data online could result in more frequent attacks. The attacks that were discussed and researched in the article only describes damage to firms. However, more attacks could pose issues for the government and even more severe consequences for nations as a whole. An economic cyberattack could potentially disable the economy of a city, state or country. Worst-case cyberattack scenarios involve attacks on critical infrastructures, and could potentially cost insurance companies billions [25]. These risks are highlighted in the change of government funding for cybersecurity. The White House states the U.S. Government will invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget. That is up from the $14 billion budgeted in 2016. This represents a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity, a necessary investment to secure [the United States] in the future [9]. Even the United Kingdom is investing £1.9 billion in cybersecurity measures [2]. With the increasing risk of cyberterrorism in the United States, the United States Government is protecting itself against the hackers looking to terrorize its country. In addition to this increase in cybersecurity spending, the Obama administration enacted a Cybersecurity National Action Plan (CNAP) that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security [12]. Perhaps another good extension of this research would be to see how strong and protected the United States Government is against cybercrime.

Most important on this issue is the fact that firms and even individuals must understand the dangers that cyberterrorism can pose. After the 9/11 attacks, people were well aware of the need for security in the United States. Hopefully, with these severe cyberattacks, people can secure themselves, even insure themselves, against cybercrime. Especially since the worst scenarios are unknown to the population, it is imperative that awareness is increased and as many people are protected as possible. Not just for economic reasons but also for the protection of confidential information. Increased awareness could lead to increased security and therefore save many consumers and entire companies from the disasters that cyberattacks can pose. It is imperative that more people will be insured and protected against these malicious attacks. Just as airport security was strengthened after the horrible 9/11 attacks, the people of the world must focus on another type of crime that can be astronomically damaging. As the Obama Administration stated that "Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person, "the challenge of being as protected as possible is more important than ever [12].

ACKNOWLEDGEMENTS.

I want to thank my various mentors and professors along the way who have contributed to my research and growth as a student including Roger Kassebaum, Pauline Kim, Indrajit Mitra, Steve Bloom, and Michael Hakim. I would also like to thank Milken Community Schools and The Ross School of Business for their collective role in my education throughout the years. Lastly, I want to thank my parents for their unconditional love and support in my academic pursuits.

References

[1] Armerding, Taylor. "The 16 Biggest Data Breaches of the 21st Century." CSO Online, CSO, 11 Oct. 2017.

[2] Arsene, Liviu. "Economic Cybercrime: The Next Economic Crime Vector." RSA Conference, 12 Apr. 2016.

[3] "Beazley Breach Insights - January 2017." Beazley.

[4] Boden, Pete. “The Emerging Era of Cyber Defense and Cybercrime.” Microsoft, 27 Jan. 2016.

[5] Campbell, Katherine, et al. “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*.” Journal of Computer Security, **11**(3), Jan. 2003, pp. 431–448.

[6] Cavusoglu, Huseyin, et al. “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), Nov. 2004.

[7] “Cybercrime Report.” Cybersecurity Ventures, 12 Aug. 2016.

[8] “Cybersecurity Market by Solution (IAM, Encryption, DLP, UTM, Antivirus/Anti-Malware, Firewall, IDS/IPS, Disaster Recovery, DDOS Mitigation, SIEM), Service, Security Type, Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2022.” Market Research Firm.

[9] “Cybersecurity Market Report.” Cybersecurity Ventures, 2 Dec. 2014.

[10] Ettredge, Michael and Richardson, Vernon J., “Assessing the Risk in E-Commerce,” May 1, 2001.

[11] Evans, Melanie. “Cyberattack Causes Surgeons to Cancel Some Operations.” The Wall Street Journal, Dow Jones & Company, 28 June 2017,

[12] “FACT SHEET: Cybersecurity National Action Plan.” National Archives and Records Administration, National Archives and Records Administration, 9 Feb. 2016,

[13] Friedman, Nicole. “Yahoo and Other Breaches Drive Surge in Corporate Hacking Insurance.”The Wall Street Journal, Dow Jones & Company, 15 Dec. 2016,

[14] Garg, A., Curtis, J & Halper, H. (2003b). Quantifying the Financial Impact of IT Security Breaches, Information Management & Computer Security, **11**(⅔), 74-83.

[15] Hardekopf, Bill.“The Big Data Breaches of 2014.” Forbes, Forbes Magazine, 13 Jan. 2015.

[16] ISACA andRSA,State of Cybersecurity: Implications for 2016, Cybersecurity Nexus, November 2015.

[17] Joch, Alan. Enterprises Re-Engineer Security in the age of Digital Transformation. BMC

[18] Kostov, Nick, and Costas Paris. “Companies Try to Contain Fallout From Global Cyberattack.” The Wall Street Journal, Dow Jones & Company, 28 June 2017.

[19] La Monica , Paul R. “Hack Attacks = Big $ for Cybersecurity IPO.” CNN, 24 Sept. 2014.

[20] McMillan, Robert. “Cyberattack Launched for Pain, Not Profit, Experts Say.” The Wall Street Journal, Dow Jones & Company, 29 June 2017,

[21] McMillan, Robert, et al. “Cyberattacks Hit Major Companies Across Globe.” The Wall Street Journal, Dow Jones & Company, 27 June 2017.

[22] PwC, CIO and CSO, The Global State of Information Security® Survey 2017, October 5, 2016.

[23] Ralph, Oliver. “Cyber Insurance Market Expected to Grow after WannaCry Attack.” Financial Times, 16 May 2017.

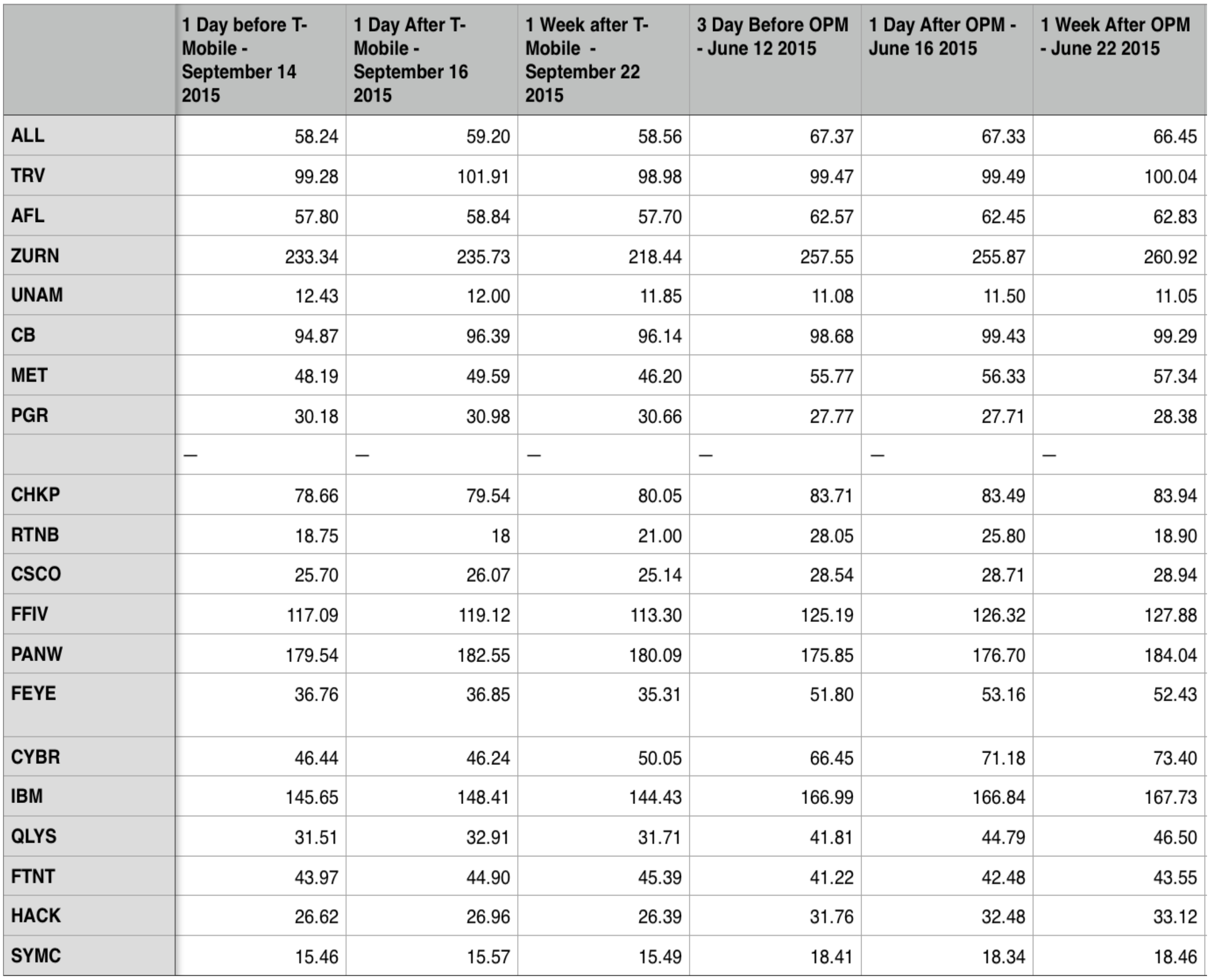
[24] Sheridan, Patrick M. “FireEye: Hot after Target Data Breach.” CNNMoney, Cable News Network, 27 Mar. 2014.

[25] “U.S. Federal Cybersecurity Market Forecast 2017-2022.” Market Research Media, Market Research Media Ltd, 2 Oct. 2017.

[26] Winton, Richard. “Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating.” Los Angeles Times, 18 Feb. 2016.

[27] Yayla, Ali Alper, and Qing Hu. “The Impact of Information Security Events on the Stock Value of Firms: the Effect of Contingency Factors.” Journal of Information Technology, **26**(1), Apr. 2010, pp. 60–77.

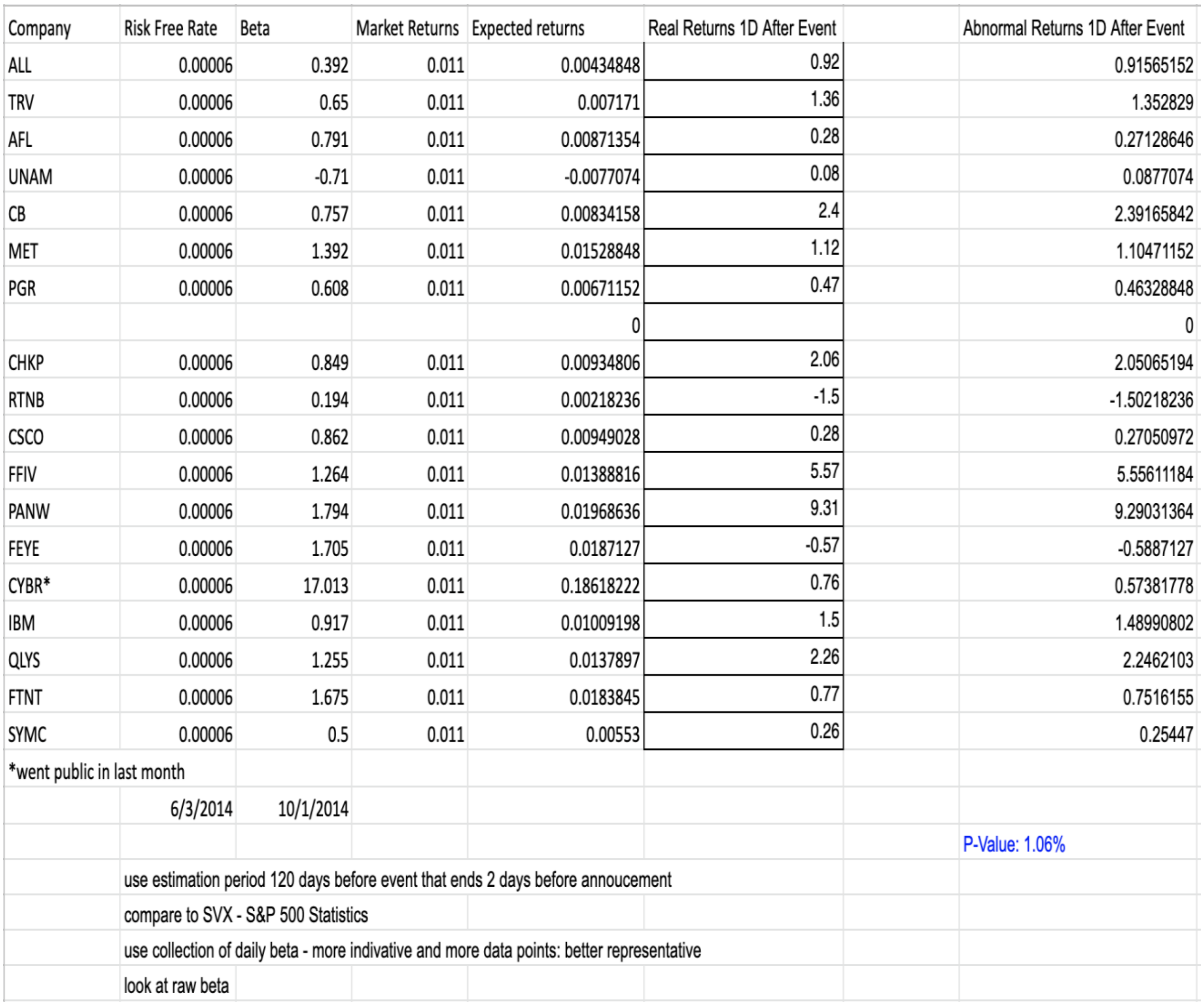
APPENDIX A:



	1 Day before T-Mobile - September 14 2015	1 Day After T-Mobile - September 16 2015	1 Week after T-Mobile - September 22 2015	3 Day Before OPM - June 12 2015	1 Day After OPM - June 16 2015	1 Week After OPM - June 22 2015
ALL	58.24	59.20	58.56	67.37	67.33	66.45
TRV	99.28	101.91	98.98	99.47	99.49	100.04
AFL	57.80	58.84	57.70	62.57	62.45	62.83
ZURN	233.34	235.73	218.44	257.55	255.87	260.92
UNAM	12.43	12.00	11.85	11.08	11.50	11.05
CB	94.87	96.39	96.14	98.68	99.43	99.29
MET	48.19	49.59	46.20	55.77	56.33	57.34
PGR	30.18	30.98	30.66	27.77	27.71	28.38
	—	—	—	—	—	—
CHKP	78.66	79.54	80.05	83.71	83.49	83.94
RTNB	18.75	18	21.00	28.05	25.80	18.90
CSCO	25.70	26.07	25.14	28.54	28.71	28.94
FFIV	117.09	119.12	113.30	125.19	126.32	127.88
PANW	179.54	182.55	180.09	175.85	176.70	184.04
FEYE	36.76	36.85	35.31	51.80	53.16	52.43
CYBR	46.44	46.24	50.05	66.45	71.18	73.40
IBM	145.65	148.41	144.43	166.99	166.84	167.73
QLYS	31.51	32.91	31.71	41.81	44.79	46.50
FTNT	43.97	44.90	45.39	41.22	42.48	43.55
HACK	26.62	26.96	26.39	31.76	32.48	33.12
SYMC	15.46	15.57	15.49	18.41	18.34	18.46

This appendix displays a small portion of the data collected to determine the significance of a cyberattack. The columns detail the dates that were investigated, and each number corresponds to the different stock prices by each security or insurance company. The rows indicate which companies were analyzed and were named based on their stock symbol.

APPENDIX B:



Company	Risk Free Rate	Beta	Market Returns	Expected returns	Real Returns 1D After Event		Abnormal Returns 1D After Event
ALL	0.00006	0.392	0.011	0.00434848	0.92		0.91565152
TRV	0.00006	0.65	0.011	0.007171	1.36		1.352829
AFL	0.00006	0.791	0.011	0.00871354	0.28		0.27128646
UNAM	0.00006	-0.71	0.011	-0.0077074	0.08		0.0877074
CB	0.00006	0.757	0.011	0.00834158	2.4		2.39165842
MET	0.00006	1.392	0.011	0.01528848	1.12		1.10471152
PGR	0.00006	0.608	0.011	0.00671152	0.47		0.46328848
				0			0
CHKP	0.00006	0.849	0.011	0.00934806	2.06		2.05065194
RTNB	0.00006	0.194	0.011	0.00218236	-1.5		-1.50218236
CSCO	0.00006	0.862	0.011	0.00949028	0.28		0.27050972
FFIV	0.00006	1.264	0.011	0.01388816	5.57		5.55611184
PANW	0.00006	1.794	0.011	0.01968636	9.31		9.29031364
FEYE	0.00006	1.705	0.011	0.0187127	-0.57		-0.5887127
CYBR*	0.00006	17.013	0.011	0.18618222	0.76		0.57381778
IBM	0.00006	0.917	0.011	0.01009198	1.5		1.48990802
QLYS	0.00006	1.255	0.011	0.0137897	2.26		2.2462103
FTNT	0.00006	1.675	0.011	0.0183845	0.77		0.7516155
SYMC	0.00006	0.5	0.011	0.00553	0.26		0.25447
*went public in last month							
	6/3/2014	10/1/2014					
							P-Value: 1.06%
	use estimation period 120 days before event that ends 2 days before annoucement						
	compare to SVX - S&P 500 Statistics						
	use collection of daily beta - more indivative and more data points: better representative						
	look at raw beta						

This Appendix displays the Capital Asset Pricing Model, the method used to regress the real returns experienced after the event with the returns these companies would have theoretically received. The above pictures are a snapshot of the computations surrounding the JP Morgan cyberattack in 2014. The expected returns were subtracted from the real returns to come to the abnormal returns which is what was used to compute the P-Value which resulted in an extremely significant 1.06%