EVALUATING THE FINANCIAL EFFECT FROM CYBER ATTACKS ON FIRMS AND ANALYSIS OF CYBER RISK MANAGEMENT

By

GANIARIDIS PANAGIOTIS

Master Thesis submitted to the Department of Economics of the University of Macedonia in partial fulfillment of the requirements for the degree of Master of Economics

THESSALONIKI, GREECE, FEBRUARY, 2018
[Special thanks to my supervisor lecturer, Mr. Livanis Efstratios, for his guidance and support throughout the writing process.]
EVALUATING THE FINANCIAL EFFECT FROM CYBER ATTACKS ON FIRMS AND ANALYSIS OF CYBER RISK MANAGEMENT

Keywords: cyber-attack, cyber risk, event study, modelling cyber risk, stock value

Abstract

In our epoch, internet is an integral part for business activity. Giant firms, like Amazon, are exclusive dependent from internet activities, while numerous other sectors, for example finance corporations, have developed online activity. Everyday online transactions produce large amount of revenue. A possible outage of normal internet operation can cause severe costs in a firm’s business. Damages can be even intangible, as company’s reputation will be questioned.

Cyber criminals are not unaware of the benefits gained from a potential cyberattack. They find vulnerable systems and expose even technology colossus such as Google.

Public is upset as countless of sensitive private data are stored in online systems and are targeted by hackers.

In this work we try to point out some tools for managing the risk emanating from a cyberattack. Furthermore, we conduct an empirical analysis to investigate the effect of a security breach on firm’s value. Our purpose is to cover the time period 2015-2017 with no relative announced studies yet as cyberattacks multiple year by year. We employed event study methodology using the single market model. Our results reveal negative impact on an affected firm due to cyberattack to the event date, although without statistical significance. Still this research field is in its infancy and we anticipate new studies with strong conclusions in the near future.
Contents

Abstract v
List of tables xi
List of charts xiii

Chapter 1: Introduction

1 Introduction 1

Chapter 2: Literature Review

2 Literature Review 3

Chapter 3: Cyber risk and management

3.1 Definition of cyber risk 9
3.2 Managing cyber risk 10
3.2.1 Modelling of cyber risk 11
3.2.1.1 Cyber insurance and determining premiums 16
3.2.2 Learning machines and artificial intelligence 18
3.2.3 Encryption data: a vital technique 21
3.2.4 The role of human behavior to cyber risk management 24

Chapter 4: Case Study

4.1 The effect of data breaches’ announcement in firm’s value: an empirical study over the years 2015-2017 26
Chapter 5: Conclusion

5 Conclusion

Appendix

Bibliography
## List of tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Cyber Risk Definitions</td>
<td>9</td>
</tr>
<tr>
<td>3.2</td>
<td>Crypto measures adopted from big firms</td>
<td>23</td>
</tr>
<tr>
<td>4.1</td>
<td>Results for full sample statistical analysis</td>
<td>31</td>
</tr>
<tr>
<td>4.2</td>
<td>Results for financial subgroup statistical analysis</td>
<td>31</td>
</tr>
<tr>
<td>4.3</td>
<td>Results for middle capitalization firms subgroup statistical analysis</td>
<td>32</td>
</tr>
</tbody>
</table>
## List of charts

<table>
<thead>
<tr>
<th>3.1</th>
<th>From Maillart and Sornette (2010)</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>A simple flow of four vertices</td>
<td>13</td>
</tr>
<tr>
<td>3.3</td>
<td>Mukhopadhyay’s et al (2013) DAG</td>
<td>14</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1 Introduction

Nowadays, economic activity is highly depended on information technology, making cyber security an integral issue for firms and governments. Furthermore huge sectors of global economy are entirely consisted of networked computer systems (for instance e-commerce companies, finance firms etc) so as cyberattacks become serious threat attracting cyber criminals.

The question how much important the electronic information and its safety is, can be responded by several reports of national organizations. In 2014, Bryan Watkins collects such reports which state that global annual cost of cybercrime surpasses $385 billion. Furthermore, beyond firms’ losses, every 1 billion is corresponded to 5080 lost jobs. Currently, a study from Allianz states that global economy suffers $445 billion every year, more than $50 billion difference than 2014.

Information technology breaches may seem hard to befall, but reality is contrasting as numerous incidents of cyberattack have been recorded in recent years. Leading companies in global economy have suffered violation of their private systems. In 2014, Google and Yahoo were hacked and users’ sensitive private information were compromised. The same year, eBay’s customers’ accounts were breached and private information was accessible to hackers. Even defense industries did not escape as Boeing was targeted and manufacturing plans of defense systems were leaked. A famous incident includes J.P. Morgan which resulted in compromising contact information of households and firms.

Cyberattack may have greater magnitude when is resulted in energy sector. Kyivoblenergo, a Ukrainian electricity distribution company, received an attack into the computer systems, on 2015. The consequences were thousands of customers to lose power as several outages happened. It is estimated that the resulted outages lasted about 6 hours. Another case of a critical infrastructure affected is Saudi Aramco, a Saudi Arabian national petroleum and
natural gas company. Its computer network was affected on 2012 and many data were deleted from the hard drives. The issue is of great importance as anything that disrupts the normal function of Middle East oil firms, has serious impact on prices and oil supplies worldwide. The United States Computer Emergency Readiness Team was alerted by the attack in order to prevent future similar incidents.

From the previous episode we can conclude that cybercrime is not restricted only on private information theft, but could cause more complex and severe problems. A second conclusion is that cyber criminals are not persons with just advanced knowledge of hacking, but experienced and well trained teams who aim well-planned targets.

So corporations should have cybersecurity as priority. Companies that realize the threat will continue to invest in cybersecurity, and by 2020 firms will have $114 billion expenditures annually.

Although there is increased need for safety in cyber space, The Law Society (the professional association that represents the lawyers’ profession in England and Wales) states that regulations have not been enacted for cyber security yet. A guide to the general data protection regulation announces the duty for all entities to report certain forms of personal data breach. The duty includes to determine the severity of the incident and report it if risk is imminent. The entity has to report it within 72 hours since the realization of the event. The report must contain a description of the nature of the personal data breach, a description of the likely consequences of the personal data breach and a description of the measures taken to deal with the personal data breach. If third party is exposed to high risk, must be informed immediately.

As a result, cybercrime and cybersecurity are now debated issues with increasing popularity over the years. The rest of this work will be divided as follows: a) in chapter 2 we sum up the existing literature about the effect of cybercrime in firms value and how severe are the costs for corporations, in chapter 3 we emphasize on measures that companies can take, in chapter 4 a case study that studies the impact of cyberattack on certain firms will be discussed. Finally, conclusions will end the work.
Chapter 2

Literature Review

2 Literature Review

Stock price is a vital factor for large companies. As big corporations compose the heart of every modern economy, their stocks are publicly traded and as a result their prices summarize the prospects of each firm. It is known generally speaking, the highest the expectations of investors for a firm’s future growth, the highest its stock price and market value.

So stock price is strictly related with firm’s value. Theoretically, the price of a firm’s stock is determined by the present discounted value of the cash flows expected to be created by firm’s output. These cash flows are the generators of shareholders wealth because will be converted into dividends.

The point that attracts researchers is whether cyberattack and security breaches can affect the stock price. In this field several studies endeavor to give an answer.

Cavusoylu et al (2004) investigate whether the change of market value of an attacked firm is linked to announcements of internet breaches. Their discussion states that several companies may be more prone to security breaches than are others. This is logical as some firms are more dependent on internet to conduct business than others and some are entirely dependent on online activities.

According to this study, the attack has a range on its severity and depends on the type of attack. Most common attack is called ‘denial of service’ or DOS. DOS is not expected to make lasting damage on firm’s system. This type of attack has the ability to interfere in the interior computer system and deter the online activity of business. A more serious type is the one which violates individual information and involves the theft of personal data.

The study continues making five hypotheses regarding the repercussions of a cyberattack. It collects a sample of 66 incidents, including 34 DOS events. Researchers observe that firms which suffered a cyberattack experience 2.1% decline in market value. So the announcement
of an internet security breach is negatively associated with the market value of the announcing firm.

Moreover, firms that are more related with internet business suffer more losses than traditional ones, 2.8% compared with the others firms that were studied. This is a logical conclusion as their revenue is derived mostly from internet activity.

Size of the firm was an important variable as smaller firms suffered larger losses than bigger ones. The authors attribute this observation to investors’ expectations. Once a company is attacked, investors find smaller firms more vulnerable to a future attack than larger ones.

A contradictory result is that the type of attack does not matter for the costs resulted whereas we would expect DOS to cause less losses. It seems that investors regard every category of attack as an overall failure of firm’s security system no matter the type.

On the other hand, security companies enjoy 1.4% rise of their market value. No one can disagree that internet firms invest in security to prevent future attacks and this explains the above rise.

A pioneer study to the field was conducted by Ettredge and Richardson (2002), who examined the reaction of capital markets due to the DOS attacks to internet companies in February 2000. The firms were split into two categories, one with traditional firms and the other with more dependent internet firms. In general all firms faced negative returns. Furthermore, the more dependent internet firms experienced on average 5% more losses than traditional ones. However Pirounias et al state that the above study was limited in sample selection and emphasized in a very narrow timeline. Thus generalization of findings is not safe.

Garg et al (2003) categorized the attacks in four different types: DOS, theft of credit card information, theft of other personal information and website destruction. All the aforementioned attacks caused losses in stock value. DOS resulted in about 3.5% drop on the third day. Theft of financial information, including credit card details, resulted in almost 10% drop on the first day and the drop reached 15% in three days. Theft of non-financial information resulted in about 1.5% decline after three days whereas destruction of website caused almost 1.2% again after three days. The researchers state that all kind of attacks caused a decline of almost 3% in the stock price of attacked firms relative to the market in the first
day. After three days of the attack corporations experienced a decline of 4.5% relative to the market. They also underline the existence of correlation between the number of credit card that were compromised and the magnitude of variation on the stock price.

Campbell et al (2003) investigated the effect of 43 attacks in 38 firms between 1995 and 2000. They found significant, modest though, drop of the stock prices of attacked firms relative to the market. They separated the attacks in those that included unauthorized access to confidential information and those that did not. It was noticed that the first type of attack caused larger decline. The latter resulted in decline of stock price that was insignificant. Thus, the authors concluded that investors do not expect DOS to be harmful for firms so expectations are not negatively influenced.

Hovav et al (2004) focused on virus attack announcements. They selected this type of attack as the damage resulted by that can be linked with billions of dollars in losses. Two hypotheses were tested: one whether an announcement of a virus attack of a company caused decline in stock price on the first day, and whether the overall sample exhibited negative returns for the event period. 186 incidents constituted the sample. The surprising fact was that abnormal returns for both assumptions were positive and insignificant. The authors argue that damage from virus attacks is anticipated from investors and market incorporates this information into the stock value. Thus market does not penalize the attacked firms and no incentive is created for security investments. However, almost half of the firms experienced negative abnormal returns after 25 days of the announcement.

Ko et al (2006) differs their work from previous ones using not event study methodology but comparison analysis to evaluate the financial performance of breached firms. The authors examined different ratios, sales etc. for both breached and non-breached firms over four quarters. Rather mixed results were found. Breached firms’ performance did not decrease apart from return on assets ratio that decreased in third quarter. Non-breached firms exhibited much better performance than breached ones, although breached corporations demonstrated higher sales in fourth quarter. The above work showed that a security breach can cause no lasting harm. It seems that hacked companies decide to invest in security technology and investors do not penalize them long term.

Ko et al (2007) repeat their work using the same methodology as previously. They introduce six performance ratios (excluding some from their study in 2006), and build six assumptions
testing whether decline (or increase for cost ratio) is noticed to each ratio due to a security breach event. Additionally, the performance of breached firms compared with the non-breached one is expected to be worse. Again, it was found that performance of breached firms was good enough to recover the negative impact of the event. Moreover, a conclusion that breached firms outperform their previous situation in order to compete with the non-breached ones was reached. According to the study, the outperformance is justified by the willingness to regain investors’ trust.

A different approach is introduced by Zafar et al (2012). Whether there is intra industry information transfer effect from a breached announcing firm to a non-breached competitor in the same industry is investigated. Contagion (the performance of breached firm is in the same direction with the non-breached one) and competition effect (the performance of breached firm is in the opposite direction with the non-breached one) are the types of information transfer. It was resulted that competition effect was not supported and contagion effect was supported in few cases.

Event study methodology is the work employed by Goel et al (2009). Their goal was to detect market reaction when a security breach is announced. Single market model and three factor Fama–French model were applied. The sample was one of the largest among relative studies, including 105 breached firms. The results supported statistically significant negative cumulative abnormal returns around the incident date for both models used. The researchers propose that affected firms should quantify the resulted losses and increase security.

Andoh-Baidoo et al (2006) deviate from the standard regression analysis, and introduce a decision tree induction method to examine the link between firm and attack characteristics and the presence of cumulative abnormal return. They found that the type of attack and firm characteristics play important role to determine cumulative abnormal return. By the time the study had been made, it was the first to support that both firm and attack characteristics were determinants of cumulative abnormal return.

Das et al (2014) compute cumulative abnormal return following standard event study methodology and using capital asset pricing model. The researchers highlight capital invested, firm type (internet specific/non internet specific) and severity of damage (without quantification though) as determents of cumulative abnormal return. They reached to several conclusions including: attacks with serious impact (theft of confidential information) caused
higher negative cumulative abnormal return, e-commerce firms attacked by DOS suffered more in comparison with firms from other sectors, if a vendor firm is hit then its client exhibited significant negative results and finally smaller and internet specific firms exhibited the largest cumulative abnormal return compared with the rest sample. One would normally expect the smaller firms to be more vulnerable in a security breach but the study found the opposite result.

Bolster et al (2010) examine the assumption for negative abnormal return if a security breach is announced. Further hypotheses were that the source which reports the breach influence the abnormal return as well as firm’s characteristics. Event study methodology using single market model was employed. The conclusion was that there was statistically significant negative influence on an affected firm’s value, if the incident was announced in a major media outlet (Wall Street Journal, New York Times, Washington Post, and Dow Jones News Retrieval Service).

Gatzlaff et al (2010) created a sample of 77 incidents. They found that data breaches caused significant negative returns to all sample. Specifically, the average cumulative abnormal return for 77 incidents was -8.4%. Firms with future growth prospects suffered more losses. Moreover, consequences of data breaches are more severe in small firms relative to larger ones. Pirounias et al state that the aforementioned authors did not compose the sample with latest incidents and as a result in previous years, security breaches incidents were considered of little importance.

Patel (2010) examined a narrow sample of 34 incidents, which include theft credit card information and compromised social security numbers. He tested three assumptions which took into consideration the cumulative abnormal returns: a) firms with permanent lost data suffer greater losses relative to ones with temporary lost data over short-time period, b) the same as previous over long-time period and c) smaller firms face greater losses compared with larger ones. The cumulative abnormal returns were calculated over 3, 8 and 30 days event windows. Only the second case exhibited significant negative abnormal returns and the author ends up rejecting assumptions a and b. Furthermore, results dealing with the type of compromised information and the size of the firm were not significant and the third hypothesis was rejected as well. The researcher explained that market may not be alerted to
absorb the information about hacking rapidly, raising issues about the consistency of efficient market hypothesis.
Chapter 3
Cyber risk and management

3.1 Definition of cyber risk

Cyber risk has been defined by many researchers. The several definitions are summarized in the panel below:

Table 3.1
Cyber Risk Definitions

<table>
<thead>
<tr>
<th>Authors</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cebula and Young (2010)</td>
<td>Operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems.</td>
</tr>
<tr>
<td>Hua and Bapna (2012)</td>
<td>Cyber risk emanates from cyber terrorism: attacks implemented by cyber terrorists via information systems to (1) significantly interfere with the political, social or economic functioning of a critically important group or organization of a nation, or (2) induce physical violence and/or create panic.</td>
</tr>
<tr>
<td>Mukhopadhyay et al. (2013)</td>
<td>Risk involved with malicious electronic events that cause disruption of business and monetary loss.</td>
</tr>
</tbody>
</table>
Moreover, World Economic Forum (2012) has defined cyber risk as ‘the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.’ whereas CRO forum (2016) as ‘cyber risk covers:

• Any risks emanating from the use of electronic data and their transmission, including technology tools

such as the Internet and telecommunications networks.

• physical damage that can be caused by cyberattacks.

• fraud committed by misuse of data.

• any liability arising from data use, storage and transfer, and

• the availability, integrity and confidentiality of electronic information be it related to individuals,

companies or governments.’

Finally Swiss Re (2014) gives the following definition ‘Any risk emanating from the use of electronic data and their transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud committed by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information—be it related to individuals, companies, or governments.’

### 3.2 Managing cyber risk

In general, experts and academic staff agree that there is need of an effective quantitative approach of cyber risk analysis. Professionals are now working on developing new techniques of modeling, a relative new research field.
3.2.1 Modelling of cyber risk

Modelling cyber risk is a challenging task due to limited data and not so much research has been done so far. Nevertheless some researchers have tested frequency and severity modelling by applying extreme value theory and the peaks over threshold method.

Frequency and severity method is popular among insurers. It is an actuarial method for determining the expected number of claims that an insurer will receive during a given time period, and how much the average claim will cost. Frequency refers to the number of claims that an insurer expects to see. High frequency means that a large number of claims is expected to come in. Severity refers to the cost of a claim, with high severity claims being more expensive than average estimates and low severity claims being less expensive than the average.

Extreme value theory measures the probability that a data point that deviates significantly from the mean will occur. It is useful in insurance to measure the risk for unlikely events, in our case cyberattack. In particular, peaks over threshold method defines an overall threshold, extracts all points above that threshold and develops a distributional model for these points. Eling et al (2015) use the above method and select several distributions such as Exponential, Gamma, Generalized Pareto Distribution, Log-normal and Weibull. They apply goodness of fit analysis and the Generalized Pareto Distribution proved to be the best distributional model.

Estimating a linear model for frequency and severity distribution was the work employed by Maillart et al (2010). They examine personal data breaches and find that the frequency of such incidents have been exponentially growing in the period from 2001 to 2006(panel A). Furthermore the severity per incident can be plotted in a heavy tailed distribution (panel B). One drawback that should be underlined is the confined set of data but the authors claim that this type of data used in the work is a representative one for other types of cyber risk.
Another method was a copula aided by Bayesian Belief Network employed by Mukhopadhyay et al (2013). Their purpose is to aggregate cyber risk and calculate a potential risk premium for cyber insurance. Concept of copula presents the advantage to calculate any possible marginal distribution and elucidate non-linear dependencies.

In general a Bayesian Belief Network (BBN) is a directed graphical model that captures a subset of the independence relationships of a given joint probability distribution. Each BBN is
represented as a directed acyclic graph (DAG) together with a collection of conditional probability tables. A DAG is a directed graph in which there is no directed cycle. In a BBN, each node in the directed graph corresponds to a random variable and each directed edge represents a statistical dependence. In addition, each node is associated with a conditional probability distribution of the corresponding random variables given its parents in the DAG. Node j ∈ G is a parent of a node i ∈ G if there is a directed edge from j to i in the graph G. We say that a joint probability distribution factorizes with respect to the directed graph G if,

\[ p(x_1, \ldots, x_n) = \prod_{i \in V} p(x_i | x_{\text{parents}(i)}). \]

**Chart 3.2**

**A simple flow of four vertices**

A directed graph with four vertices A, B, C, and D. If \( p(x_A x_B, x_C, x_D) \) factorizes with respect to G, then we must have:

\[ p(x_A x_B, x_C, x_D) = p(x_A) p(x_B | x_A) p(x_C | x_B) p(x_D | x_C) \]
Mukhopadhyay’s et al (2013) DAG

Mukhopadhyay’s DAG is consisted from 20 random variables. Each random variable has a marginal cumulative distribution function. A joint cumulative distribution is computed, the so called copula function.

Copula is a function that describes dependencies among variables, and provides a way to create distributions that model correlated multivariate data.

Let

\[ F_X(x) = P[X \leq x] \]

and
\( F_2(y) = P[Y \leq y] \)

be cumulative distribution functions of the random variables \( X \) and \( Y \) and let

\( F(x, y) = P[X \leq x, Y \leq y] \) is their joint distribution.

Then mathematical theory says that under fairly general conditions there is a unique function \( C \),

such that (1) \( F(x, y) = C(F_1(x), F_2(y)) \),

\( C \) is called a copula function.

Thus if one knows \( C \) the joint distribution \( F(x, y) \) can be derived from the marginal distributions \( F_1(x) \) and \( F_2(x) \).

Denoting the probabilities \( u = F_1(x) \) and \( v = F_2(y) \), we can take \( x = F_1^{-1}(u) \) and \( y = F_2^{-1}(v) \).

Then

(2) \( F(x, y) = F(F_1^{-1}(u), F_2^{-1}(v)) = C(u, v) \) is a copula (Sklar’s theorem).

A Gaussian copula is:

(3) \( C(u, v) = \Phi_\rho(\Phi^{-1}(u), \Phi^{-1}(v)) \) where

\( \Phi_\rho \) is the bivariate standard normal distribution function with correlation \( \rho \), \( \Phi \) is the standard univariate normal distribution.

The authors use the Gaussian copula to measure the number of security failure and the costs given in order to create an overall loss distribution on a cyber risk portfolio.

Bohme et al (2006) start with an attempt to aggregate the correlated marginal distributed cyber risks. Correlation can be found within the entity of the firm, for example among its multiple systems, and within insurer’s risk portfolio that contains risk from multiple firms. This is important because risk premium is going to be affected due to global correlation. The researchers use the t-copula to model the correlations among a global insurer’s portfolio but were hesitant about the suitable copula due to limited data.
3.2.1.1 Cyber insurance and determining premiums

Once cyber risk is effectively modeled and measured, the results can be used to compute cyber insurance premiums. Actuarial calculations and historical data are fundamental sources for pricing premiums but still there is lack of them, making pricing questionable. Nevertheless, few researchers seek to design a model for estimating premiums.

Herath et al (2011) follow some steps to achieve their goal. Firstly, they introduce a loss function for a corporation: \( \Pi = g(\pi, q) \) where \( q \) is the number of affected computers and \( \pi \) is the observed dollar losses. \( \Pi \) depends on random variables \( \pi, q \) and is built using copula. Secondly, a binary variable \( \omega \) is used with values 1 if an incident has transpired or 0 if not. Thirdly, \( T \) represents the time till the contract is paid. After that, the following function is introduced:

\[
\alpha_1, \text{ if } q<l \\
\Pi = g(\pi, q) = \alpha_2 + [(q-l)/q]*[\pi/10], \text{ if } l\leq q < m \\
\alpha_3 + [(q-m)/q]*[\pi/10] \text{ if } q \geq m
\]

where \( l \) and \( m \) are the lowest and the highest limits of the number of possible affected computers and \( \alpha_i, i=1,2,3 \) are constants.

[From Herath et al (2011)]

Then a Monte Carlo simulation attributes jointly distributed values. Cost of cyber insurance is given by: \( C = \omega e^{rT}P \) where \( P \) is the amount paid by the insurer in the case of a breach and \( r \) is a discount rate. Premium is therefore calculated by:

\[
E(C) = E(\omega)*E(e^{rT})*E(P) , \text{where } E(\omega) = \text{Prob}(\omega=1)
\]

Insurers will add an additional amount to the premium that represents some expenses and profit.

The above copula approach is reliable when large amount of data is available in order to determine the appropriate copula. Gordon (2003) and Hareth (2011) point out the scarcity of data due to limited publications by affected firms.
Cyber insurance could serve as a solution to cyber threats. Bolot et al (2008) build an expected utility to model in an attempt to measure the utility gained by a network of agents when they invest on insurance products. Their work discusses that a chain of agents that face correlated interdependent risks will gain augmented benefits if they choose to invest. Kesam et al (2004) mention self-protection (investment on information technology security systems), self-insurance (the firm itself saves an amount to cover potential cyber losses) and cyber insurance as different ways to face cyber risk. Their analysis state that cyber insurance and self-protection are complements and both are needed. But self-insurance is likely to create moral hazard issues because firm needs to choose effectively the right amount of fund for save. This decision may prove costly from the perspective of time and effort dedicated, and moreover it is possible more funds to be kept constant than the optimal (further costs will be created as those funds could be used for greater capital returns). Even self-protection can cause moral hazard issues despite being necessary because it may be costly for a firm to continuously invest and update safety systems. Thus cyber insurance should be prior.

On the other hand, Bandyopadhyay et al (2009) argue that existing information asymmetry between contracts is an obstacle to the development of market insurance. Insurers charge higher premiums due to information asymmetry and insured companies are burdened beneath the optimal. Adverse selection is a typical problem according to Hedrick (2007) that delays cyber insurance growth. Insurers require to conduct an information security audit before designing the product.

Several managers need to revise their perspective for cyber insurance (Kirkpatrick, 2015). Contracts with general liability insurance regard only physical damages and this is what managers underestimate. A cyberattack can cause intangible losses and thus normal contracts do not cover it.

Insurers are not unaware of the demand for cyber insurance products and design several insurance policies. Marotta et al (2015) summarize some of the existing policies. Coverage is offered for loss or damage to digital assets, business interruption, cyber extortion, and theft of money and digital assets. In addition if third party (customers) are affected, insurers provide coverage for loss of third-party data, security and privacy breaches, computer forensics investigation, third party contractual indemnification and multi-media liability. Further cyber insurance products are directed for specific areas such as medical field. Perakslis (2014)
warns for the perils arising from a cyberattack to a medical center as its infrastructure is critical for caring patients.

### 3.2.2 Learning machines and artificial intelligence

Artificial intelligence is a field that centers the efforts to develop systems that outperform human decision making. Experts expect from these systems to accurately predict the economy or analyze credit risk. Trippi et al (1992) summarize the applications of neural networks and predict their future growth. Similarly Wong et al (1998) highlight their rich usefulness in applications in the list below:

- Bankruptcy prediction of firms
- Stock performance/selection prediction
- Bankruptcy prediction of banks/thrifts
- Bond trading
- Commercial loan application analysis
- Financial distress forecasting
- Real estate appraisal
- Bond rating
- Credit evaluation
- Futures price forecasting
- Initial public offering pricing
- Security performance prediction
- Capital market index forecasting
- Checking account overdrafts
- Construction contract bond claims prediction
- Corporate health estimation
- Federal reserve decision-making
- Financial statement analysis and interpretation
- Future options hedging
- Future options pricing
• Future spot rates prediction
• Futures trading volume forecasting
• Insurance problem examination
• Interest rate prediction
• Intermarket analysis
• Loan evaluation
• Loan payment default classification
• Mortgage prepayment rate prediction
• Mortgage-backed security portfolios management
• Mutual fund net asset value forecasting
• Optimal stock portfolio selection
• Portfolio management
• Residential property values evaluation
• Stock market holding period return investigation
• Stock market volatility forecasting
• Stock's systematic risk forecasting
• Treasury bond market prediction

We will focus on the support provided for cyber risk management.

Despite the human efforts on cyber risk analysis with conventional tools, virtual artificial intelligence analyst are being developed with the task to predict cyberattacks. Computer Science and Artificial Intelligence Laboratory of MIT created a system that receives inputs from human experts, analyses data using clustering algorithms and ends up predicting 85\% of cyberattacks.

Liebergen (2017) further discusses the approach of machine learning techniques and its role in finance. Machine learning can be achieved through a special way. Firstly, complex data are analyzed with advanced existing statistical tools and models but without adopting restricting assumptions for the variables. The ‘unsupervised’ technique, as it is called, uses the algorithm thousands of times with the task to detect complicated patterns in the analysis of cyber risk.
Financial firms have increased urgency to adopt this kind of machines in their businesses. They are obliged to assemble extended and unstructured data. Especially after the economic crisis of 2007-2009, stricter regulations have been introduced which demand reports with detailed data (guarantees, capital levels, monetary deposits, liquidity measures). Machine learning offers analytical tools to handle massive amounts of data.

Machine learning has been already tested in some real cases. Credit card frauds are faced wielding monitoring systems when a payment is taking place. In a previous time, the monitor system analyzed high frequency of credit card transactions data and displayed a historical business dealing dataset. It then determines whether the payment is suspicious, and if yes, blocks it.

Adamson (2016) in a panel discussion explained some adversities of systems based on rules. Additionally, Tiffin (2016) argues for the efficiency of conventional analysis tools because they target to crystalize the causality between variables but fail to make predictions. Instead, learning machines are able to distinguish complicated patterns of transactions from multiple sources and thus are capable of making decisions without human intervention.

There is another field that learning machines can serve financial institutions: scrutiny for market infringements by insider traders. Traders who violate market rules can cause significant intangible costs related with firm’s reputation. Learning machines are able to decode trader’s behavior analyzing integrated trading portfolios. They form a ‘behavior picture’ for each trader according to past investing choices, preferences and other behavioral information including phone calls, signing checks and e-mails. The system is further aided with behavioral patterns borrowed from other sciences such as psychology and judges the normal human behavior. Once the behavioral pattern is designed, the system can determine whether there are suspicious diversion from normal behavior. A practical obstacle is the assemblage of the inputs as they must be recovered from multiple sources, in most times from various different databases. Moreover, there is growing critique for ethical purposes. The system uses for inputs sensitive private data that should accessible only to the owner. Opponents argue that if the system provides false signal, responsibilities are raised due to violation of privacy. The Law Society criticizes the vast collection of private data, even if this is done for security reasons. Monetization of personal data and misuse of personal information puts privacy into question.
We ought to underline the overfitting problem linked with learning machines. Everitt (2010) defines overfitted model as a statistical model that includes more parameters that can be justified by the data. Overfitting is a phenomenon that often emanates from extremely complex models. Breiman (1994) is the first to introduce ‘bootstrap aggregation’ or else bagging technique. It is a machine learning ensemble (ensemble refers to multiple learning algorithms) algorithm which confronts overfitting. The algorithm is asked to run multiple times a model with slightly different subsample data each time. The purpose is to generate a final model which is an average approximation of the previous runs.

Deep learning machines follow the evolution of learning machines. They are based on neural networked systems (neural networks mimic to some extent the processing characteristics of the human brain) and exhibit marvelous results but still there are some barriers. Najafabadi et al (2015) demonstrate some typical problems. Firstly, there is difficulty in operating non-stationary and continuous data. Rogue patterns are expected to change through brief time and algorithms need to handle streaming data. Zhou et al (2012) introduces the so called ‘denoising’ autoencoders to cope with this problem. An autoencoder is an artificial neural network which tries to encode a set of data. A ‘denoising’ autoencoder isolates features from depraved input which are robust to noisy data and forms new patterns.

Secondly, high dimensional data limit the value and rapidness of learning process. The problem of having more variables than observations still confuses the systems and unfortunately analysis of high dimensional data is infant. Nevertheless, Chen et al (2012) employ marginalized stacked ‘denoising’ autoencoders which improve the training process by isolating noise and avoiding stochastic gradient descent (stochastic gradient descent is a stochastic approximation of the gradient descent optimization for optimizing a function consisted of many differentiable functions (from Stanford.edu)). These type of algorithm reduces the computational costs and speeds up the process.

### 3.2.3 Encryption data: a vital technique

Data encryption is a method that firms can adopt to reduce cyber risk. It is a technique that encodes part of data in such a way that only authorized individuals can access them using a key.
According to a survey published by Sophos.com, many corporations guarantee their customers’ sensitive information by encrypting but are not similarly concerned for their employees’ data. More specifically employees’ bank data are not encrypted for 31% of firms asked and HR records are encrypted by only 57% that store them. It is distressing that 60% of firms report that not all documents and files created by employees are encrypted. A nearly 30% neglect to encrypt their financial documents and 41% their intellectual property. Among the reasons why firms avoid encryption are pessimism about the effectiveness, lack of law pressure and hierarchy of budgets for operating goals.

Electronic frontier foundation, a nonprofit organization, released in 2014 a survey asking several big companies for their crypto measures. The National Security Agency run a program that gained access to communications inside on companies’ system through the fiber-optic lines. Companies were asked what crypto technologies have already developed and whether they intend to adopt more. Dropbox, Facebook, Google, Microsoft, Sonic.net, Spider Oak, Twitter, and Yahoo run five of the best crypto technologies while some giants such as Amazon and AT&T need to make further improvements. The table below summarizes the results:
Table 3.2

Crypro measures adopted from big firms

<table>
<thead>
<tr>
<th>Company</th>
<th>Encrypts data center links</th>
<th>Supports HTTPS</th>
<th>HTTPS Strict (HSTS)</th>
<th>Forward Secrecy</th>
<th>STARTTLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>undetermined</td>
<td>limited</td>
<td>X</td>
<td>undetermined</td>
<td>X</td>
</tr>
<tr>
<td>Apple</td>
<td>undetermined</td>
<td>(Cloud)</td>
<td>X</td>
<td>undetermined</td>
<td>(mac.com, mac.com)</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>undetermined</td>
<td>undetermined</td>
<td>X</td>
<td>(att.net)</td>
<td>X</td>
</tr>
<tr>
<td>Comcast</td>
<td>undetermined</td>
<td>undetermined</td>
<td>X</td>
<td>(comcast.net)</td>
<td>X</td>
</tr>
<tr>
<td>Dropbox</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foursquare</td>
<td>undetermined</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinkedIn</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySpace</td>
<td>undetermined</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sonic.net</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tumblr</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verizon</td>
<td>undetermined</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WordPress</td>
<td>undetermined</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo</td>
<td></td>
<td>X</td>
<td></td>
<td>planned 2014</td>
<td></td>
</tr>
</tbody>
</table>

Note: "X" indicates adoption or implementation of the feature, and "undetermined" indicates uncertainty about adoption.
According to Nordquist personally identifiable information is the first type of data that must be encrypted. This kind of information can be found in every gadget an employee uses, such as tablet, laptop and phone. The other critical kind of information is confidential business intellectual property. Customer information, research and development data, product releases information and financial reports are potential targets that should be well guarded.

### 3.2.4 The role of human behavior to cyber risk management

According to Pfleeger et al (2011) investing on the latest technologies in not adequate for mitigating cyber risk. Along with the most advanced systems, human behavior is a crucial factor for handling cyber threats. Studies state that individuals may be unwilling to launch the internet security measures due to the complexity that emanates from system’s operation. They even may be skeptical for the necessity and the effectiveness of security systems. They end up mistreating the system or staying dormant on purpose. In some cases firms run programs to execute the security safety algorithms and systems but researchers point out that it is prerequisite human training from young ages. Individuals must be trained to be responsible and trustworthy.

Behavioral science can assist to decode human behavior for how trust and responsibility is rooted in human brain. Then programmers must contain the human element in the development of a system. For example behavioral science indicates how human should interfere with the system: human brain is more effective in remembering constantly changing motives than remembering one password, or it is easier to recognize a pattern than to recall it from many similar ones. These findings have already been used to develop authentication systems (Lamande 2010).

Pfleeger suggests further aspects that should be taken into consideration when systems are designed:

- Individuals tend to be ultra-careful when the negative consequences are concrete and not abstract
- Individuals tend to be logical and conscious when are motivated to be careful. Potential motivation could be anxiety and fear.
Cognitive dissonance occurs when human brain filters two contrasting thoughts about the person itself. This can lead the person to adjust or change its behavior. If a system exposes the person, whereas the person thinks that this should not happen, it is likely the person to review his stance.
Chapter 4

Case Study

4.1 The effect of data breaches’ announcement in firm’s value: an empirical study over the years 2015-2017

In economics, it is often to use event study analysis to assess the change on a firm’s value due to an important economical event. It is a statistical method that quantifies the magnitude of an event on stock prices. The basic idea is to find the abnormal return attributable to the event being studied by adjusting for the return that stems from the price fluctuation of the market as a whole (Gilson et al (1995)).

We are going to describe the structure of our event study following the analysis of MacKinlay (1997). We are interested in capturing the effects of security breaches announcement in stock prices, thus in firm’s value. The first important decision is the length of the event window. It is natural to include the day of the announcement and the day after that. Whatever the event is to cause change in prices, it should be reflected the day of the announcement according to efficient market hypothesis. Thus we assume a semi-strong efficient market where all publicly information is immediate reflected.

Several researchers suggest including large event windows so as to capture the long term consequences of the event on prices. However some others, like Pirounias et al (2014), claim that large event windows may coincide with important events beyond the one being investigate, and invalid results may occur.

In our case we will use the following event windows: [0,0] event day, [-1,0] one day before the event, [0,1] one day after the event, [-4,4] four days after and before the event. The windows prior to the event are used to investigate whether the market absorbs the information in advance and pre event returns are created due to insiders’ information.
4.2 Data selection

Defining the sample is another crucial task. Studies characterized as cornerstones select small samples due to scarce data and limited announced events, for instance Hovav et al (2003). However Pirounias et al (2014) underline the necessity of forming a sample consisted of at least 50 events. As far the distribution of the population of abnormal returns created by security breaches is unknown, there is need of applying the central limit theorem. For example Livanis et al (2012) fulfill this obligation with over 500 incidents between 2001 and 2011. For this reason our sample is consisted of 60 events.

Furthermore it is logical to assume that events are independent of each other so as the occurrence of one event has no influence on the next event. The independence assumption may be violated if events concerning the same firm and happened at the same time are included in the sample. Thus, the sample is consisted of events concerning different firms.

Finally it is natural to believe that the sampling distribution will be normally distributed.

The incidents cover a time period between 2015 till 2017. It is a time period which aggregates the most severe and numerous events, like Anthem and Equifax cases. Although the selected period includes some of the biggest data breaches in history, it has not been studied yet. The absence of related work during this period guides us to select the aforementioned years.

All events were collected from breachlevelindex.com, a large public data breach database. Furthermore, all cases were confirmed from reports published by non-profit organizations like Privacy Rights Clearing House or by government attorneys or by related credible sites. All the confirmation sources are listed in the table after conclusions.

The sample includes the following types of breach: account access, nuisance, and identity theft. These could be resulted by either malicious outsider or insider or accidentally. In contrast with previous studies that focus on specific type of security breaches, for instance Hovav et al (2003) deal with only virus attack, we believe that every case, that puts in question the safety of personal and private information, can harm the goodwill of the breached firm. For that reason we did not restrict our sample only to big data leakages, but include and cases with insiders stealing data or firm denying the breach (that is the case of Microsoft that denied Minecraft server breach).
We chose to collect firms only from United States. This is because the majority of global security breaches are reported in United States, and every incident involving corporation that may have exposed personal information of third party must be reported and investigated.

Moreover each firm that announced a security breach incident is publicly traded in NYSE or NASDAQ. More specifically 39 companies are listed on NYSE and 21 on NASDAQ respectively. These two composite indexes constitute the heart of U.S. economy and undeniably our firms should be listed there. The market capitalization of companies listed on NYSE exceeds 19.29 trillion. On the other hand, NASDAQ contains the largest companies by market capitalization (Apple, Microsoft, Alphabet).

We gathered the daily prices of stock data from Bloomberg. The prices are adjusted for stock splits and dividend payments to avoid sudden and large turnarounds.

One extra criteria that should be fulfilled is that the stock of a corporation should be publicly traded for all the estimation period (Pirounias et al (2014)).

4.3 Statistical methodology

Following the methodology adopted by previous studies, we are going to determine the abnormal returns for a firm which announced a security breach incident. According to MacKinlay (1997) abnormal return is defined as ‘the actual ex post return of the security over the event window minus the normal return of the firm over the window’. If the breach had not occurred, the normal return would be the expected one. We need to calculate the cumulated abnormal returns (CAR) over a specific event window \([t_1, t_2]\).

Similarly with Gatzlaff et al (2010) we use the market model which relates the return of a given stock to the return of the market portfolio. That is:

\[
R_{it} = a_i + b_i R_{mt} + \epsilon_{it}
\]

Where \(R_{it}\) = return of stock \(i\) on period \(t\)

\(R_{mt}\) = return of market \(m\) on period \(t\)

\(\epsilon_{it}\) = disturbance term with \(E[\epsilon_{it}] = 0\), \(Var[\epsilon_{it}] = \sigma^2\)
Using the above model, $\varepsilon_{it}$ coincides with abnormal return of stock I on day t or

$$AR_{it} = R_{it} - a_i - b_i R_{mt}$$

The two coefficients $a_i$ and $b_i$ are calculated using the regression method of ordinary least squares (OLS). The parameters were estimated over the window [-246 , -7]. This window is almost one year before the incident and by doing that the stock’s return is calculated assuming the breach was absent.

Then $CAR_i$ for n days is:

$$CAR_i(n) = \Sigma AR_{it}$$

We further need to test the hypothesis by applying the student-t statistic test, a vital tool in statistical analysis. If $av(CAR) = \Sigma CAR_k / N$ is the mean CAR for N cases and $var(CAR) = \Sigma var(CAR_k) / N^2$ is the variance of CAR then the student-t distribution with $T-1$ degrees of freedom is:

$$t = av(CAR) / var(CAR)^{1/2} \sim t(a, T-1)$$

In order to avoid appearance of clustering, covariance between individual sample CAR must be zero. We can safely assume that there is no correlation between the abnormal returns on individual securities if the event windows of the affected stocks do not overlap over time.

### 4.4 Hypothesis development

As it has already been mentioned, stock prices are linked with investors’ expectations. One may expect that a security breach will have negative impact on firm’s value. That is customers trust their sensitive data on firm’s system and nevertheless there is information exposure. Even if direct and tangible costs are confronted immediately intangible costs may be irreversible because of disappointed customers. So we expect negative abnormal return during the announcement day:

H1: When a firm announces a security breach incident, its value is negatively influenced by abnormal stock return.
Further with the full sample hypothesis, we are interested in the repercussions caused by cyberattack in specific sector. Public worries are raised when financial firms fall victims of cyberattack. Sensitive data related with online accounts are exposed and clients may face direct economic losses. Financial corporations like banks develop online transactions making them attractive to hackers. The Financial Stability Oversight Council that the American financial firms are champions in internet safety investments in comparison with other sectors. So we formed a subgroup of 13 financial firms.

H2: A security breach will have greater negative impact in financial firms compared with full sample firms.

Another interesting point is whether market penalizes smaller firms than larger ones. Firm size is an element that hackers evaluate. After recent big blows for firms like Home Depot and Alphabet large capitalization companies harden the penetration of malicious outsider by investing more in internet security. But smaller and middle capitalization firms either are unaware of the danger or hesitate to invest on internet safety.

At the same time middle capitalization companies outperform larger ones (for instance Credit Suisse reports that for European firms). One possible explanation is that investors expect future growth for middle capitalization corporations, as that happened with Apple in mid 90s, or acquisition by large ones.

Thus a possible hit in the reputation of a middle firm is expected to deter its growth prospects and investors’ beliefs will be revised. In general a middle capitalization firm is consisted of 1.5 to 10 billion. As the bounds are negotiable through the investment world, for our study we formed a subgroup of 19 firms with market capitalization till 15 billion and even included a small one with 721 million.

H3: Middle capitalization firms will exhibit greater negative abnormal returns than the larger ones when a security breach incident is announced.
4.5 Results

Table 4.1

Results for full sample statistical analysis

<table>
<thead>
<tr>
<th>Event window</th>
<th>Sample size</th>
<th>Average CAR</th>
<th>t-statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-4,4]</td>
<td>60</td>
<td>0.000920678</td>
<td>0.012937888</td>
</tr>
<tr>
<td>[-1,0]</td>
<td>60</td>
<td>-0.00355672</td>
<td>-0.14058667</td>
</tr>
<tr>
<td>[0,0]</td>
<td>60</td>
<td>-0.000766819</td>
<td>-0.03867482</td>
</tr>
<tr>
<td>[0,1]</td>
<td>60</td>
<td>0.000434852</td>
<td>0.012466796</td>
</tr>
</tbody>
</table>

The table above shows the results for full sample after statistical analysis has been employed. We observe that negative average CAR have been found on [0,0] and [-1,0] event windows but without statistical significance.

Table 4.2

Results for financial subgroup statistical analysis

<table>
<thead>
<tr>
<th>Event window</th>
<th>Sample size</th>
<th>Average CAR</th>
<th>t-statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-4,4]</td>
<td>13</td>
<td>-0.038617036</td>
<td>-0.363327118</td>
</tr>
<tr>
<td>[-1,0]</td>
<td>13</td>
<td>-0.00406572</td>
<td>-0.185128908</td>
</tr>
<tr>
<td>[0,0]</td>
<td>13</td>
<td>-0.004076463</td>
<td>-0.222461847</td>
</tr>
<tr>
<td>[0,1]</td>
<td>13</td>
<td>-0.014487987</td>
<td>-0.341314645</td>
</tr>
</tbody>
</table>

Table 2 summarizes the findings for the created financial subgroup after statistical analysis has been applied. In this case average CAR for all event windows have been found negative but again without statistical significance.
Table 4.3

Results for middle capitalization firms subgroup statistical analysis

<table>
<thead>
<tr>
<th>Event window</th>
<th>Sample size</th>
<th>Average CAR</th>
<th>t-statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-4,4]</td>
<td>19</td>
<td>0.003821257</td>
<td>0.057519898</td>
</tr>
<tr>
<td>[-1,0]</td>
<td>19</td>
<td>-0.004712064</td>
<td>-0.155278347</td>
</tr>
<tr>
<td>[0,0]</td>
<td>19</td>
<td>-0.003338371</td>
<td>-0.144543161</td>
</tr>
<tr>
<td>[0,1]</td>
<td>19</td>
<td>0.004017511</td>
<td>0.107334632</td>
</tr>
</tbody>
</table>

Table 3 shows the results for middle capitalization firms’ subgroup after statistical analysis has been run. Negative average CAR has been noticed in [0,0] and [-1,0] event windows. Again our results fail to be statistical significant.

4.6 Debate

The findings from our statistical analysis differ from our expectations to detect strong negative abnormal returns due to security breach incident. We examined a time period where cyberattacks are multiplied but at the same time firms seek to invest more in qualitative security solutions. We can not neglect the fact that market will reward firm’s value if a security investment is announced. Back to 2010, Sangmi et al conclude that an average of 1.46% excess return was created due to measures taken against cyber risk. It is the large firms that are more concerned about the dangers of cyber risk and proceed to this kind of investments. As 41 from our total 60 firms have market capitalization higher than 15 billion, we believe that future studies should focus on incidents happened in small firms.

According to cybersecurityventures.com the cyber security market is estimated to grow to $155.74 billion by 2019. We are approaching an era where a vast growing market emerges, the cyber security market. Moreover, Gartner’s research vice president Andrew Wells stated that the security awareness training market approaches $1 billion in annual revenue. Most expenses are originated from large companies that already have decided to train their employees. Thus, it is possible a security breach to be treated professionally and cause no
problems and costs. This should lead market to attribute low awareness and significance in cyberattacks.

4.7 Limitations and possible biases

It is necessary to discuss some issues that may influence negatively our process to generate valid results. For the needs of an event study the accurate date of the incident must be known. In our case, our sources may provide a date that diverges from the date of the announcement of the cyberattack. As we are concerned for the announcement day (as this is the day that the incident is public known) and not for the incident date, there may be a confusion between these dates. This is a common pitfall for this kind of studies when there is lack of access in high validity sources.

Furthermore, there are many events that may coincide with the announcement of the event and influence stock prices as well. We handled stock splits and dividend payments by using adjusted values but Pirounias et al (2014) mention mergers, acquisitions, CEO replacement announcements and unexpected earnings announcements as further key factors. Due to lack of access in confidential and valid sources the aforementioned factors were not isolated if existed. As a result it is not easy to detect the influence of the cyberattack.

Brown et al (1984) warn that the population of daily abnormal returns is not expected to follow normal distribution unless the sample is large. We have ensured normality for the full sample but subgroups exhibit a Jarque-Berra value around 30. Nevertheless we find this value acceptable for a tendency to normal distribution.
Chapter 5
Conclusion

5 Conclusion

In this work we quoted some aspects of cyber risk management. This new kind of risk has emerged the recent years due to the increased online activity by firms. Whether cyber risk belongs to the family of operational risks is an issue still debated. Professionals and academic stuff are assigned with the task to measure cyber risk both qualitatively and quantitatively.

The developed techniques will be used from insurers to design cyber insurance products with fair premiums. Cyber insurance offers various options for firms in order to cover possible losses from cyberattack. The sector has further growth prospects as many firms are still hesitant for the necessity of cyber insurance.

Beyond cyber insurance, managers are advised to approve investments on information technology security systems. When human fails to manage cyber risk, learning machines and artificial intelligence can exhibit an outstanding performance. These advanced systems can analyze massive amount of complex data, and are able to make decisions whether a fraud is going to be done. Although there is the argument of violation of private information (the systems need many private data as inputs), experts continue to make further improvements to the existing systems.

One could justify the incomplete investment on information technology security systems due to lack of funds. But encryption data is a method that could ensure the misuse of private information even if they are stolen. Nevertheless, some firms neglect the perils and avoid encrypting their employees’ data. Customer information, research and development data, product releases information and financial reports are important data that should be encrypted.

Lastly, one crucial factor in cyber risk management is human behavior. Surveys show that human behavior is responsible for misusing security systems because of either complex operations or skepticism about the effectiveness. So, systems should incorporate the human behavior aiming to guide employees to act right.
The empirical part of this work investigated the impact of a security breach on firm’s value. The event study methodology applied in a sample of 60 companies that suffered a security breach. Security breach could come of malicious outsider and insider acting on purpose or accidentally. Additional subsamples were consisted, one including financial firms and one with middle capitalization firms.

Our analysis showed that when a firm announced a security breach incident, negatively cumulative abnormal return were formed in the event date and one day prior the event in all samples. Nevertheless, all the results were statistically insignificant. It seems that either we need to enlarge our sample more or include cases with specific attack characteristics. An interesting extension of this work, in an attempt to get more valid statistical results, would be to employ a multi factor model. Multi factor models have already been used by Gatzlaff et al (2010) and Pirounias et al (2014). A possible multi factor model could include factors with common characteristics for sample firms, for instance the industry and the market capitalization the firms belong to. With this technique we aim to reduce the variance of the estimated abnormal return.

We hope future studies to use large amount of data (scarce data in this research field is common) in order to produce credible results. As modern economy continues to bleed due to cybercrime, more related studies are anticipated in the near future.
## Appendix

### Sample and Sources

<table>
<thead>
<tr>
<th>FIRM</th>
<th>TICKER</th>
<th>DATE OF ANNOUNCEMENT</th>
<th>SOURCE</th>
<th>ADDITIONAL SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Company</td>
<td>Stock</td>
<td>Date</td>
<td>Source</td>
</tr>
<tr>
<td>---</td>
<td>-------------------</td>
<td>-------</td>
<td>--------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>Company</td>
<td>Abbreviation</td>
<td>Date</td>
<td>Website</td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>--------------</td>
<td>------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Company</td>
<td>ShortName</td>
<td>Date</td>
<td>Source</td>
</tr>
<tr>
<td>---</td>
<td>---------------</td>
<td>-----------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>38</td>
<td>COSTCO</td>
<td>COST</td>
<td>15/7/2015</td>
<td>breachlevelindex.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>#</td>
<td>Company</td>
<td>Stock Code</td>
<td>Date</td>
<td>Source</td>
</tr>
<tr>
<td>---</td>
<td>---------</td>
<td>------------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>56</td>
<td>IMAX</td>
<td>IMAX</td>
<td>3/7/2017</td>
<td>breachlevelindex.com</td>
</tr>
</tbody>
</table>


15. CRO forum, 2016


18. Eling Martin, Wirfs Jan Hendrik, Modelling and management of cyber risk, 2015, Institute of insurance economics, university of St Gallen


30. Kirkpatrick Keith, Cyber policies on the rise, October 2015


33. Lamande Emmanuelle, GrIDSure authenticates Microsoft’s latest remote application platform, April 2010


37. Maillart T., Sornette D., Heavy-tailed distribution of cyber-risks, March 2010, The European physical journal


39. McAfee, The Economic Impact of Cybercrime and Cyber Espionage, 2013

40. MIT news, “System predicts 85% of cyber-attacks using input from human experts,” April, 2016, (internet source)

41. Mukhopadhyay Arunabha, Chaterjee Samir, SahaBebashis, Mahanti Ambuj, Sadhukhan Samir, Cyber-risk decision models: To insure IT or not?, May 2013, Journal of Decision Support Systems


45. Perakslis Eric D., Cybersecurity in Health Care, July 2014


47. Pirounias Sotirios, Mermigas Dimitrios, Patsakis Constantinos, The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study, August 2014, Journal of Information Security and Applications


49. Swiss Re, 2014


52. Vallesi Fabiano, Cybersecurity: a top spending priority for corporates, September 2017, (Internet source)

53. Walters Riley, Cyber Attacks on U.S. Companies in 2014, October 2014


55. Wells Andrew, CYBER SECURITY BUSINESS REPORT, May 2015, (Internet source)


57. World Economic Forum, 2012


60. www.lawsociety.org.uk

61. www.utdallas.edu


64. http://www.stamford.edu

65. https://www.storagecraft.com/blog/what-data-should-your-company-encrypt/