INFORMATION TECHNOLOGY, ITS MARKET VALUE AND RELATED RISKS ON MANUFACTURING AND SERVICE FIRMS

CANSU TAYAKSİ

SEPTEMBER, 2017

INFORMATION TECHNOLOGY, ITS MARKET VALUE AND RELATED RISKS ON MANUFACTURING AND SERVICE FIRMS

A THESIS SUBMITTED TO THE

GRADUATE SCHOOL OF BUSINESS

OF THE

IZMIR UNIVERSITY OF ECONOMICS

BY

CANSU TAYAKSİ

SEPTEMBER, 2017

Approval of Graduate School of Business

....

Prof. Dr. Hasan Fehmi BAKLACI

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

....

Assoc. Prof. Dr. Burcu Güneri ÇANGARLI

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Yiğit
....

Assoc. Prof. Dr. Yiğit KAZANÇOĞLU

Co-Supervisor

....

Prof. Dr. Hasan Fehmi BAKLACI

Supervisor

Examining Committee Members

Prof. Dr. Gülem ATABAY ....

Prof. Dr. Hasan Fehmi BAKLACI ....

Prof. Dr. Ayla Özhan DEDEOĞLU ....

Prof. Dr. Semra TUNALI ....

Assoc. Prof. Dr. Yiğit KAZANÇOĞLU Yiğit ....

Assoc. Prof. Dr. Ali Serdar TAŞAN ....

ABSTRACT

INFORMATION TECHNOLOGY, ITS MARKET VALUE AND RELATED RISKS ON MANUFACTURING AND SERVICE FIRMS

TAYAKSİ, Cansu

BUSINESS ADMINISTRATION Ph. D PROGRAM

SUPERVISOR: Prof. Dr. Hasan Fehmi BAKLACI

CO-SUPERVISOR: Assoc. Prof. Dr. Yiğit KAZANÇOĞLU

SEPTEMBER, 2017

For businesses, information is a permanent asset and it needs to be preserved as the other worthful assets of the company (ISO/IEC 27002, 2013; Misra et al., 2007). In today’s world there is an increased competitive landscape for businesses and the data is very crucial for the firms to survive under those circumstances (Borek et al., 2013).

Cyber systems are also known as Information and Communication Technologies (ICT) and there are many advantages embedding those technologies into the main business processes like the operational efficiency increase, decision quality improvement and cost decrease. Information systems and related technologies get into the nearly every direction of the modern life from smart phones to the usage of smart grids; this seems like the lifestyle of the 21th century. Of course this new life style brings its drawbacks with, like the security and assurance problems (Mailloux, 2013). The Computer Emergency Response Team (CERT) Coordination Center states that the attacks on businesses through the Internet have almost doubled every year since 1997 (CERT, 2004).

The violations on security issues of those information systems will have costly effects (Sun et al., 2006). These problems could cause huge costs to both manufacturing and service firms. According to the Computer Crime and Security Survey of the Computer Security Institute which was held in 2010 with 738 organizations, there were $190 million total estimated annual loss due to information systems security related cases (Gordon et al., 2010). Firms which integrate the usage of the Information Technology into its operations should also deal with some negative consequences that the operations could bring and the firms should manage the process well in the case of an emergency. Firms should have a better and deeper understanding level for providing a better management. After a higher level of understanding, the strategy of the firm could be rearranged more properly. In a natural way the executives of the firms are more concerned with the financial effects of the risk events, they are tense about the reaction of the stakeholders and the leading economic impact on their firms.

This dissertation explores information technology and its related risks and impacts on the firms that are operating under manufacturing and service industries by employing "Event Study Methodology" to examine the impacts of privacy breaches. Event study is the accepted method for examining the effects of the public announcements on stock prices of listed firms and the related studies have taken place in the literature since the late 1960s. Efficient capital markets concept of Fama (1970) offers a concrete theoretical foundation for the event study methodology by indicating the stock market is "informationally efficient" and the stock prices reflects all the available information for a firm. Fama (1991) also says that if there is new information in the market, such as the new technology usage in a firm, stakeholders will reflect their opinions to the firm's stock prices and there will be a change in the value of the firm. In brief, there could be experienced a positive (upwards) impact on the firm value due to the new technology usage announcement (Konchitcki, 2011).

The underlying principle of the methodology is based on the expectation of an unexpected event will cause positive or negative reaction in the stock prices of a

firm and the return of the stock prices will become abnormal. The normal return estimation of a firm is derived from the previous stock price returns and when it is abstracted from the actual return, the abnormal return could be obtained. If the calculation gives positive results, then the event’s impact to the stock price of the firm is assumed as positive. Similarly, if the result is derived as negative, the impact to the stock prices is assumed as negative.

The expected return on the stock after the security related events is calculated in several ways in different studies. The dissertation will use the three major models for being able to compare the results between them. The models are: The Market Model, Market Adjusted Model and Mean Adjusted Model. The research questions in the dissertation are answered by using all of the three models.

Key Words: Information Technology, IT, Cybersecurity, Market Value, Event Study Methodology.

ÖZET

BİLGİ TEKNOLOJİLERİ, PİYASA DEĞERİ VE ÜRETİM VE HİZMET FİRMALARI ÜZERİNDEKİ RİSKLERİ

TAYAKSİ, Cansu

İŞLETME DOKTORA PROGRAMI

DANIŞMAN: Prof. Dr. Hasan Fehmi BAKLACI

EŞ DANIŞMAN: Doç. Dr. Yiğit KAZANÇOĞLU

EYLÜL, 2017

İşletmeler için, bilgi kalıcı bir varlıktır ve şirketin diğer değerli varlıkları gibi korunması gerekmektedir (ISO / IEC 27002, 2013; Misra vd., 2007). Günümüz dünyasında işletmeler için rekabet artmaktadır ve verinin varlığı firmaların bu koşullar altında hayatta kalması için çok önemlidir (Borek vd., 2013).

Siber sistemler ayrıca Bilişim ve İletişim Teknolojileri (BİT) olarak da bilinir ve ana iş süreçleri ile bu teknolojileri birleştirmenin işlemlerin verimliliğinin artışı, karar kalitesinin iyileştirilmesi ve maliyet düşüşü gibi pek çok avantajı vardır. Bilgi sistemleri ve ilgili teknolojilerin, akıllı telefonlardan akıllı şebekelerin kullanımına kadar modern hayatın neredeyse her yönüne ulaştığı görülmektedir; bu 21. yüzyılın yaşam biçimi olarak benimsenmiştir. Elbette bu yeni yaşam tarzı, güvenlik ve güvence sorunları gibi dezavantajlarını beraberinde getirmektedir (Mailloux, 2013). Bilgisayar Acil Müdahale Ekibi (CERT) Koordinasyon Merkezi, internet üzerinden işletmelere yapılan saldırıların 1997'den bu yana neredeyse her yıl ikiye katlandığını belirtmektedir (CERT, 2004).

Bilgi sistemlerinin güvenlik konusundaki ihlallerinin maliyeti işletmeler için yüksektir (Sun vd., 2006). Bu sorunlar hem imalat hem de hizmet firmaları için büyük maliyetlere yol açmaktadır. 2010 yılında 738 kuruluşla gerçekleştirilen Bilgisayar Güvenlik Enstitüsü Bilgisayar Suç ve Güvenlik Araştırması'na göre, bilgi

sistemleri güvenliği ile ilgili konular nedeniyle toplam 190 milyon dolarlık tahmini yıllık zarar oluşmuştur (Gordon vd., 2010). Bilgi teknolojisinin kullanımını operasyonları ile birleştiren firmalar, bu sürecin getirebileceği bazı olumsuz sonuçlarla uğraşmalıdır. Bu tür sorunların ortaya çıkması durumunda firma süreci iyi bir şekilde yönetmelidir. Firmalar daha iyi bir yönetim için daha iyi ve daha derin bir anlayış düzeyine sahip olmalıdır. Daha yüksek bir anlayıştan sonra firmanın stratejisi daha düzgün bir şekilde düzenlenebilir. Doğal olarak, firma yöneticileri, risk olaylarının finansal etkilerinden daha fazla endişe duymakta, paydaşların durumlara tepkileri ve bunun firma üzerindeki ekonomik etkileri konusuna önem vermektedirler.

Bu tez, bilgi teknolojisi ve bilgi teknolojisi ile birlikte gelen gizlilik ihlalleri risklerinin imalat ve hizmet alanında faaliyet gösteren firmalar üzerindeki etkilerini incelemek için olay etüdü yöntemini kullanmaktadır. Olay etüdü, halka açıklanan duyuruların, borsada işlem gören şirketlerin hisse senedi fiyatları üzerindeki etkilerini incelemek için kabul gören bir yöntem olup, ilgili çalışmalar 1960'ların sonlarından beri literatürde yerini almıştır. Fama'nın etkin piyasalar hipotezinin (1970) piyasaların "bilgi açısından verimli" olduğunu ve hisse senedi fiyatlarının bir firmanın mevcut tüm bilgilerini yansıttığını öne sürmesi ile olay etüdü yöntemi için somut bir teorik temel oluşmaktadır. Fama (1991), ayrıca bir şirkette yeni teknoloji kullanımının başlaması gibi pazarda yeni bir bilgi varsa, menfaat sahiplerinin görüşlerini şirketin hisse senedi fiyatlarına yansıtacağı ve firmanın değerinde bir değişiklik olacağını belirtmiştir. Kısacası, bilgi duyurusu nedeniyle firma değeri üzerinde olumlu (yukarı doğru) bir etki yaşanabilir (Konchitcki, 2011).

Yöntemin altında yatan ilke, beklenmedik bir olayın bir firmanın hisse senedi fiyatlarında olumlu ya da olumsuz tepkilere neden olacağı ve hisse senedi fiyatlarının getirisinin anormal hale geleceği beklentisine dayanır. Bir firmanın normal getiri tahmini önceki hisse senedi getirilerinden türetilir ve gerçek getiriden çıkartıldığında anormal getiri elde edilebilir. Hesaplama olumlu sonuçlar verirse, olayın firmanın hisse fiyatına etkisi olumlu olarak kabul edilir. Benzer şekilde, eğer

sonuç negatif olarak çıkar ise, hisse senedi fiyatlarına olan etki negatif olarak kabul edilir.

Güvenlikle ilgili oluşan olaylardan sonra hisse senedi üzerinde beklenen getiri, farklı çalışmalarda çeşitli şekillerde hesaplanmıştır. Bu tez, aralarında sonuçları karşılaştırmak için üç ana modeli kullanacaktır. Tez içerisinde kullanılan modeller, piyasa modeli, piyasa getirisi ile düzeltilmiş ve ortalama ile düzeltilmiş modellerdir. Tezdeki araştırma soruları bu üç model kullanılarak cevaplanmaktadır.

Anahtar Kelimeler: Bilgi Teknolojileri, BT, Siber Güvenlik, Piyasa Değeri, Olay Etüdü Yöntemi.

ACKNOWLEDGEMENTS

Firstly, I would like to indicate my sincere regards to Prof. Dr. Erhan ADA, who has been my advisor from the first time that I entered the program at the Izmir University of Economics. He has always been an excellent mentor during my Ph.D. studies; he showed me the way to the professional working environment and was like an intellectual father to me with his constant support both inside and outside the university. I always felt honored for having the chance to work under supervision such a valuable academician. I hope he knows how much we love and respect him as "his team". Although situations may vary in life, I will always refer him as my advisor.

I also would like to express my gratitude to my co-advisor Assoc. Prof. Dr. Yiğit KAZANÇOĞLU. His valuable collaboration, continuous support and ideas about the new studies thought me a lot during my studies. I would always appreciate the time and invaluable insight that he has provided for me since the first day I began to work with him. I feel so lucky for having the chance to meet and work with such an encouraging person.

I would like to give a special thank you to my advisor Prof. Dr. Hasan Fehmi BAKLACI for not leaving me alone after the advisor changes on my dissertation. His support was very valuable for me.

In addition to my advisors, I would like to thank the rest of my thesis committee: Prof. Dr. Semra TUNALI, Prof. Dr. Gülem ATABAY, Prof. Dr. Ayla DEDEOĞLU and Assoc. Prof. Dr. Ali Serdar TAŞAN for their insightful contributions during my studies.

I owe a debt of gratitude to my family, my dad Tayfun TAYAKSİ; my mom Hayal TAYAKSİ and my brother Mert TAYAKSİ, who always been there for me during my good and bad days. Their loving support was essential during my doctoral work. I would also like to thank my friends and colleagues who have been a part of this journey. Their friendship, support, and the way they stand there for me every time I need help is priceless.

I could not finish this part without thanking Tezer YELKENCİ for his continuous support during my Ph.D. studies and being like a second brother to me.

Thank you, everyone who has been there for me in the last 5 years!

Cansu TAYAKSİ

İzmir, September 13, 2017.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Information Technology is widely used in manufacturing and service companies for being able to increase the efficiency and the effectiveness of the operations. Along with the many advantages that Information Technology provides for the companies, the technological advancements in business processes also brings some vulnerabilities for the firms. This dissertation will explore the effects of cyber security breaches on the stock prices of publicly listed companies. After the detailed review of the literature and collecting a comprehensive data set, the effects will be explained according to 5 research questions of the dissertation.

1.1. MOTIVATION

For businesses, information is a permanent asset and it needs to be preserved as the other worthful assets of the company (ISO/IEC 27002, 2013; Misra et al., 2007). In today’s world there is an increase competitive landscape for businesses and the data is very crucial for the firms to survive under those circumstances (Borek et al., 2013).

Cyber systems are also known as Information and Communication Technologies (ICT) and there are many advantages embedding those technologies to the main business processes like operational efficiency increase, decision quality improvement and cost decrease. Information systems and related technologies get into the nearly every direction of the modern life from smart phones to the usage of smart grids; this seems like the lifestyle of the 21th century. Of course this new lifestyle brings its drawbacks with, like the security and assurance problems

(Mailloux et al., 2013). The Computer Emergency Response Team (CERT) Coordination Center states that the attacks through the Internet on businesses have almost doubled every year since 1997 (CERT, 2004).

Information systems have a wide range of usage area in management of businesses, so the violations on security issues of those information systems will have costly effects (Sun et al., 2006). These problems could cause huge costs to the firms. According to the Computer Crime and Security Survey of the Computer Security Institute which was held in 2010 with 738 organizations, there were $190 million total estimated annual loss due to information systems security related cases (Gordon et al., 2010). In addition, Kaspersky Lab has conducted Global IT Risk Survey and the results have pointed that 50% of the respondents rated cyber threat as a major business threat after the economic uncertainty (Kaspersky Lab, 2012). The threat and risk sources are the hackers, malicious softwares, bad-tempered employees, rivals and other risk generators; all of them are called as threat agents. Those threat agents could be originated internally or externally to an organization and all of them could have diverse interest and motivations (Harris, 2010; Landoll, 2006). According to a report of the Ponemon Institute, the average data breach cost in the United Kingdom increased from £47 million in 2007 to £79 million in 2011 which makes 68% increase (Ponemon Institute LLC, 2012). That powerful increase shows the importance of the information for organizations. Also some kind of information examples are the matter of life or death like the medical records of the hospitals which value cannot be measured only with monetary terms (Wilcox and Brown, 2004).

The problems related to the security problems is continuing to happen through time although the existence of numerous security guidelines and software for the security evaluation and risk management. In addition, there is a different approach to those problems from the business managers and security issues although the security issues are the same, and that leads to a hard communication between them while solving the security issues (Solic et al., 2015). The causes of the risks of information systems arise from the loss of data confidentiality, integrity, or availability, and contains the negative impacts to organizational operations, organizational assets, individuals, or other organizations (NIST SP, 2013).

Data Breach Investigations Report of Verizon showed that 96% of security breaches which is occurred in 2012 have objectives as financial or personal gains (Verizon, 2012). The report also demonstrates that 79% of the organizations that suffered from those breaches were targets of opportunity, which means that they are targeted only because their vulnerability and 96% of all attacks were not thought to be hard to commit. Those facts have caught the attention of many different people as the researchers, professionals, journalists, legislators, governments, and normal citizens to information security and its application areas (Jourdan et al., 2010). By looking at the results of the 11th Annual Computer Crime and Security Survey 74.3% of the total losses of the organizations are caused by viruses, unauthorized access, theft of the laptop or mobile hardware, proprietary information theft (Gordon et al., 2005). McCue (2008) conducted a study indicating that 70% of fraud is committed by insiders rather than by external offenders in spite of 90% of security controls are centered upon the external threats. There are some important examples of the Information System implementation failures such as the situation Hewlett-Packard (HP) was facing in 2004. They loss $160 million due to the implementation failure (Koch, 2007), also Nike and Hershey Foods have confronted with huge losses which will be discussed below in more detail (Koch, 2004).

As mentioned earlier, security breaches that occurred in an organization could harm the customer and business partners’ trust and confidence. The firm that dealt with breach issues also faces the labor cost for damage repair process. The productivity and revenue loss are also other concerns that a firm will face due to the unanticipated downtime and as a result firms could suffer decrease in sales in accordance with reputation loss. Thus, a firm encountering a security breach should expect a downfall in net future cash flows. After the announcements regarding to security breach have been made to the investors, a revision could be made by the investors about the firm value according to efficient market theory. The anticipation is a negative effect on net cash flows, thus the expected movement of valuations would be a decrease (Kannan et al., 2007).

The public awareness upon the security breaches increased rapidly during the denial-of-service (DOS) attacks to the big Internet companies like Amazon, eBay, and Yahoo in February 2000. Software developers are aware of the necessity of the secure products. In the year of 2002, Microsoft took an important and unique step as cutting the development of the new Windows operating system that will released and send the 7000 systems programmers to a special training program for security (Markoff, 2002). The president of the company, Bill Gates, made an announcement about the situation and explained now the security is more important than everything in their work life and said if they did not do this, people would not be willing to benefit from the advantages of their work. They chose to resolve the security issues before adding new features to their operating system (CBS, 2003). That memo showed the importance of security from a major software developer company's point of view.

There are also examples regarding to the service industry besides the for-profit industry. University of Massachusetts has encountered such a failure. More than 27000 students of the university have faced with not properly working portals and ERP applications, so they could not find their classes of that semester. In addition, they had confronted with problems while collecting their financial aids (Wailgum, 2005).

1.2. RESEARCH QUESTIONS

Firms which integrate the usage of the Information Technology into its operations should also deal with some negative consequences could bring and the firms should manage the process well if the case of an emergency. Firms should have a better and deeper understanding level for a better management. After a higher level of understanding, the strategy of the firm could be rearranged more properly. In a natural way the executives of the firms are more concerned with the financial effects of the risk events, they are tense about the reaction of the stakeholders and the leading economic impact on their firms. Therefore, in this dissertation the research questions are listed as follows:

1.2.1. ARE THE LISTED FIRMS BEING AFFECTED FROM INFORMATION TECHNOLOGY RELATED FAILURES?

Information Technology related systems could be used nearly in all of the functions throughout an organization. The usage of the IT systems brings its risks with. When those IT related risks occurred in firms, the executives of those firms are responsible for making an announcement to their stakeholders about the situation.

There are numerous studies in literature which focused on the Information Systems failure. Loch et al. (1992) stated in their research that system security is a vital issue that firms are facing and there are always risks as the accidental or unauthorized access, disclosure or destruction of the system and the data. The article reported a study about MIS executives' concerns about these threats. The results showed that the managers were exposing their firms to the risks which they even are unaware of, and they often refused to acknowledge and the management process was poorly equipped. Their study does not have an analysis on the stock price change caused by the risk failure announcements. Some other studies focused upon the security risk assessment such as Solic et al. (2015) which presented a model for information systems security evaluation. Although they focused on the security risk assessment that study doesn't include the change in stock price due to the risk failure announcements.

Jouini et al. (2014) proposed a security threat classification model to study the threats class impact. These studies focused on the security issue of the firms are facing, however, but they do not include the announcement effect on the stock prices of the listed firms.

Based on the reason that the literature has gaps in the topic of the risk failure announcements' effect on the listed firms' stock prices, the first research question tries to find an answer about it. The first hypothesis tested is the market reaction to an information security breach on the market values of the firms in the overall sample.

$H1_0$: IT related failures do not have statistically significant impact on the market value of the publicly listed firms.

For following research questions, sample will be divided into sub samples. The second research question is as follows:

1.2.2. WHAT ARE THE EFFECTS OF INFORMATION TECHNOLOGY RELATED FAILURES ON MANUFACTURING AND SERVICE FIRMS SEPARATELY?

When firms are affected from a security breach, data theft or misusage, there are consequences in the valuation of that firm. The main concern is the listed firms and the effect rate after the announcement of the attacks. By analyzing the existing data, the effect of the announcement will come to the surface. Due to reason that, the attacks are occurring not only against manufacturing firms but also to the service firms, the analysis will include both types of organizations. With this knowledge firms could be aware of what kind of effect they would have if any of the security risks will occur.

For the second research question, two hypotheses are developed for testing the effect of information security breaches on manufacturing and service companies separately:

$H2_0$: IT related failures do not have statistically significant impact on the market value of the manufacturing firms.

$H3_0$: IT related failures do not have statistically significant impact on the market value of the service firms.

Third research question is as follows:

1.2.3. WHICH SECTOR IS AFFECTED THE MOST FROM THE INFORMATION TECHNOLOGY RELATED FAILURES?

There are many manufacturing and service organizations and there are many studies in the literature that analyzed the security breach announcements and their effects on the listed firms. However, none of these has analyzed the effects based on the industry (Acquisti et al., 2006; Andoh-Baidoo and Osei-Bryson, 2007; Bolster et al., 2010; Hovav and D'arcy, 2003). Pirounias et al. (2014) divided their sample into two sub-samples for analyzing the security breach impact as sector-based. Their sample consists of the technology & non-technology and financial & non-financial firms. However, they suggested that usage of a larger dataset would be more effective for insuring the assumptions are made by dividing the overall sample into sub-samples.

In this dissertation the data is collected in a way that can be analyzed and made assumptions in sectoral basis.

Four hypotheses are developed for testing the effect of information security breaches on different sectors:

$H4_0$: IT related failures do not have statistically significant impact on the market value of the consumer goods sector.

$H5_0$: IT related failures do not have statistically significant impact on the market value of the financials sector.

$H6_0$: IT related failures do not have statistically significant impact on the market value of the technology sector.

$H7_0$: IT related failures do not have statistically significant impact on the market value of the communications sector.

The forth question is as follows:

1.2.4. DOES THE LOST RECORD SIZE HAVE EFFECT ON THE FAILURE IMPACT?

During some breach events, the firms are losing important amount of data. An analysis has been made between the firms which have announced their lost record sizes. The impact of the IT-related failure will be analyzed by 4 groups of firms including different "lost record sizes".

Four hypotheses are developed for testing the effect of information security breaches on different group of lost data sizes:

$H8_0$: IT related failures do not have statistically significant impact on Group 1 data size loss

$H9_0$: IT related failures do not have statistically significant impact on Group 2 data size loss

$H10_0$: IT related failures do not have statistically significant impact on Group 3 data size loss

$H11_0$: IT related failures do not have statistically significant impact on Group 4 data size loss

The fifth question is as follows:

1.2.5. AMONG ALL THE OTHER INFORMATION TECHNOLOGY RISKS, IS "HACKING" THE GREATEST RISK FOR BUSINESSES?

Although being hacked seems to be the most well-known risk that a firm could encounter, there are other kinds of IT risks as theft risk, poor security risk and insider jobs. All of these risk events are assumed to have different effects on both internal processes of the firm and external valuations of the stakeholders. This final question compares the effects of those risks separately and finds if "hacking" is the greatest risk for businesses or not.

Two hypotheses are developed for testing the effect of information security breaches caused by hacking or the other types of breaches:

$H12_0$: Hacking do not have statistically significant impact on the publicly listed firms.

$H13_0$: Other kinds of IT related risks do not have statistically significant impact on the publicly listed firms.

1.3. RESEARCH APPROACH

1.3.1. SECURITY RISK ANALYSIS

Many scholars are making research about the security risk analysis for information systems in recent years (Cavusoglu et al., 2008; Karabacak and Sogukpinar, 2005; Peltier, 2007). The risk analysis approaches could be grouped into 3 main categories, which are: quantitative approaches, qualitative approaches, and the combination of both (Feng et al., 2014). Among those approaches, the quantitative ones use mathematical and statistical models for representing the risk (Karabacak and Sogukpinar, 2005). Security risk revelation is denoted as a probability function of the threats and the expected damage regarding to the weakness to those threats (Büyüközkan and Ruan, 2010). Gordon and Loeb (2002) have studied on a mathematical model with the aim of determining the optimal investment level to security for information systems. Their study and following studies focus on the security risk analysis on a single system or on a single protection technology type. Yue et al. (2007) has taken those studies one step far with the formulation and conclusion of the problem about the risk management pattern and have contributed additional insights for optimal decisions for the future use of managers.

A risk-based method is proposed by Grunske and Joyce (2008) which generated modular attack trees for every element in information systems. Those attack trees were detailed as parametric constraints and that specification allowed the quantifying process of the probability of security breaches which arisen because of the vulnerabilities in the deployment environment of the component.

In addition to the quantitative methods, there are also numerous qualitative security risk analysis methods and techniques. For instance, OCTAVE (The Operationally

Critical Threat, Asset, and Vulnerability Evaluation) method (Alberts and Dorofee, 2002) describes a set of impact evaluation criteria for launching a common ground for defining the impact values caused by the threats to the critical assets. Peltier (2007) also offered a qualitative risk analysis approach using practices like Practical Application of Risk Analysis (PARA) and Facilitated Risk Analysis Process (FRAP) for being able to evaluate both tangible and intangible risks. Due to the usage of this approach, systematic evaluation could be made on risks, threats, hazards, and concerns and the approach also provided cost-effective actions for decreasing risk into a more acceptable level. There are also some popular qualitative approaches as CCTA Risk Analysis and Management Method (CRAMM) which is established by the Central Computer and Telecommunications Agency (CCTA) by the UK Government and INFOSEC Assessment Methodology (IAM) (Douglas, 2006).

Third category is the comprehensive methods which combine quantitative and qualitative methods together (Alter and Sherer, 2004; Salmela, 2008). Chen and Chen (2003) implemented the similarity measures of generalized fuzzy numbers for handling with fuzzy risk analysis problems. This method is useful with handling unclear information derived by the human judgements; however, it could not provide graphical relationships between the security risk factors.

Fan and Yu (2004) have represented the relationships among risk factors by developing a procedure based on Bayesian networks (BNs) for providing support on risk analysis. Their Bayesian network is organized specially based on the experience of the domain experts. Sun et al. (2006) presented in their study an evidential reasoning approach under the Dempster–Shafer theory for the information systems security risk analysis. That approach provided rigorous and organized means for including the appropriate security risk factors, associated precautions, and the interrelationships between them while estimating information systems security risk.

The methods mentioned before made great contributions to the improvement of security risk analysis. However, Event Study Methodology will be used in this dissertation for providing information about an event that occurred throughout a company and the perception about the issue by the market participants.

Event studies are powerful tools and the initial requirement of it is the identification of the event of interest, for instance the announcement of the buying of particular software for the company. After the definition of the event, the time period over which the stock price changes of the firm would be investigated will be agreed upon. After the event announcement, the unexpected change in the stock prices would be analyzed to determine the scope of the evaluation change of the market participants (Konchitchki and O'Leary, 2011).

1.4. ADDRESSING THE LITERATURE GAPS AND LIMITATIONS OF PREVIOUS STUDY

The dissertation shapes around the IT related risk failure and the related literature gaps are listed as follows:

Former studies in the operations management area focused on the effects of the performance level of IT on the firm level (Cao and Dowlatshahi, 2005; Dehning et al., 2007; Hendricks et al., 2007) or the industry sector level (Shah and Shin, 2007). In spite of the increased adoption and usage rates of Information Technology by manufacturing organizations, there are not enough studies about the impacts of the IT on the operations manufacturing firms, especially at the plant level (Banker et al., 2006).

Gordon and Loeb (2002) indicated that there is research on the technical and organizational aspects of the breaches of information security, however there are not enough attention for the economic impacts of the security breaches. Andoh-Baidoo and Osei-Bryson (2007) also remark that there is a little emphasis on the Internet security breaches and their impact to firms’ market value.

There are also limitations for the research that have focused on the economic aspects of Information Security breaches. Some of the research in the literature has similar limitations. For example, Hovav and D’arcy (2005) stated that their sample was limited to only one type of defect, which is the effect of viruses, and they examined the effect on only one category of products, which are produced by mass production technology. There is lack of evidence if the results are valid for the other types of defects and other types of products. They stated that future research could focus on the announcement of various types of Information Systems defects.

The studies in the literature have lack of a big sample size in general as stated in the limitations sections (Acquisti et al., 2006; Andoh-Baidoo and Osei-Bryson, 2007; Campbell et al., 2003; Hovav and D'Arcy, 2003; Bose and Leung, 2013). All of the authors of those states are like minded that when the dataset will be expanded, the robustness of the findings will increase. Andoh-Baidoo and Osei-Bryson (2007) also stated that the public firms are eager for making announcement about positive developments like e-commerce implementation initiatives, new mergers, and change in executive management but the situation is the opposite when a company faces the security breaches. Campbell et al. (2003) also declares that firms have no incentive to share the information related to information security breaches and finding data is not so easy because the incidents could not be observed externally and not all the incidents are reported to the media. In the major newspapers there are only a few information security breach related news, hence they are not comprehensive data sources.

California law requires the notification about the when the data of the customers are compromised, however, the effected firms don't always make announcements by using press releases about that kind of events by following law. They prefer to notify the customers by sending them personal letters after the breach becomes widely known. This also affects the timeline of the event. The notice period of a security breach may take weeks or months after the occurring date. After, it also takes some time to determine the effected customers and sending them official notification letters. Finally, there is also a delay until the media finds out the letters are sent to the customers. These delays make a blurred "event window" and reduces the statistical power of the analysis (Aytes et al., 2006).

1.5. RESEARCH CONTRIBUTION

The first contribution of the dissertation is its wide dataset. The dataset is gathered from various sources as the studies in the literature, major newspapers, related websites and results of the different queries that are made through different search engines. The lack of data issue which is pointed in the earlier research has been taken into account and a comprehensive dataset has been gathered with the largest time frame and number of incidents.

Also, the research questions in the dissertation are not answered anywhere in the literature. The table about the related research and their research questions can be found below:

Table 1: Aims of the previous studies.

1	**Acquisti et al. (2006)**	The impact analysis of a company's privacy incidents on the market value.
2	**Arcuri et al. (2014)**	Exploring the impact of information security related breaches on stock returns of a company.
3	**Campbell et al. (2003)**	Analyzing the economic effect of information security breach announcements reported in newspapers on publicly listed corporations.
4	**Cardenas et al. (2012)**	Examining the impact of publicly announced security breaches on the market value of the companies.
5	**Cavusoglu et al. (2004)**	Assessing the impact of security breaches on the market value of breached firms.
6	**Goel and Shawky (2009)**	Examining the impacts of security breaches of a firm on the market value.
7	**Gordon et al. (2011)**	Resolving conflicting arguments from previous studies focusing on the effect of information security breaches on stock price returns of firms.
8	**Morse et al.**	Examining the impact of the breach announcements in

	(2011)	computer security on the behavior of stock markets.
9	**Pirounias et al. (2014)**	Examining the impact of information security breaches on the firm value.
10	**Ishiguro et al. (2006)**	Investigating the economic effects of information security incident announcements on the value of a corporation in the Japanese stock market
11	**Smith et al. (2010)**	Investigating 10 case studies of public companies which affected by cybercrime with the aim of finding its impact on marketing activity and shareholder value.
12	**Aytes et al. (2006)**	Examining the impact of announcements of the information security breaches on the value of stock prices. Additionally, investigating the effects of those announcements on the portfolio of the firm's competitors with the effort to examine whether there is a contagious effect and analyzing the competitive intra-industry effects.
13	**Bolster et al. (2010)**	Investigating whether information security breaches result in significant economic losses and whether the venue of announcement has an impact on business valuation or not.
14	**Bose and Leung (2013)**	Revealing the fact that whether adopting identity theft countermeasures are worthy for a firm or not.
15	**Ettredge and Richardson (2002)**	Describing the risks of e-commerce with a sample of Internet and other firms by assessing the effects of hacker attacks to stock market values of a firm.
16	**Bose and Leung (2014)**	Investigating the impact of the phishing announcements released on the market value of publicly listed firms.
17	**Leung and Bose (2008)**	Examining the impact of the phishing announcements indirectly on the firm value.

18	**Gatzlaff and McCullough (2010)**	Studying the cost of data breaches through the change in the market value of publicly traded companies where the personal information is exposed.
19	**Hovav and D'arcy (2003)**	Reporting the Denial-of-Service (DOS) attack announcements' impacts on the market value.
20	**Hovav and D'arcy (2005)**	Analyzing the effect of the public virus announcements on the market value of responsible IT vendors.
21	**Hinz et al. (2015)**	Assessing the reaction to the data theft announcements on companies' stock prices.

There are various researches in the literature which measure the effects of the cybersecurity risks on the public firms as can be seen above. The research papers between the numbers 1 and 9 are measuring that effect in general terms for the firms which are publicly traded in the US stock market. The research number 10 measures also the general effect of the cybersecurity incidents on the stock prices; however, the stock market based on is the Japanese Stock Market rather than the other research that made on the US stock market.

The studies 11, 12 and 13 have extended the aim and ask whether the cybersecurity incidents have effect on the marketing activities, the public announcements of cybersecurity incidents have effect on a portfolio of the firm's competitors or not and whether the venue of incident announcements has an impact on business valuation.

The research papers between the numbers 14 and 22 have focused only one type of security breach as identity theft, hacking, phishing, data breaches.

The dissertation differs than the research in literature in numerous ways. First of all, the sample size is greater than all of the research in the literature. The most important limitation was the lack of sample size as indicated in most of the research in literature. Also the time frame that is used by collecting the sample size is wider than all the research in literature.

The first question investigates whether the publicly listed companies affected from the IT related cybersecurity incidents or not. With of the biggest sample sizes and the widest time frames in the literature there will be a comprehensive analysis on that general question.

The dissertation also investigates the effects of the IT related failures on manufacturing and service organizations separately in its second research question. After dividing the sample into two as manufacturing and service companies there is also an analysis about the effects on sectoral base. There is an analysis about which sector is affected the most from the announcement of IT related failures. While collecting the data, the lost record size related to the cybersecurity incident is also collected whenever it is convenient. Upon this data, the dissertation also measures whether the lost record size has an effect on the impact of the incident or not in the fourth research question. As the last research question, the dissertation aims to find if the “Hacking” is the greatest cybersecurity issue. The reason “Hacking” has been chosen for being the most well-known cybersecurity type among all the other types.

1.6. ORGANIZATION OF DISSERTATION

This dissertation consists of 6 chapters. The present chapter is the “Introduction” chapter. The rest of the dissertation proceeds as follows:

Chapter 2 begins with the History of Information Technology for having a better understanding on the Information Technology world and the related effects of it. Then, IT Usage in Manufacturing and Service Sectors and IT related Risks on those environments are widely explained.

Chapter 3 continues with the IT related risk factors in the literature.

Chapter 4 develops a thorough understanding about the Event Study Methodology that is used in this dissertation and involves the data, sample selection and classification parts.

Chapter 5 discovers the results and discussion about the results.

Chapter 6 is the conclusion to the dissertation and discusses the implications for both academicians and practitioners.

CHAPTER 2: HISTORY OF INFORMATION TECHNOLOGY

This chapter of the dissertation will include the history of information technology in detail. The narrative of the chapter will begin with the mechanical age of the Information Technology and end in today's world technological developments.

2.1. DEFINITION OF INFORMATION SCIENCE

It is important to know the history and the nature of information before making any research in information systems or information technology areas. The base of having meaningful, purposeful and understandable information is having valuable data to be processed and interpreted to meet the information need. The information derived from the data which is timely, accurate, relevant, sufficient and worth its cost could be used to manage business processes.

Information could become by the shape of documented text, it could come with verbal or virtual communication, and it could be a statistical fact or an expression. It has been used for a long time in history. Even everything in the world can be counted as information.

Information and Information Science has different meanings. As Machlup and Mansfield (1983) stated in his study the meaning of the word "information" takes its origin from Latin. The original word was "informare" in Latin which corresponds to the phrase "to put into form" (In this age we are living, we are exposed to any kinds of information and knowledge, however, it is important not to confuse these two terms). For the historian of information science, it is very difficult to distinguish whether information is a process or a product. They should consider that it is whether a text or document or the content of verbal communication or a reflection of meanings.

Information Science represented by Machlup and Mansfield as "a rather shapeless assemblage of chunks picked from a variety of disciplines that happen to talk about information in one of its many meanings" (Machlup and Mansfield, 1983).

Borko (1968) stated the Information Science as the theoretical discipline concerned with the uses of mathematics, systems design, and other information processing concepts; it is an interdisciplinary science that involves the works and expertises of librarians, logicians, linguists, engineers, mathematicians and behavioral scientists. The outputs of the information science lead to an information system. The part of information science is clarifying the conceptual and ethodological foundations on which existing systems are based.

Hayes propounds a not dissimilar view. According to Hayes (1985), the Information science study consists of the means by which organised structures (it is called now 'information systems') process recorded symbols to meet their defined purposes.

Physical world of the information technology and social sciences that includes 'people' as the most important factor is combined and constructed the Information Systems.

Like every other traditional scientific disciplines, Information Science has also a history. The difference between the traditional sciences and information science is that information science is less stable recognizable and tangible. By using information technology and information systems, efficiency could be increased in all the functions of businesses.

Understanding the history of information technology is important for technology dependent studies. It could be considered as a historical inter-discipline. It comes to our day with a combination of science, technology, publishing, libraries, archives and people. Due to the importance of the history of information technology and science, the rest of this chapter is focused on the emergence of this technology and reached out to contemporary use of it.

2.2. DEFINITION AND USAGE OF INFORMATION TECHNOLOGY

While the usage of technology rapidly increasing, the nature of work in all of the workplaces are changing as well. The increasing rate of information exposure and the technology usage leads to some changes in the businesses.

Information Technology has all its advantages like fast data processing, optimization in processes using automation, ensuring better management and coordination between various functions of an organization, data storing and being able to turn that data into usable information, firms of today will gain competitive advantages among the other their rivals.

2.2.1. INFORMATION AND COMMUNICATION TECHNOLOGY HISTORY

Today's youth which is used to explore everything through the help of the Internet should know the fact that the developments only has started 20-30 years ago. In that time, even most practitioners were unaware of that fact. The technological developments have taken its roots in early sixties and by the late seventies & early eighties some major systems have already been established.

Although the developments in Information and Communication Technology exist for 20-30 years, the Information and Communication history goes far back. The history could be split up into four phases, which are: Pre-mechanical, Mechanical, Electromechanical and Electronic (Digital).

Pre-mechanical age is the earliest age of the information technology. It could be said that this era has started in 3000 B.C. where the drawings on the walls of the caves has appeared and finished in 1450 A.D. where first mechanic computing devices have appeared. This era includes communication through speaking, existence of the alphabet, paper and pens, books and numbering systems. The era has continued until mid-1400s and then mechanical age has begun.

Mechanical age has taken place between 1450 and 1840. Some basic Technologies are invented in this era like the Slide Rule (William Oughtred), the Pascaline (Blaise Pascal), Leibniz's Machine (Gottfried Wilhelm von Leibniz) and Babbage's Engines (Charles Babbage).

Electromechanical age is considered as the beginning time of the telecommunication. Big advances have been appeared between 1840 and 1940. Some examples of the innovations are: The telegraph (early 1800s), morse code (in 1835 by Samuel Morse), the Telephone (in 1876 by Alexander Graham Bell), the Radio (in 1894 by Guglielmo Marconi). Census Machine, Punch Cards and the first large scale computer MARK 1 (by Harvard University in 1940) was the milestones of the age.

Electronic age represents the time fence between 1940 and present. There are four generations of digital computing until today. The inventions in this era are the vacuum tubes, rotating magnetic drums, programs written in assembly language which requires a compiler were the elements of the first generation. Transistors instead of vacuum tubes, magnetic tapes and discs, high level programming languages like FORTRAN and COBOL are the elements of second; integrated circuits, operating systems, the programming language BASIC are the elements of the third and the large-scale integrated circuits, CPU, personal computers, and some software products for the personal use are the elements of the fourth generation. Some pioneers from electromechanical and electronic ages could be seen in the section below. Due to the main concern of this dissertation is related to the use of the Information Technology, the most important era for us is the Digital Computing Era.

2.2.1.1. ELECTRONIC DIGITAL COMPUTING ERA

This era contains inventions that could be considered as the first generation of digital computing. Understanding the pioneers of that era and their work would give an insight while studying information technology & information systems. With that purpose, in the following it will be disclosed some important historical milestones of the age, including the erising of the first digital computer.

2.2.1.2. PIONEERS OF DIGITAL COMPUTERS

In the computing history there is an ongoing debate about who is the inventor of the first computer is. There are some outstanding names as Konrad Zuse, Howard Aiken, John Atanasoff, John Mauchly and J. Presper Eckert. Konrad Zuse is recognized as the father of the computer due to his work Z1 and building first programmable automaton. Mauchly and Eckert are known as building the ENIAC which is called the first electronic computer of the world. On the other hand, Atanasoff has won a patent law case against Mauchly and Eckert and take the “inventor of the first computer title”. Howard Aiken, inventor of the Mark 1, is also called the constructor of the first computer because the Mark 1 was electromechanical machine unlike the other all-mechanical computing devices at their times.

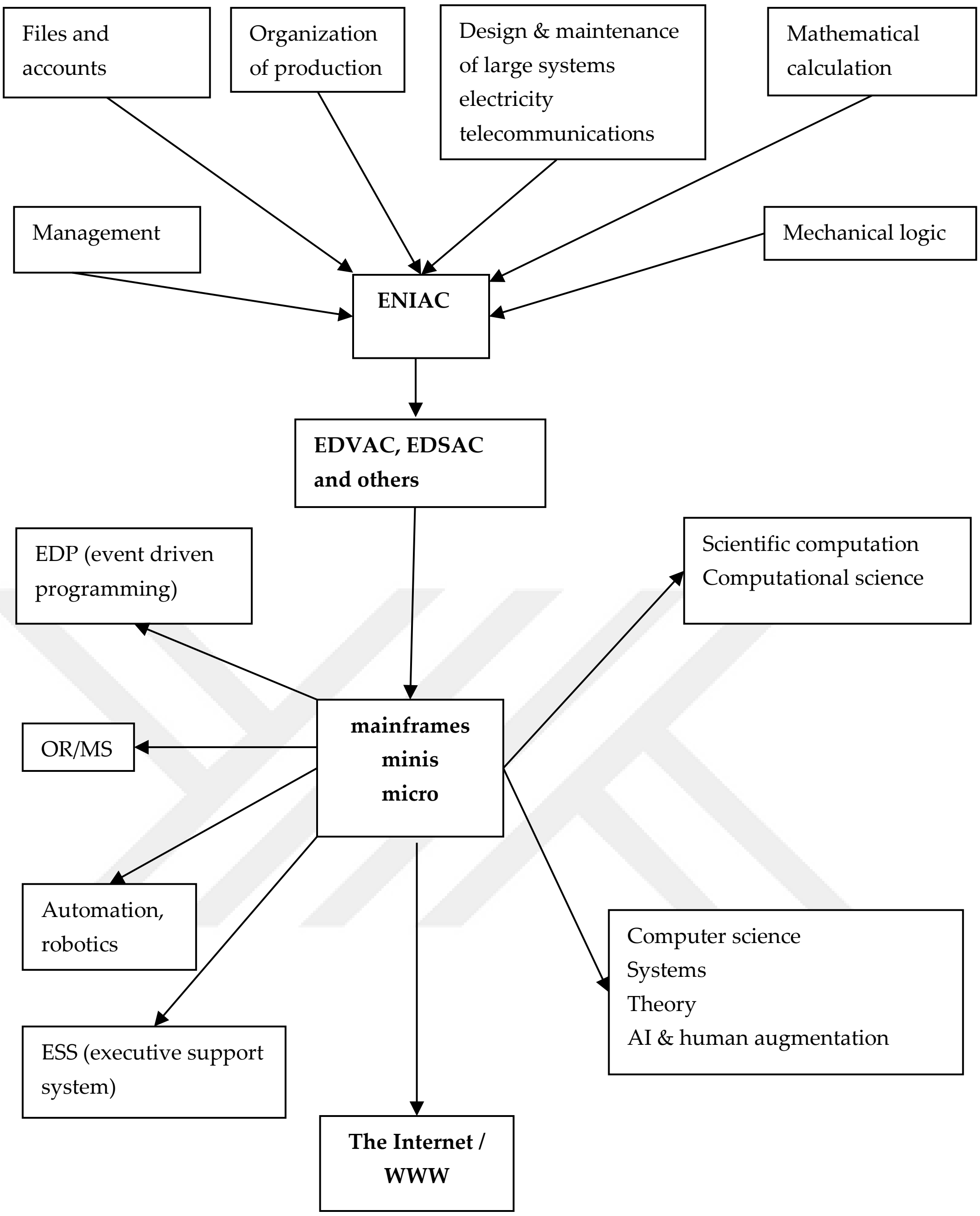

Files and accounts
Organization of production
Design & maintenance of large systems electricity telecommunications
Mathematical calculation
Management
Mechanical logic
ENIAC
EDVAC, EDSAC and others
EDP (event driven programming)
Scientific computation Computational science
OR/MS
mainframes minis micro
Automation, robotics
Computer science Systems Theory AI & human augmentation
ESS (executive support system)
The Internet / WWW

Figure 1: The machine centered version of the history of computing (Mahoney, 2005)

Z1 and Z2

Konrad Zuse, who was a German engineer and inventor, built his first computing machine Z1 between the dates 1936 and 1938. Afterwards, he also built Z2, Z3 and Z4. Zuse is recognized as the father of the computer, and Z1 has been called as the first computer in the world which is a programmable automaton that built between the dates 1936 and 1938 (Rojas, 1997).

Unlike the ABC, ENIAC and MARK 1, Z1 had more flexibility and was designed to execute a long modifiable sequence of instructions on the punch tapes (Rojas, 1997).

TURING MACHINE

Davis (2000) explains that the Leibniz's proposal for an algebra of logic is the point of departure which leads to the invention of the universal Turing machine. According to Davis (2000), "Leibniz dreamt of an encyclopedic compilation, of a universal artificial mathematical language in which each facet of knowledge could be expressed, of calculation rules which would reveal all the logical interrelationships among these propositions. Finally, he dreamed of machines capable of carrying out calculations, freeing the mind for creative thought".

The invention of Turing machine is counted as a milestone in the computing history. The original concept of the machine led to great theoretical advances. The concept of the Turing machine (released in 1936) should be clear to everyone who wants to learn the emergence of the first electronic digital computers.

The ABC

John Atanasoff (1903 - 1995) is the recognized Computer Pioneer in the history of computing. The father of the computer designed the ABC with one of his graduate students, Clifford E. Berry. The initials of the ABC have derived from Atanasoff-Berry Computer and it is built between the years 1939 and 1942.

The ABC was designed to do a special task for the Statistical Laboratory of the Iowa State College. The machine is designed to solve a problem which the lab regularly undertook which hadn't been automated with IBM punched card equipment (Grier, 2000).

In 1940, Atanasoff and Berry wrote manuscripts about the working principles and details of the ABC and were waiting the patent application. The patent applications and manuscripts have not been filed by the Iowa State University, which caused problems in the future.

In 1941 John William Mauchly came to visit Atanasoff's house to discuss and learn how the ABC was working. He leaves his house in a very enthusiastic state about digital computing. Just after 2 years of his visit, Mauchly started to build ENIAC with his college John Presper Eckert in the University of Pennsylvania.

The trial began at 1971. The statement of Mauchly involves that the ABC was a specific-purpose digital computer instead of a general-purpose one. However, in 1973, the Federal Judge Larson decided that "the subject matter was derived" from Atanasoff's the ABC. After that day, the patent rights held by Sperry Rand considered as invalid. Mauchly, his co-workers and wife denied the subject was taken from Atanasoff until the end of their lives.

MARK 1

It is proposed to IBM in 1937 by Howard Aiken and also called as "IBM Automatic Sequence Controlled Calculator". The machine was built between the years 1940 and 1943. Mark 1 is considered as the first electro-mechanical number-crunching computer. The 750,000 parts of the machine produced voice like the operation of a textile mill (Davis, 2000).

Mark 1 funded by the military like the ENIAC and its purpose was doing numerical calculations during the war. After the war, semi-numerical applications as accounting, scheduling and record-keeping have been improved (Davis, 2000).

COLOSSUS

Colossus had high importance for Britain for the effort of breaking the German codes during the World War 2. Based on the evidents, people who played roles for the installation and running of the first Colossus are Thomas Flowers, Alan Turing, William Tutte and Max Newman. Britain's wartime code-breaking establishment was made at the famous Bletchley Park in December, 1943.

Traditionally, Alan Turing was pointed as the key figure of the design of Colossus. However, there is official history that recently declassified that claims he was not

(Copeland, 2004). In the reports, it is declared "Colossus was the idea of Mr. Flowers" (Good et al., 1945).

Colossus was a large-scale special purpose electronic computer has been invented and used for breaking codes during the wartime. The first trial run of the computer has been completed in December 1943. It was just 2 years before ENIAC became operational (Flowers, 1983).

The title of first fully operational programmable computer has been claimed by Colossus project since previous decades. (Copeland, B.J., 2004; Copeland, B.J., 2005).

ENIAC

The ENIAC has been built between the years 1943-1945 at the Moore School of the University of Pennsylvania for the War effort by John Mauchly and J. Presper Eckert and started to operate in 1946. However, it was not delivered to the Army after the war. ENIAC is the short form of Electronic Numerical Integrator and Calculator and considered as the first general-purpose electronic computer. The size of the computer was 150 feet wide and has 20 banks of flashing lights about 300 times faster than Mark 1 in addition. Wallace Eckert was the influencer on the designers of both Mark 1 and ENIAC. The ENIAC was more like a digital calculator and predecessor of digital computers. It only helped on doing mathematical calculations. It can be defined more precisely as "a collection of electronic adding machines and other arithmetic units, which were originally controlled by a web of large electrical cables" (Grier, 2004).

For 32 years long ENIAC was considered as the first digital computer. However, as mentioned above, the ABC won the patent case in 1973 and titled as the first digital computer instead of ENIAC.

EDVAC, BINAC, UNIVAC 1

EDVAC (Electronic Discrete Variable Automatic Computer) is one of the pioneers of the digital computers; it is the next iteration of the design of ENIAC. The difference between them was, while the ENIAC was using the decimal numeral system, EDVAC was using the binary system. The original design of the EDVAC is for solving the problems which are occurred in ENIAC.

It could do things that no earlier machines could have done. It was making logical decisions based on the calculations it was carrying out and was modifying its own instructions (Mahoney, 2005).

ENIAC was a high speed electronic computer and surely it leaded to enormous improvement in the digital computing area, however, it didn't have the ability to save the programs into its memory. For running a new program, computer should be switched off and configured again for a special problem (Haigh, 2011). John Mauchly and J. Presper Eckert (also the designers of the ENIAC) proposed the design of the EDVAC in 1944. They introduced the pioneer approach of the modern stored program electronic computer (Rosen, 1990). The distinguishing feature of the computer was its multipurpose computing ability due to the internal memory it contains.

Eckert and Mauchly, constructors of ENIAC and EDVAC, invented the **BINAC** (BINary Automatic Computer) which was the first general computer for the commercial usage areas and also **UNIVAC** (UNIVersal Automatic Computer).

2.2.1.3. THE RISE OF THE PERSONAL COMPUTERS (1970s-90s)

Building the computers like the MARK 1, ABC or ENIAC was too expensive, so it took a great vision for seeing the manufacturing possibility of something like the personal computers.

The original idea of developing a personal computer is derived from the Xerox Palo Alto Research Center (PARC) (Roberts and Wessler, 1970), although most of the personal computer today are designed and sold by the companies like Apple, IBM, Sony and others (Press, 1993).

Researchers at PARC made a decision upon developing an experimental personal computer, which is called as the Alto and they aimed to duplicate the community surrounding timesharing systems context. This thought led to the development of

Local-Area-Network which became essential for the design of the Alto. An experiment has been made which contained approximately 1000 Altos in a network. At the end of the experiment client-server computing concept emerged (Press, 1993). As the Alto designers has been specified (Metcalfe and Boggs, 1976):

“The high bandwidth communication provided by the Ethernet has been more valuable than anticipated, since we underestimated the importance of servers. The network and network services have been the mainstays of the environment, and we feel that a facility with an order of magnitude lower bandwidth would have had a qualitatively different effect”

In the first years of the development of the personal computers, there was a rapid increase in the production of assemblers, high-level languages, operating systems, CPUs and some modern application in proportion with the allowance of the falling cost (Press, 1993).

Today’s systems are still similar to the Alto, which is an indication of the influence from the developments at MIT, SRI and PARC (Press, 1993).

There are some remarkable examples of the personal computing as Three Rivers Computer Company’s PERQ (1981), Apple Lisa (1982) and Apple Macintosh (1984). PERQ is a workstation computer that influenced from Xerox Alto. Apple Lisa was one of the first personal computers with a Graphical User Interface (GUI). While the “Lisa” project was continuing, the success of the Apple Macintosh has been increased. After that Lisa project has been shut down and brought with some other projects of Apple (Apple II, Apple III) under Macintosh project.

Computing Approach	**Communication Approach**
Batch Processing in **1950s**	Transmit Batches of Jobs
Timesharing in **1960s**	Interactive Terminals
Desktop Computers in **1980s**	LANs (Local-Area Networks)
Portable Computers in **1990s**	WANs (Wide-Area Networks)

Table 2: Evolving of computing/communication approaches (Press, 1993)

Project	Technology
Analytical Engine **in 1838**	Mechanic
Unit-Record Machines **in 1890**	Electro-mechanic
ENIAC **in 1946**	Electronic

Table 3: Major inventions about calculation and programming (Press, 1993)

Project	Technology
Whirlwind/Sage in 1950	Electronic
Timesharing in 1960	Electronic
ARPANET in 1969	Electronic
Alto/Ethernet in 1973	Electronic
The Net in 1996	Wireless

Table 4: Inventions that have played a bridge role between communication and computing (Press, 1993)

Some of the other personal computers that were important in the early development times were: The LINC, the IBM 5100 and the Tektronix 405X. However, the first practical computing machine that sold in the mass-market was the MITS Altair. Altair sold as $397 for a whole kit (Roberts and Yates, 1975).

Today, the intended usage of computers is seen as “communication” between users as Licklider and Taylor (1968) have declared:

"The use of the computer as a communication device . . . promises to bring a new depth of intellectual interchange to the fine old art of fact-to-face communication"

They also presumed their consistence from different geographic places sometimes as small clusters and sometimes as individual workers. The bond that would bring them together will be the common interest (Licklider and Taylor, 1968).

2.2.1.4. FIRST DIGITAL NETWORK & THE INTERNET, ITS INITIAL USE AND COMMERCIALIZATION PHASE

Even though in the history it is referred to the late 1980 as the rise of the Internet networks, the starting point for it goes back to the academic ARPANET of the 1970s.

ARPA (The Advanced Research Projects Agency Network) is encouraged to fund a national network named ARPANET; four nodes began to operate and led to today's developed network age (Press, 1993). As it was said, first ARPANET operation was in 1969 and it was funded by U.S. Department of Defense with the aim of connecting the researchers in different universities (Haigh, 2008).

According to Haigh (2008), the fundamental of the Internet is not the hardware or software, it's the protocols: the rules provide the communication between computer programs. TCP/IP, the data transmission protocol suite of the Internet, is established in the late 1970s. Simple Mail Transfer Protocol (SMTP) was developed in the early 1980s with the aim of realizing Internet e-mail transmissions. The World Wide Web was developed much later than those protocols (early 1990s) but still uses those existing standards of the Internet.

In the mid-1990s the usage of the Internet has become public and that led the increase of the Internet age. The US National Science Foundation's NSFNET played a vital role in the commercialization phase of the Internet, by providing a transition from government to private operations. The role of the NSF was balancing the needs and wants of scientists, politicians and private sector during the transition (Abbate, 2010).

According to the Greenstein (2001), there are four reasons of the success of the commercialization of the Internet. First, the Internet access did not cause any technical and operational challenge as expected. Entrepreneurs discovered the business opportunities that the Internet access will provide. Second, the access to the Internet was manageable as technologically and economically. Entrepreneurs discovered the business opportunities that the Internet access provided. Third, the commercialization promoted the Internet use in new usage areas, new locations, new market usages, new business lines. At last, the Internet access spread at a favorable time which was the growth of the World Wide Web technology.

Commercialization of the Internet has been motivated by some simultaneous events at the time. The restrictions about the commercial usage of the Internet have been removed by the National Science Foundation. There were browser wars which initiated by Netscape. In addition, there was the rapid entry of thousands of firms into commercial ventures using Technologies which uses the TCP/IP standards (Greenstein, 2001). The timing of the events accelerated the privatization process.

ISPs (Internet Service Providers) are one of the important assets of the internet connection. ISPs are the source of most of the households and businesses in the United States (NTIA, 1999). Market for the Internet grew rapidly; it attracted thousands of new users and achieved the mass-market status in short time. Firms offering the Internet service became outspread geographically, which was a rare situation in infrastructure markets. Service firms also did not have one standard menu to provide and this was the indication of the new business opportunity (Greenstein, 2001).

Before its commercialization, the Internet is used exclusively by military, government or for academic purposes. Before 1992, the technology developed at the academic research centers. These operations were small-scaled, usually serving less then several hundred users, were a combination of routine hardware and software applications. A server was required to monitor traffic and be a gatekeeper, a router was required to manage between the Internet and users within a local-area-network, and a connection to the internet was required. The operation could be handled by a small staff (Greenstein, 2001).

Today, searching many forms of media (photos, videos, movies etc.), advertising products, examining products, communication, education, making research as using the Internet as a library are just a few examples of the usage areas of the Internet.

As declared above, the Internet evolved so fast after the 1990s and it has turned its form from being "an academic system base" to world's mostly used tool of daily communication, shopping, travel, entertainment, and business (Haigh, 2008). After the Internet has gone public, the most attractive programs for the users were World Wide Web and e-mail communication.

2.3. USAGE OF INFORMATION TECHNOLOGY IN BUSINESSES

Since the early sixties until the late seventies or early eighties, the world was unaware of the dramatic developments, because social and political upheaval is more outstanding in the daily life (Vietnam War, Watergate, Civil Rights Movements etc.). When the practitioners started to notice the improvements, the major systems were already well established and running the operations (Hahn, 1996).

As years go by, the capacity and the speed of the computers continue to rise with the negative relationship to their size and cost. Now, with the developments of computer hardware, algorithms, databases, floppy disks and CD-ROMs, worldwide network connections and information exchange people get used to the usage of the computers both in their personal life and business life. If "people" are added as an actor to the usage side of the information technology, the result will be the existence of the Information Systems.

In the late 1950s the new concept of Management Information Systems was introduced. Design of the system was for tying all the important operations of a firm together. Firms have adapted the information systems for running their businesses more efficiently by automation. With the usage of these information systems, it was clear that there will be improvement in the way business processes will be handled.

The computer applications for documenting reference retrieval began in the 1950s through the records on the magnetic tapes. The generation of the online retrieval systems is going back to the early 1960s; the time some innovative systems were developed for experimentation. Those prototypes mostly had small databases and operated with one terminal. The systems were sharing the resources of a mainframe computer system and they can run only for limited hours in a day. The mainframe computers which were considered as powerful that day had less ocre memory than today's average personal computers (Hahn, 1996).

Even though back then many databases, new human-computer interfaces and some new hardware technologies like CD-ROM, videodiscs and world-wide interconnected networks are the tremendous innovations, none has represented and valued as it should be (Hahn, 1996).

There were many online retrieval systems in 1960s which are used by small populations. Most of them did not interpass to the commercial or government systems. Today they can only be found in the literature, reports or memories of their users (Hahn, 1996). For acting like a bridge between the information system and the organization, converting the data into information and then knowledge carries great importance of understanding (Rowley, 2007).

With the usage of Information Systems, the organizations will gain so many opportunities for improving the business process efficiency and effectiveness. There are many works in the literature that center on the IT usages and the related impacts. Some of these studies focus on the IT Governance which aims to enable effective usage of IT and by coordination the IT decision making process through the organization (De Haes and Van Grembergen, 2009; Peterson, 2004). While the governance method provides only the coordination between IT decisions and business, the business process bonds the business world and IT world together (Harmon, 2010). Business processes act as a link between the business strategy and IT capability of the firm. There are also some studies that have concentrated on the the interdependencies between IT systems and business processes (Smith and Fingar, 2003; Tarafdar and Gordon, 2007). In addition, IT applications are a driving force for business process reengineering in organizations (Irani, 2002). This IT driven approach for business process management brings process innovation in line with the industrial applications and newly coming Information Technologies (Smith and Fingar, 2003).

2.3.1. THE ROLE OF INFORMATION SYSTEMS

The Information System success research is one of the oldest studies in the area. In the first International Conference on Information Systems (ICIS) which has taken place in 1980, there were many questions about what Information System success is and what are the determinants of IS success (Petter et al., 2013).

DeLone and Mclean (1992) had written a stimulating paper that suggesting the necessity of unrivaled dependent variable of Information Systems success for the Information Systems field.

2.3.2. COMPUTER SUPPORTED COOPERATIVE WORK

Doug Engelbart made a demonstration of NLS in 1968 and there were multiple actors like ARPA, NASA and Rome ADC which participated from different locations (Engelbart and English, 1968).

Electronic mail was enabled by ARPANET in 1969 and is still the most widespread multiuser software and Ethernet was developed by Xerox in 1973. Also, Turoff's EIES system was an early computer conferencing system which took place at the New Jersey Institute of Technology in 1975 (Myers, 1988)

Most of the information systems are used for developing management control process, designing and analyzing and planning coordination. The essential parts of the information systems also are storage, communication, work and presentation of the information. In any business, information is the most important part of the development process (Gupta, 2011). Information Systems also play a vital role in organizations with the knowledge sharing part – after people learn the knowledge sharing possibilities in an organization, they established communities and that is the place where Information Systems become crucial (Von Krogh, 2002).

Organization and competence of individuals in team organizations are two important issues for enhancing employee-involvement and cross-functional collaboration between them (Eklund and Ellström, 2000). For passing the knowledge through the organization, communication flow between workers and team structure become very important, where the technology and IS could be used as a tool for conducting the processes and procedures (Kakabadse et al., 2003).

Firms inner spending on hardware and software was %5 in 1978 and it has increased to %22 in 2005, which is a near percent to the investments in land and structures (Bureau of Economic Analysis, 2007). Even though there was a huge amount of increase in the IT expense, the contribution provided by the IT remained light (Brynjolfsson, 1996; Peslak, 2005). There were studies in the late 1990s (Hitt and Brynjolfsson, 1996; Dewan and Min, 1997; Stratopoulos and Dehning, 2000) which found evidences for positive outcomes from IT spending and some reports from the works (Kivijärvi and Saarinen, 1995; Brynjolfsson and Hitt, 2003) proposed opposite findings because valuing IT usage in businesses takes time. Melville et al. (2004) states that IT is valuable for a firm, however, the level of the value depends on some external and internal factors. Institutional pressure which is counted as one of the external contingent factors has the same importance level as Enterprise Resource Planning systems' (ERP) post-implementation phase (Liang et al., 2007).

Vendor selecting, implementation goal, and implementation time period which are the issues related to the implementation of IT are considered as Internal contingent factors. They are counted as vital factors which can affect a firm's attainment to actualize performance outputs from the ERP adoption (Nicolaou, 2004). Im et al. (2001) stated in their research that announcing a firm's investment on IT also has effects on stock price reactions.

2.3.3. INFORMATION TECHNOLOGY FOR MANUFACTURING

Computers have a fundamental part for effieciency, capability and adaptability increase in manufacturing practices. Some examples of technology integrated manufacturing systems are Computer Integrated Manufacturing (CIM), Distributed Manufacturing (DM), Agile Manufacturing (AM), Cyber-Physical Systems (CPS) and Cloud Manufacturing (CM). The named technologies have been derived from the other existing technologies alike.

For instance, Cyber-Physical Systems are the derivation of the embedded systems and Cloud Manufacturing could be count as the combination of Cloud Computing and Distributed Manufacturing (Yu, 2015).

For making the facility operations more automated, Information Technology was important to adopt in 1970s and 1980s. After early 1990s, there was an increase in the IT investments for buying ERP and SCM softwares in the manufacturing industry. The new technology that used in manufacturing operations raises the efficiency of the shop-floor operations, increases the communication and cooperation between different functional areas of an organization (Akkermans et al., 2003; Banker et al., 2006; Kelley, 1994).

Computer Aided Design (CAD)

In the International Federation of Information Processing Societies (IFIPS) meeting in 1963, a few CAD systems have been introduced. Two of them were Doug Ross's CAD Project (Ross and Rodriguez, 1963) and Coon's work (Coons, 1963) who studied at MIT.

The pioneering work on the interactive 3D CAD system was Timothy Johnson's doctoral dissertation which was finished in 1963 and it was supported by the U.S. Air Force (Johnson, 1963). First system that uses CAD and CAM systems was the DAC-1 of General Motors (Myers, 1988)

Sketchpad program of Ivan Sutherland shows the power of direct manipulation to the world. The program Sketchpad was written for the TX-2, which was a descendent of Whirlwind and was a CAD program. The users could draw directly on the screen with a light pen using the program (Press, 1993).

Today's consumers are demanding the highest quality products and a total product experience which demands together both the information and services from manufacturing organizations (El Kadiri et al., 2016).

In addition, consumers increasingly giving value to the sustainable, pure and real products which makes the industry concern more about the lifecycles of individual products. More new products are introduced by the companies to the market due to the decreased time-to-market and that leads to the shortened product life cycles. Previous to other concerns that mentioned above, manufacturing firms have focused only on the quality improvement of their products despite today's necessity to develop their after-sales market with the aim of staying competitive. Manufacturers which produce complex and high-valued products are looking for new ways to enhance their serviceability by deriving information from the actual usage rate of the products by the customers. Those firms are offering maintenance, updates, upgrades and refurbishing opportunities as service activities and social network services for keeping up with today's consumers' demands (Horvath et al., 2015)

63 terabytes of information were processed in 2008 by the sum of the companies exist in the world and the servers in the world have processed 12 gigabytes for an average day per worker (that makes 3 terabytes information for a worker per year) (Short et al., 2011).

The Internet plays a big role about the situation change about this data flow for companies, now more and more data is available. After these developments in the technological side (data gathering, data flow, data storage), new concepts of business conducting through the help of technology have appeared. One of the trending opportunities that provided by the technology is Internet of Things (IoT) (Gamarra et al., 2016). Now, based on the new technology, more complex products could be produced by more complex production systems which helps to keep up to increasing demand for flexible products (Jain et al., 2013)

Manufacturing operators could use help from some of the technological tools such as information sharing systems or decision support systems for simplifying the complex tasks they need to handle (Mattsson et al., 2014; Wilkinson, 1998) Also information utilization and communication technology (ICT) could be used for this purposes (Karlsson, 2013).

In addition to the positive effects, the organization should adopt to the new changes what technology brings because usage of the decision support systems could bring a negative effect on the workplace environment which is also known as the dysfunctional sociotechnical system (Hendrick and Kleiner, 2001).

Automation technology, which is a self-control technique, could be both implemented on the physical and cognitive areas. Physical automation is implemented to the physical duties and carries on the self-control jobs, conceptional automation is implemented to the cognitive duties. The self-activation level of the jobs would be classified and measured by using levels of automation (Fasth, 2012).

Cognitive automation could be used for information sharing purposes like giving instructions to workers on their new tasks. Technology could also be used to develop information sharing channels. For instance, information and communication technologies can be used for arranging formal and informal meetings between people in different time and space (Gullander et al., 2014)

Consequently, the connection between the every day tools and the Internet could be used to detect their state and information systems could collect data on those objects and processes, which could be used by transforming them into information (Mattern and Floerkemeier, 2010).

Also, the objects could communicate with each other and generate a behaving pattern with a level of intelligence. That kind of thought leads to the researchers to the IoT, which is grounded in advancements in electronics, communications and Information Technologies (Gamarra et al., 2016).

Regarding to the size, price, energy consumption rate decrease of the processors, communication infrastructure and electronic tools, the integration rate to everyday objects has started to a rapid increase. The main aim of the integration with the everyday devices are data gathering, measuring and communication (Gamarra et al., 2016).

Internet of Things (IoT)

Internet of Things (IoT) works by collecting data from different sources (Tsai et al., 2014).

Usage of Internet of Things for manufacturing

Said and Masud (2013) declared the 5-level architecture of IoT:

- Business layer: which runs the IoT applications and process the privacy of management and users.
- Application layer: which determines what kind of applications will be used in the IoT.

- Processing layer: processes the information gathered from the perception layer
- Transport layer: acts like a bridge by receiving and transmiting the information gathered from the perception layer to the processing layer or the opposite way.
- Perception layer: is the technology level of the IoT, determines what kind of technology will be used in it, gathers information from field devices, transformed data into signals in a way they can go through the other levels.

Data Mining

With the help of Data Mining, first, data is transformed and fed into the decision-making process, then patterns are extracted and useful models are created. As a result, data would be transformed into useful knowledge which is ready to be used in different functions in an organization (Tsai et al., 2014).

ERP

ERP is seen as the most important advancement of the information technology for the business use in the 1990s (Davenport, 1998). An ERP system is an integrated software solution that spans the range of business processes that enables companies to gain a holistic view of the business enterprise ERP is an integrated software solution for the business companies and with the usage of an ERP system a company could gain a wholistic point of view to its business process (Ehie and Madsen, 2005).

Along with the usage of ERP, different business functions could be integrated in terms of more effective information exchange and flow and also the integration of different business functions like accounting, finance, human resources, operations, sales, marketing, customer information and even the supply chain (Koh and Saad, 2006; Motwani et al., 2005; Tarn et al., 2002; Kumar and van Hillegersberg, 2000; Palaniswamy and Frank, 2000).

Businesses have adopted the ERP quickly. According to the observations of Willis and Willis-Brown (2002) the ERP market is one of the fastest growing markets in the software industry. Yen et al. (2002) and Adam and O'Doherty (2000) suggest that the growth of ERP will continue to in the next decade and it will remain as one of the influential players in the application software industry.

This growth is achieved despite of the high numbers of failing ERP projects, according to Appleton (1997) nearly %50 of the ERP projects failing to achieve anticipated benefits. Scott and Vessey (2002) indicated that %90 of SAP R/3 projects run late. Even in some cases, companies have even had to close, because the huge ERP investments didn't paid off as in the example of the FoxMeyer Drug Company that went into bankruptcy and closed its doors (Scott and Vessey, 2002).

The ERP implementation cost can be very high (Hayes et al., 2001), these high costs are observed by Cooke and Peterson (1998). They stated in their research that until 1998, 6000 companies had implemented ERP packages and the average cost was $20 million US dollars. Mabert et al. (2001) declares the total implementation cost as "tens of millions" of dollars for a medium-sized company and between $300 and 500 million US dollars for a large international corporation. Companies have to endure with this is financially astronomic burden (Brakely, 1999; Kumar and van Hillegersberg, 2000).

The burden is not only directed to system implementation cost of the ERP, it can also be about the unachieved goals and loss of sales as in the Hershey Foods' ERP implementation example. The company lost US $150 million in sales (Burritt, 2000; Reuters, 1999).

At the end of the consideration, the potential risks outweigh the risks and businesses continue to use the ERP systems at an increasing rate.

Potential benefits of ERP systems is providing to a company a chance to manage its business process with better process flow, improved data analysis, high-quality data for decision-making process, inventory reduction, developed coordination throught the supply chain actors and a more qualified customer service (Gattiker and Goodhue, 2005; Lengnick-Hall et al., 2004; Gupta, 2000; Fan et al., 2000). According to Zheng et al. (2000) the ERP systems help to increase the efficiency of managerial decisions and strategies and the rise of the flexibility which is needed in some business decisions. As opposed to their research, Huang and Palvia (2001) claim that using ERP systems assists the manufacturer or service business while coordinations vital business parts. All of these lead to profit margin increase (Fan et al., 2000).

2.3.4. INFORMATION TECHNOLOGY FOR SERVICE ORGANIZATIONS

Information Technology is described as the most important factor influencing the performance of the economy in the 1990s not only by automating production processes, but also by new ways of organising and managing work, and networking with suppliers and customers, that result in efficiency gains (Stare et al., 2006).

Zeithaml et al. (1990) view improvements in service as being critical elements of a competitive edge in the 1990s, which in turn can be facilitated by improvements in information technology.

It is generally believed that information technology has a positive impact on a firm's performance, though some caution has been mentioned regarding replacing employees in favor of technology (Urgo, 1996). Furthermore, Rubenstein and Geisler (1990) note that to use information technology effectively, one must invest in human resources as well as technology. Considering the effect of information technology on the operations of service firms, Heskett et al. (1990) point out that the use of information technology would affect both the customers and the service providers.

In a recent study, Mathe and Dagi (1996) found that the use of information technology contributes to the success of the implementation of international strategies in service industries.

While ICT as a generic technology can be applied to all industries, the evidence from developed economies shows that service industries are the most intensive ICT users (Pilat, 2003).

CHAPTER 3: INFORMATION TECHNOLOGY RISKS IN BUSINESSES

If there was a system failure in Information Technology, the whole business process will be affected whether it is a manufacturing or service organization. Major risks that have a national impact level regarding to the usage of Information Technology is coming from:

- Natural disasters
- Human error activities
- Economic depressions originated from financial factors
- Technical disasters as in nuclear energy systems

3.1. THE INTERNET RISKS

Information security is a necessity for today's world for preventing risks with great impacts at national level. There are targets to the critical infrastructure, telecommunications systems, computer systems, financial and banking systems, public administration, health or education systems. Today, the largest impact on the society consists of the information technology and the Internet risks (Gaftea, 2014).

3.2. INFORMATION SYSTEM FAILURE CAUSES

Information systems could provide great benefits to both manufacturing and service organizations which use them. However, there are also so many IS implementation failures recorded (Nelson, 2007) which causes the firms facing with negative outputs as financial losses and other risks (Bruque et al., 2008; Laumer et al., 2012; Maier et al., 2013).

After an IS failure, often there occurs a dispute between the software vendor and the user company about the reasons of the failure and the responsible actors for the huge amount of financial loss. For instance, Waste Management, which is a garbage-disposal firm had a $100 million legal battle with SAP over for the 18-month installation of its ERP system. Waste management claimed that management of SAP have taken place in a fraudulent sales scheme which resulted in the failure and SAP responded with the statement that that Waste Management failed to define the business requirements accurately and provide sufficient and knowledgeable users qualified for the project (Wailgum, 2009). In spite of the wide research on the IS failure, the failure rates are not decreasing and failing project still continues to exist (Nelson, 2007).

IS failure studies are being more dominant in the literature for nearly 40 years rather than success studies. These studies are focusing on the gap between the actual performance and required performance (Bignell and Fortune, 1984).

Another definition for IS failure is stated in the research of Ewusi-Mensah (2003) as "either the implemented system not meeting the user expectations or inability of creating working or a functioning system" (Ewusi-Mensah, 2003). In this understanding, while implementing Information Systems in organizations lessons should be learned from the failures. (Scott and Vessey, 2000). In addition, there exist many IS failure related research, description and discussion in the literature and different cause and outcomes have been suggested (Avison and Wilson, 2002; Barker and Frolick, 2003; Beynon-Davies, 1995; Bussen and Myers, 1997; Fitzgerald and Russo, 2005; McGrath, 2002; Nelson, 2007; Pan et al. 2008; Scott and Vessey, 2000).

In addition, there is also a research area that center upon developing countries. Developing countries have high failure rates due to the government related plans and "ICT for development" projects (Heeks, 2002).

Original purpose of IS is developing and integrating the different functions in a business and increasing the efficiency and effectiveness of the processes. It is a fact that using Information Technology in business practices improves productivity, increases efficiency and effectiveness of employees and connects them if necessary. Of course implementing IS has its own challenge and drawbacks and those can cause obstacles for having IS achieving its own objectives. The IT failure studies are split into diverse ways. Some of the studies have tried to reveal the organizational factors which connected to IS project failure (Lyytinen and Hirschheim, 1988). Lyytinen and Hirschheim (1988) ascertained the Information Systems failure causes and came to a conclusion that there are 4 main responsible categories for IS failures: failure of correspondence, failure of process, failure of interaction and failure of expectation. As opposed to their research, Sauer (1993) presented his critization and offered a more conformist explanation for information systems failure. He insisted that an Information System could be assumed to have failed only when development or operation stops, and end-users are disappointed with the degree of the needs-met criteria of the system. Another important cause of the failure is that they are too complex for the employees to operate (Murray, 2000).

3.3. INFORMATION TECHNOLOGY RISK RELATED FAILURE

George David, VP and CIO of Hershey Foods stated in August 22, 2002 in the news release as the follows:

"Hershey's information systems are providing the necessary data to support the transformation of the organization and business processes. The successful upgrade to SAP R/3 4.6 was a critical element of our strategy."

The former CEO and Chairmen of the Hershey Foods Kenneth L. Wolfe indicated in a conference meeting in September 1999 to the analysts of the Wall Street that the company was confronting problems with the new order-taking and distribution computer system which is bought for $112 million dollars and a combination of the ERP (by SAP), CRM (by Siebel) and supply chain softwares. He also stated that these problems were keeping Hershey management to give $100 million worth to Kisses and Jolly Ranchers (Koch, 2002).

Nike also confronted with an information system problem which costs to Nike more than $100 million in sale loss, %20 decrease in stock prices and a number of class action lawsuit. The chairman, president and CEO Phil Knight declared as "This is what you get for $400 million, huh?, a speed bump." Of course Nike could have talked about $100 million like that easily because its 32 percent worldwide market share and a $20 billion market position in the athletic footwear business. They were ahead of the rest of the manufacturers and rivals.

The main objective of Nike was forming a sole, giant, integrated database within its SAP ERP system for its workers in North America and EMEA (Europe, the Middle East and Africa). It was a risky and difficult strategy and the meaning was that everyone has to agree on the business practices and common data definitions

Realizing the information integration throughout a distributed company is not easy and it brought difficulties to many ERP projects. For instance, the drugstore chain FoxMeyer’s SAP ERP system in the late ’90s and Tri-Valley Growers’ integration to the Oracle’s ERP package in 1997. Both companies did not have the chance to have properly working systems, at the end of the struggle they had to shut down their companies. As a result of these bad instances, the other companies gave up having a fully integration and they had installed different sets of ERP systems. According to the statement of AMR, nearly 400 different versions of ERP softwares are installed to a single vendor’s ERP system at some giant companies (Koch, 2004).

3.4. INFORMATION TECHNOLOGY RISK FACTORS

In the aspects of various studies, several concepts have been proposed to determine the Information System failures and its determinants. Lucas (1975), Lyytinen and Hirschheim (1988), and Sauer (1993) were some of the early scholars in this subject. They have examined Information Systems failure both in social and organizational forms. Lyytinen and Hirschheim (1988) have emphasized the correspondence importance, process and factors of interaction. In addition, Sauer (1993) highlighted the termination factors causing IS failures.

The IS failure studies in the early days has been expanded in the last decades with more concentration on IS projects or project managements. Nelson (2007) analyzed 99 Information Systems projects in his research and found 36 standard faults which leads to the reasons why an IS fails. Those mistakes are grouped into 4 categories as: process, people, product, and technology. First group is the "process" and it focuses on IT project management factors, including the management process and technical project management methodologies. The second category, people, indicates the factors related to people which are the actors of a project. Third category is the "product" and it shows the project characteristics like the extent or the priority of the project. As the last category, the technology, it could be said that the IS failure factors comes from the misusage of the new technology.

There are also additional studies (e.g. Al-Ahmad et al., 2009; Barclay, 2008; Dwivedi et al., 2013; Kappelman et al., 2006; Schmidt et al., 2001; Wallace et al., 2004; Yeo, 2002) that found some common ground for the failures of the Information System projects and the "project escalation" is one of them (Keil et al., 1998). Strong and Volkoff (2010) have developed a technology focused categorization of enterprise system failure in organizations and proposing "organization-enterprise system misfit" concept to explain IS failures. Their findings state that misfitting situations in functionality, data, usability, role, control, and organizational culture could increase the failure risk.

Kelly (2003) claims that there is not a concept as a computer project. The real case is the business change projects including the Information Technology. For the successfully implementation stories on those types of projects, the people factor should be considered. The issues about the project should be explained to them, motivation and training should be provided and it should be explained them how the productivity will fall in the way while moving from old way of doing things to the new way.

"User resistance" issue also takes an important place in the IS failure literature (Bhattacherjee and Hikmet, 2007; Hirschheim and Newman, 1988; Laumer and Eckhardt, 2012). Researchers also study on the reasons of the end-users' resistance while using the Information Systems and behavioral patterns like resistance, non-usage or sabotage (Gibson, 2003). Klaus and Blanton (2010) identified some sources of user resistance in their research; they pointed the importance of individual, system, organizational, and process issues of user resistance causing IS failure in organizations.

A comprehensive study about the main causes for the Information Technology related project failures was carried out by a group of researches (Schmidt et al., 2001). The research is conducted with different project managers on three different locations, which are: Hong Kong, Finland, and the United States. 53 Information Technology risk factors have come down to the surface throughout the study. The list is shortened to 17 items by ranking and paring down. The 17 items could be read as below:

- Inadequate commitment of the top management to the project
- Not being able to understand the user requirements in the right way
- Not being able to manage the changes smoothly
- Not gaining user commitment successfully
- Having inadequate user involvement
- Conflict between different departments of users
- Scope and objectives changes
- Number of organizational units involved
- Failing while trying to manage end-user expectations
- Insufficient understanding of scope and objectives.
- The lack of proper roles and responsibilities definitions.
- Not enough frozen requirements
- New technology introduction to the organization
- Not having of effective project management through the organization
- Not having effective project management methodology through the organization

- Not having enough team knowledge and skills
- Having insufficient and inappropriate staff in organization

3.4.1. Network Partioning: There are two options for Network Partioning: partitioned & non-partitioned. Virtualization and network resource partitioning strategy is used for lowering the chance of network attacks. The separation of network resources limits the resource access in a partition. As a result of that action, the system that exists in one partition cannot reach the resources in another one. Unauthorized access to resources and malware expansion is prevented by using that strategy (Souppaya et al., 2011).

3.4.2. Network diversity types are homogeneous and heterogeneous. If a firm uses homogeneous type of network, it uses a single protocol software or technology in each level its network's architecture. Using homogeneous networks reduces cost and improves interoperability in comparison with using heterogeneous networks. However, homogeneous networks stay more defenseless against the malicious attacks; when there is a security gap, whole system can be affected negatively against a single vulnerability. In contrast to the homogenous network, heterogeneous networks use different protocols and different implementations, so when there is an attack to a weakness in the system it doesn't affect the whole network (Zhang et al., 2001).

3.4.3. Wireless status is wireless connection and wired connection. The entire defense gaps that wired connectivity have is valid for the wireless connected networks, however, some could be more severe in wireless connections and also some new security gaps exist for them.

Also it is stated in an NIST report as:

The most important risk cause in wireless networks is the technology's communication understructure, the airwave, and vulnerability to invaders which makes easier to intrude in an Ethernet port (Karygiannis and Owens, 2002).

3.4.4. Network footprint types are: distributed and centrally managed. If an organization uses the distributed communication network, all stations are connected to their adjacent station unlike the centralized system connection through a few switching points. The positive side of using a distributed network for communication is under possible enemy attacks the connection understructure of the firm has greater chance of survivability (Baran, 1964).

3.4.5. Connectivity types are high connectivity and low connectivity. The term is about the network availability concept, which means the network's ability to stay as operational if some elements of the network crash (Clemente et al., 2005).

CHAPTER 4: METHODOLOGY

Event study methodology is used in this dissertation for being able to assess the effects of Information Technology related breaches. 3 models have been used for measuring the effects and comparing the results: Market model, market-adjusted model and mean-adjusted model. Efficient markets hyphotesis which created the foundation for the event study methodology is also explained in this chapter.

4.1. EVENT STUDY METHODOLOGY

Event-study is the accepted method for examining the effects of the public announcements on stock prices of listed firms and the related studies have taken place in the literature since the late 1960s. Efficient capital markets concept of Fama (1970) offers a concrete theoretical foundation for the event study methodology by indicating the stock market is "informationally efficient" and the stock prices reflects all the available information of a firm. Fama (1991) also states that if there is new information in the market, such as the new technology usage in a firm, stakeholders will reflect their opinions to the firm's stock prices and there will be a change in the value of the firm. In brief, there could be experienced a positive (upwards) impact on the firm value due to the information announcement (Konchitchki, 2011).

The underlying principle of the methodology is based on the expectation of an unexpected event will cause positive or negative reaction in the stock prices of a firm and the return of the stock prices will become abnormal. The normal return estimation of a firm is derived from the previous stock price returns and when it is abstracted from the actual return, the abnormal return could be obtained. If the calculation gives positive results, then the event's impact to the stock price of the firm is assumed as positive. Similarly, if the result is derived as negative, the impact to the stock prices is assumed as negative. The characterization of the estimation model is dependent to the number of factors that are used to estimate the normal return (Spanos and Angelis, 2016).

There are different usages of this methodology in the literature. For example, Karpoff and Rankime (1994) have focused on the impact of changes in the name of the corporate and witnessed that the changes had insignificant impact when they use a two-day period. Cooper et al. (2001) made an analysis about the dot-com effects on the companies which had "-com" at the end of their names and drew a conclusion that they had an abnormal return on the order of 74 percent over a 10-day window. Hendricks and Singhal (1996) examined in their research the impact of the announcements which are related to the quality-award winning situation on the market value of firms and the results have showed positive abnormal returns for the firms which won quality awards.

Event study methodology has also been used in information systems related studies. Hayes et al. (2001) stated that the effect Enterprise Resource Planning systems provide is the benefit of increased firm efficiency and effectiveness which could be observed in the growth of the financial performance and competitive position of the firm.

Jeong and Lu (2008) studied the effect of the Radio Frequency Identification (RFID) usage in the manufacturing sector and confronted with a superior market reaction that points the benefits of the technology.

Subramani and Walden (2001) determined that e-commerce related announcements of firms have resulted in significant increase of the stock prices.

4.1.1. EVENT STUDY METHODOLOGY FOR INFORMATION TECHNOLOGY FAILURES

Currently, the Internet and Information Systems are taking a major role in the business world due to their capability of providing powerful managerial tools for the firms. Further, it can be said that the most of the operational procedures are using these tools for accomplishing companies' goals. However, despite the supporting nature of the Internet and information systems there are threats to information systems security. It is a fact that getting completely rid of the vulnerabilities is unfeasible despite the complex security assurance which is gained through advanced infrastructures, protocols, mathematical tools and algorithms. Meanwhile, the attackers are also developing the technological sides of their malevolent systems; as a result, information security is a continuously evolving research field both in academia and in business world (Spanos and Angelis, 2016).

The first investigation of the relation between information security related events and the stock price of the firms was in the early 2000s. The first events that are analyzed were the information security breaches, which are successful attacks to information systems by hackers with the aim of harming confidentiality, availability or the integrity of a system (Spanos and Angelis, 2016).

Some of the important researches that investigate the impacts of the information system security impacts using event study methodology can be seen in the table below:

Table 5: Event Study Methodology usage in Information Systems failure

Authors, Date	Type of Event	Number of events	Sample Time Interval	Event Window	Model
Acquisti et al., 2006	-Data Breaches - Practices about bad security - Attacks of hackers - Attacks of insiders - Other (individual data handling or the illegal sale) - Computer thefts or data thefts - Lost data or lost equipment	79 events	2000-2006	One-Day Event Window	Market Model, Market Adjusted Model, Mean Adjusted Model
Andoh-Baidoo and Osei-Bryson, 2007	Internet security breach	110 events	1997–2003	Three-day event window	Market Model
Arcuri et al., 2014	Information security breaches	128 events	1995-2012	Various event windows	Market Model

Aytes et al., 2006	Information security breaches	67 events	1995-2005	Five-Day event window	Market Model
Bolster et al., 2010	Security breach	76 events	2000-2007	Three-day event window	Market Model
Bose and Leung, 2013	Security Breaches	87 events	1995-2012	Five-Day event window	Market Model
Campbell et al., 2003	Information security breaches	43 events	1995-2000	Three-day event window	Market Model
Cardenas et al., 2012	Security Breaches	38 events	2002-2008	Three-day event window	Market Model
Cavusoglu et al., 2004	Security Breaches	66 events	1996-2001	Two-day event window	Market Model
Chai et al., 2011	Security Breaches	101 events	1997-2006	Various event windows	Market Model
Ettredge and Richardson,	Denial of Service	6 events	February 2000	Three-day event	Market Model

2003	attacks			window	
Gatzlaff and McCullough, 2010	Breaches of customer and/or employee data.	77 events	2004-2006	Two-day event window	Market Model
Goel and Shawky, 2009	Security Breaches	168 events	2004-2008	Five-day event window	Market Model
Gordon et al., 2011	Security Breaches	121 events	1995–2007	Three-day event window	Market Model
Hinz et al., 2015	Data Thefts	6 events	2011-2012	Various event windows	Market Model
Hovav and D'arcy, 2003	Denial of Service attacks	23 events	1998-2002	Various event windows	Market Model
Hovav and D'arcy, 2005	Virus attacks	92 events	1988-2002	Various event windows	Market Model
Ishiguro et al., 2006	Information security incidents	70 events	2002-2005	39 day event window	Market Model
Kannan et al., 2007	Security Breaches	86 events	1997-2003	Various event windows	Market Model
Modi et al., 2015	Customer information	146 events	2005-2010	Various event	Market Model

	security breaches			windows	
Pirounias et al., 2014	Security Breaches	105 events	2008-2012	Various event windows	Market Model
Telang and Wattal, 2007	Vulnerability	147 events	1999-2004	Various event windows	Market Model, Market-Adjusted Model, Mean-Adjusted Model
Yayla and Hu, 2011	Security Breaches	123 events	1994-2006	Various event windows	Market Model

The market value change of firms due to the system breaches have been focused by the prior event study analyses on the information security area (Cavusoglu et al., 2004; Kannan et al., 2004). The results of those studies indicates that a security breach announcement effects the Cumulative Abnormal Return (CAR) of a firm negatively when there is an information system breach takes place.

According to the previous studies, the Information System security breaches have impact on both direct and indirect costs of organizations (Coursen, 1997; McAfee and Haynes, 1989) and they could affect the firm's market value negatively (Campbell et al., 2003; Ettredge and Richardson, 2003; Hovav and D'Arcy, 2003).

Campbell et al. (2003) employed event study methodology in their research and found that the impact of confidentiality-related security breaches is negative and significant and the impact of non-confidentiality related security breaches is not significantly different from zero. They indicated that the breached firms had loss in their value over a two-day period, and attacks involving access to confidential data has led to greater drawbacks than attacks did not.

Cavusoglu et al., (2004) state in their research that, breached firms have faced with a 2.1% decrease in their market value within the two-day window. In spite of the situation, no negative abnormal returns have been detected in the analysis for observing the market reaction to attacks that prevented resource availability. According to them, it is impossible to make a direct quantification of the costs related with the breaching of consumer trust and confidence; however, an indirect estimation could be made by taking capital market valuations of the firms into account (Cavusoglu et al., 2004).

Ettredge and Richardson (2002) have presented first study for measuring security breach effects on the capital markets. They examined the February 2000 DOS attacks and the stock market reaction to them and finally they found that Internet firms have suffered from market reactions more severely than brick-and-mortar firms.

Bharadwaj and Keil (2001) have studied on the IT failure announcements' impact (including DOS attacks on capital markets) and they've found significant decrease in the market value of firms when there is a failure happening.

By facing the negative consequences of the security gaps, the firms have come to a greater understanding of the importance of security and even that understanding phase assessing the economic value is still challenging. In general terms, firms have considered security as an insurance policy which reduces consequences rather than prevents those (Cavusoglu et al., 2004).

To sum up, the study of Cavusoglu et al. (2004) uses the event-study methodology as the works of the mentioned authors, but so far the research has the first large scale research of the security breach effects of on capital markets. With the data set scale, their study becomes different from the earlier works of Ettredge and Richardson (2003) and Bharadwaj and Keil (2001). Unlike the work of Ettredge and Richardson (2003), it isn't restricted with the analysis of only DOS attackes, it considers all types of breaches. While the paper of Bharadwaj and Keil (2001) focuses on study security breaches among several other types of IT failures (only DOS attacks considered), they focused exclusively on security breaches.

Cavusoglu et al. (2004) looked at sixty-six announcements about Internet security breaches from 1996 to 2001. The results suggest that financial markets react negatively to such announcements. Furthermore, financial markets seem to respond more negatively when security breaches are released by smaller firms. Also stocks of Internet firms seem to be more affected than stocks of traditional firms.

A wide set of data (79 events) indicating the exposure of personal information has been analyzed by Acquisti et al. (2006). The reason of the exposure was the failure in the security mechanism (hacking, stolen or lost equipment, poor data handling etc.). According to the results of their analyses (including event study analysis), there exists a negative and statistically significant impact of data breaches on the market value of the company on the announcement day of the breach.

Ettredge and Richardson (2003) compared stock movements of four companies (Amazon, eBay, E*Trade, and Yahoo!) whose websites were subject to hacker attacks, with 275 other companies which were not attacked. The abnormal returns were calculated for three days: February 7, February 8, and February 9 of 2000. Stocks of companies providing security products appear to benefit from reports of hacker attacks.

Hovav and D'Arcy (2003) found similar outcomes as the Denial of Service (DoS) type attacks are not related to any important value loss for firms. They have also examined stock market reaction to Denial-of-Service (DOS) hacker attacks on corporate websites. This study examined twenty-three public announcements about DOS incidents released from January 1, 1998 to June 30, 2002. According to the results, the stock market seems to not react negatively to such announcements. Hovav and D'Arcy (2005) also examined stock market reaction to announcements about defective IT products. This study looked at ninety-two announcements collected from 1988 to 2002. In general, the financial markets appear not to penalize companies which announce that they sold defective IT products in the past.

However, the results suggest that the stock market reacts negatively to announcements of IT products containing computer viruses.

Andoh-Baidoo and Osei-Bryson (2007) examined stock market reaction to Internet security breaches and used forty-one announcements for the years 1997-2003. Decision tree induction was used for assessing the magnitude of the stock market reaction. This study confirmed that stock markets react negatively to Internet security breaches. The characteristics of the attack and firm size are among influential factors.

Telang and Wattal (2007) looked at the effect of software vulnerability disclosures on the stock market. The study examined 147 announcements about software vulnerability lapses from January 1999 to May 2004. In contrast to an earlier study conducted by Hovav and D'Arcy (2005), which did not find a significant stock price reaction, Telang and Wattal (2007) found the stock market reaction to such announcements to be overall negative.

Kannan et al. (2007) used 102 events involving 60 companies to analyze the market reaction to information security breaches. Their results show that the overall negative abnormal market reaction was limited to the time period following September 11, 2001.

The study of Gordon et al. (2011) investigates the information security breaches announcement effects for an extended period as 1995-2007 for 121 incidents in total. The impact was examined for two sub-periods as before and after the 9/11 attacks and investigates if there has been a shift in costs of information security from one sub-period to the next. Major finding of the study is the impact of information security breaches on the stock market returns of firms is significant in general. However, the security breach impacts have shifted over time.

Goel and Shawky (2009) examined 168 incidents of corporate security breaches during the period 2004 to 2008, and found significant impact on the financial performance of the firms.

The study by Yayla and Hu (2010) looked at the effect of contingency factors in security events based on 130 firm-specific security breaches between 1994 and 2006.

The efficacy of the methodology lies in the rationality in the financial markets and the belief that the effects of any substantial event will be reflected instantly in security prices which relies on the efficient market hypothesis of Fama (1970).

4.2. EFFICIENT MARKET HYPOTHESIS

The event study methodology is based on the efficient market hypothesis (McWilliams and Siegel, 1997) and it is important to gain a thorough understanding of EMH for having a better understanding of the event study methodology. The efficient market hypothesis (EMH), known as Random Walk Theory, is a proposition that current stock prices fully reflect current information on the value of a firm and that there is no way to earn excess returns using this information (more than the market). This theory refers to one of the most basic and exciting issues in finance - why prices in securities are changing and how those changes happen. The term "efficient market" was first mentioned in 1965 by E.F. Fama, which stated that competition will cause "immediate" reflection of new information on the stock prices. EMH is effectively defending any of these techniques (in other words, the advantage gained does not exceed the costs of actual transaction and research) and no one can predict the market and outperform it (Clarke et al., 2001).

There is probably no other theory in the economy or finance that has created a more passionate debate between oppositionists and advocates. For example, Harvard financial economist Michael Jensen wrote, "There is no other theory of economics apart from the Efficient Market Hypothesis which has more solid empirical evidence." Peter Lynch, the investment guru, said, "Active markets? - it's madness."

The Efficient Market Hypothesis (EMH) shows that the gains from estimating price movements are very difficult and unlikely. The main mechanism behind price changes is the arrival of new information. If prices are adapting quickly and without prejudice to new information, the market is called "efficient". As a result, current prices of securities reflect any available information at any point in time. So, there is no reason to believe that prices are too high or too low. The prices of securities are set before an investor makes a profit from trading and a take advantage of new piece of information.

However, when prices are based on rationality, it is expected that the changes in prices will be random and unpredictable because the nature of the new information is unpredictable. For this reason, it is said that stock prices follow a random walk. The efficient market hypothesis predicts that market prices should include all available information at any point in time. However, there are different kinds of information that affect the stock values. As a result, financial researchers indicate that the "Efficient Market Hypothesis" has three different versions depending on what is meant by the term "all available information" (Clarke et al., 2001).

3 levels of market efficiency by considering 3 types of information set (Roberts, 1967):

4.2.1. WEAK FORM EFFICIENCY

Weak form of the efficient market hypothesis emphasizes that the stock prices fully reflect all the market information stored in the historical sequence of prices.

Therefore, investors cannot perform an investment strategy to yield abnormal profits by analyzing the past price patterns (technical analysis). This form of efficiency is associated with "Random Walk Hypothesis".

Weak form of efficient market hypothesis argues that the current price incorporates the information contained in the past history of prices. That is, nobody can detect securities which are falsely priced and cannot beat the market by analyzing past prices. The hypothesis has taken the "weak" name for the following reason: stock prices are the most public and most readily available piece of information without dispute. Thus, analysts should not benefit from information that "everyone knows". On the other hand, many financial analysts try to generate profits by working on historical stock price series and transaction volume data, thinking that what this hypothesis suggests is worthless. This technique is called technical analysis. The empirical evidence of this market efficiency form and therefore the evidence it shows against the value of the technical analysis is quite strong and consistent. Once you have considered the analysis and transaction costs for trading securities, it is very difficult to make money with publicly available information such as past sequence of the stock prices (Clarke et al., 2001).

4.2.2. SEMI-STRONG FORM EFFICIENCY

The semi-strong form of efficient market hypothesis points that stock prices do not only reflect historical price information but also they reflect publicly available information related to a company's securities. If markets are efficient, the analysis of income statements, balance sheets, announcements about dividend changes or stock splits, or any other kind of public information will not yield abnormal profits.

The semi-strong form of the efficient market hypothesis reveals that the current price entirely includes all public information. However, public information is not only about past prices but also about the financial statements of a company (annual reports, income statements, filings for the Security and Exchange Commission, etc.), earnings and dividend announcements, merging plans announcements, financial positions of competitors, macroeconomic factors (as inflation, unemployment, etc.). In fact, the public knowledge should not necessarily have to be financial. For example, for analysis by pharmaceutical companies, relevant public information may include current research on analgesic drugs.

The argument behind the semi-strong market efficiency is still that one should not make a profit from information that "everyone knows". However, this assumption is much stronger than in the weak form of the hypothesis. Semi-strong market efficiency requires not only the financial economists who can grasp intense financial knowledge but also the existence of macroeconomists who can understand the processes in the product and input markets. Obviously, it takes a lot of time and effort to acquire such skills. In addition, the collection of "public" information can be relatively difficult and costly to process. For example, it may not be enough to obtain information from major newspapers and publications produced by companies. The wire reports, professional publications and databases, local newspapers and research journals need to be followed to collect all the information necessary to effectively analyze securities (Clarke et al., 2001).

4.2.3. STRONG FORM EFFICIENCY

The strong form of efficient market hypothesis points that any “known” information by any participant of a company is already fully reflected by market prices. Thus, even with the privileged information holders cannot use it to secure superior investments.

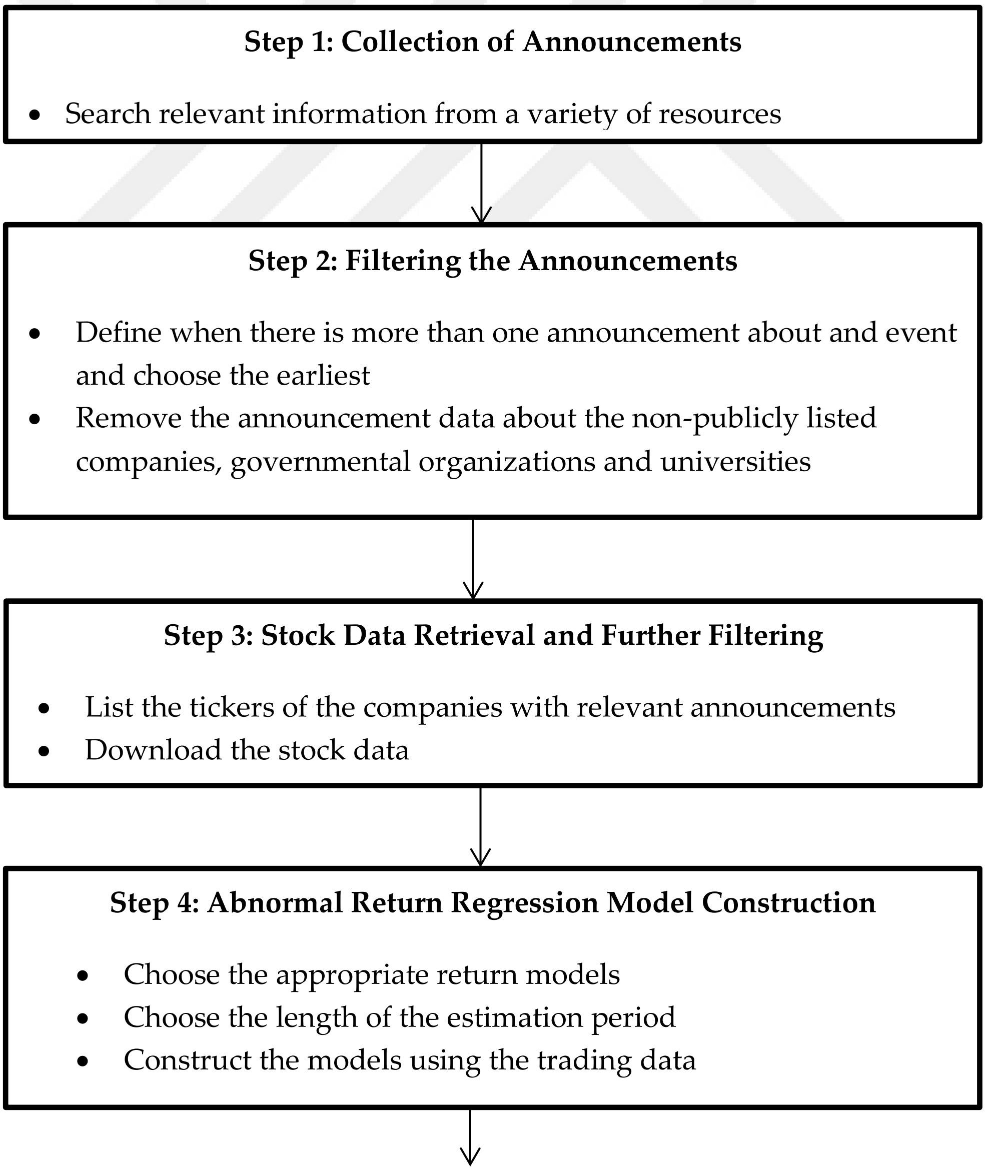
The strong form of the efficient market hypothesis is that the current price includes all available information both public and private (sometimes called insider information). The biggest difference between the semi-strong and the strong forms is that in the second case, even if trading is done on information that has not yet been disclosed to the public, no one should profit systematically. Which means that the strong form of EMH indicated that the management of a company (insiders) is not able to systematically gain from inside information by buying company’s shares ten minutes after they decided (not publicly announced) to continue what they observe to be a very profitable acquisition. Similarly, members of the company's research department cannot benefit from information about the new revolutionary discovery they completed half an hour ago. The rationale for strong-form of EMH is that the market can expect future developments in an unbiased manner and therefore the stock price may have incorporated the information and evaluated in a much more objective and informative manner than the insiders (Clarke et al., 2001).

Based on the Efficient Market Theory, it is expected that the information security related events will create a negative impact on stock prices. It is also assumed that, publicly announced information security breach related events will create a stock market reaction and that reaction would result in negative abnormal returns (Cardenas et al., 2012).

4.3. DATA COLLECTION AND RESEARCH MODEL

Social scientists have used the Event Study Methodology to study the impact of a specific event on the company value. In this dissertation, the case is the announcement of a security incident.

Below you can see the step-by-step description to how to conduct an event study.



Step 1: Collection of Announcements

- Search relevant information from a variety of resources

Step 2: Filtering the Announcements

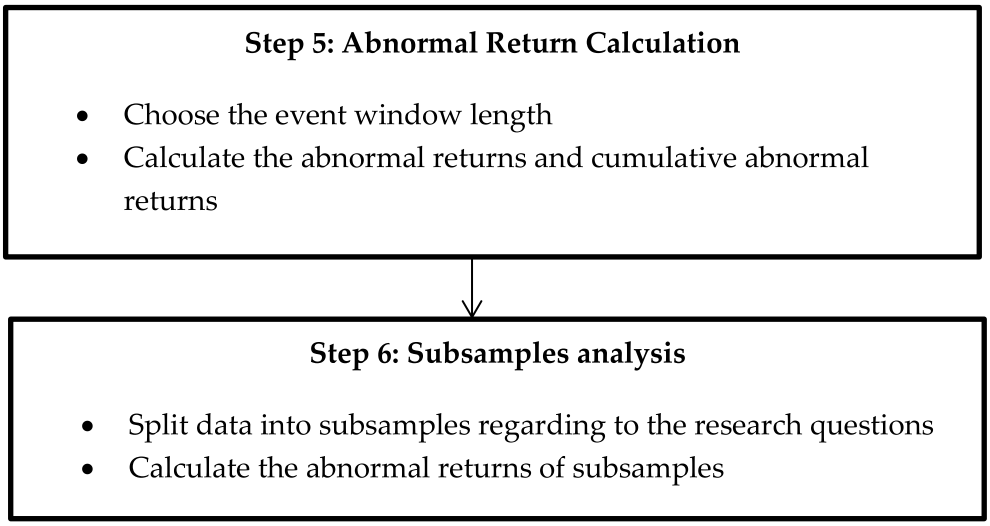
- Define when there is more than one announcement about and event and choose the earliest
- Remove the announcement data about the non-publicly listed companies, governmental organizations and universities

Step 3: Stock Data Retrieval and Further Filtering

- List the tickers of the companies with relevant announcements
- Download the stock data

Step 4: Abnormal Return Regression Model Construction

- Choose the appropriate return models
- Choose the length of the estimation period
- Construct the models using the trading data



Step 5: Abnormal Return Calculation

- Choose the event window length
- Calculate the abnormal returns and cumulative abnormal returns

Step 6: Subsamples analysis

- Split data into subsamples regarding to the research questions
- Calculate the abnormal returns of subsamples

Figure 2: Steps of the Event Study Model

First three steps are more about the data collection part of the model.

In the first step, security breach announcements are collected from a variety of resources as it is explained in the data collection part in a more detailed manner.

In the second step, when there were several announcements about a specific event, the earliest announcement date is retained and the others are deleted. While collecting the announcement that is related to the security incidents, some security breach incidents data from non-publicly traded firms, governmental agencies and universities are seen. Due to the usage of the event study methodology requires stock price information from publicly listed companies, the announcement information about those organizations are also removed. After filtering of the redundant information, the final version of the announcement list is obtained. Second step is also explained in more detail in the data collection part.

In the third step, both Reuters and Bloomberg tickers of the companies are listed in the data collected. However, only Reuters tickers are used during the collection of the stock prices.

In the fourth step, a model should be selected for the calculation of the abnormal stock returns.

In the fifth step, the abnormal return of stock prices is calculated. The abnormal return (AR) shows how the return on a firm is different from the expected return around the security breach incident. So, AR is identified as the difference between the actual return and normal return. Actual return captures the event effect. Calculations have been made according to the three models that are used.

In the sixth step, appropriate subsamples are established based on the organization types, industries, and the cybersecurity incident methods for finding answers to the research questions. The analysis results and discussions about the research questions can be found in the next chapter.

4.3.1. DATA COLLECTION

During the first phase of the data set collection, it is encountered with a vast majority of additional privacy breach incidents in the organizations as the non-publicly traded companies, governmental agencies or universities. With all the data coming from publicly-traded, non-publicly traded and non-profit companies, 317 events between the years 2000 – 2015 are collected. Prior studies; major newspapers of the US as New York Times, Washington Post, Financial Times, USA Today, Wall Street Journal; business magazines as Business Week, Economist; news wires as Business Wire, PR Newswire; technology portals as CNET and ZDNET; number of IT security related blogs, and various sources through the search engines Google and Yahoo! and the website of a non-profit organization named Privacy Rights Clearinghouse have been searched for compiling a comprehensive list of the privacy incidents. The keywords used are: "cyber-attack", "cyber security incidents", "information security breach", "information system incidents", "information system hack", "hacked companies", "information system attack", "computer attack", "computer system security" are used while searching the reports about the cybersecurity incidents. It is not always clear on the media when the initial announcement is made about the incident and for that reason, each event is searched in several outlets for having an exact announcement date and therefore having a more accurate market response. If the exact date of the initial announcement could not be found, the event has been removed from the data list. In some cases, there are several companies which are exposed to a major attack. In those cases, each company is treated as a separate event.

For being able to use the data in the event study approach, the focus should be on the breaches of the publicly traded companies. Therefore, the data related to the Government, Military, Academic Organizations and the data of the private companies that are not publicly listed had to be eliminated from original the data set. Those eliminated data include 111 events between the years 2000 and 2015. The organization types in the eliminated data set include Government, Military, Academic organizations and private companies in the Retail, Tech, Healthcare, Telecoms, Transportation, Financial, Energy industries. The data set related to those organizations can be found in Appendix I for further interest.

After removing 111 events that couldn't be used in the event study analysis, there are 206 events remained which are occurred between the years 2000 and 2015. The cleaned data size that can be used in event study was 206; however, all those events could not be used in the analysis because of the following reasons:

- Some of the companies have been acquired by other companies and data price of the original company that faced the event at the event date could not be found.
- Some of the companies was not publicly traded at the event date
- Some of the companies were publicly traded at the event date, but after some period of time they are delisted, so the market data has been removed.
- Market was closed at the event date.

After the second phase cleaning of the events with the unavailable data, the number of events that can be used in event study is reduced to 172 which have been occurred between the years 2000 and 2015.

The companies that are exposed to the cybersecurity incidents are split into two main groups as manufacturing and service based organizations. The companies can be grouped into 7 sectoral classes which are Communications, Consumer Goods, Energy, Financials, Healthcare, Industrials and Technology. The companies also decompose into 26 industrial groups which are: Aerospace & Defense, Apparel &

Textile products, Asset Management, Automotive, Banking, Biotech & Pharma, Commercial Services, Consumer Products, Consumer Services, Electrical Equipment, Gaming & Lodging & Restaurants, Hardware, Healthcare Facilities & Services, Institutional Financial Services, Media, Oil & Gas & Coal, Passenger Transportation, Retail – Consumer Staples, Retail – Discretionary, Semiconductors, Software, Specialty Finance, Technology Hardware & Storage & Peripherals, Technology Services, Telecom and Transportation Logistics. All of industrial and sectoral information of the publicly traded companies are taken one by one from the website of the Bloomberg. The information about both Reuters and Bloomberg tickers of the companies are listed in the data collected. All of the industrial, sectoral and ticker information of the companies can be found in Appendix II.

While measuring the effects of the incidents on the stock prices the most important issue is the announcement date because of its triggering position on the behavior on the markets. The announcement dates of the incidents which have taken place in media are listed in Appendix III. The events are listed according to their announcement dates in a decreasing rate. Appendix III also includes the method of the leak that a company has encountered. The reasons of the events in the data set can be seen as below:

- Accidentally published
- Hacked
- Inside job
- Lost/Stolen computer
- Lost/Stolen media
- Poor Security

The incidents may have been caused by accidentally published data, hacking, inside job, lost/stolen computer, lost/stolen media or poor security. When there is an outside attacker has been mentioned in the announcement, the cause of that incident is labelled as hacking. If there is lost/ stolen media (stolen mail, hard drives, important documents etc.) or lost/stolen computer, those events are labelled separately. The poor security category comprises the times when internal mistakes are made throughout the company and made the company more vulnerable to the unauthorized access to their internal systems. Inside jobs are the incidents made by trusted parties inside the company with the purpose of making harming in a deliberate way. Accidentally published data incidents are also made by the people who have connection with the company; however, this incident type has no aim to harm the company on purpose. Those types of incidents could be sourced by human errors or system errors.

Table 6 describes the distribution of events across the years. The majority of breaches have occurred in 2006 (%11.63) and in 2013 (%10.47), within the 172 security risk related events. In addition, there was no incident that was reported publicly in 2009.

Table 6: Breakdown of the privacy breaches by year

Year	**Number of Incidents**	**% of Sample**
2015	2	1.16
2014	9	5.23
2013	18	10.47
2012	7	4.07
2011	14	8.14
2010	3	1.74
2009	0	0
2008	7	4.07
2007	10	5.82
2006	20	11.63
2005	16	9.30
2004	12	6.98
2003	15	8.72
2002	7	4.07
2001	15	8.72
2000	17	9.88

Table 7 shows the descriptive statistics of the privacy breaches by the incident types. The overwhelming majority of incidents were due to "hacking" (%62.79) while the other types of incidents made up %37.21 of the sample all together. This situation helped to reveal the fifth research question of this dissertation: "Among all the other IT risks, is "Hacking" the greatest risk for businesses?"

Table 7: Distribution of the number of privacy breaches by the incident type

Type of Incident	**Number**	**% of Sample**
Accidentally Published	6	3.49
Hacked	108	62.79
Inside Job	10	5.81
Lost/Stolen Computer	11	6.40
Lost/Stolen Media	11	6.40
Poor Security	25	14.53
Unknown	1	0.58

Table 8 describes the distribution of events in the data sample according to the type of organization, i.e. whether a firm is operating under a service or manufacturing setting. As it can be seen in the following table the majority of privacy breaches have been occurred in the organizations which are operating under service settings (%82.56). The reason that the incidents are more widely spread in service industries is most likely because the operations of the service industries are more information oriented than the other industries.

Table 8: Distribution of the number of privacy breaches by the manufacturing or service companies

Type of Organization	**Number**	**% of Sample**
Service	142	82.56
Manufacturing	29	17.44

Table 9 describes the number of privacy breaches according to the industry type. Most affected industry is the media industry (%16.28) followed by the telecom and banking industries (%9.88 each). Also the least affected industries are: biotech & pharma, electrical equipment, oil & gas & coal and semiconductors industries (%0.58 each).

Table 9: Distribution of the number of privacy breaches by the industry

Type of Industry	**Number**	**% of Sample**
Aerospace & Defense	2	1.16
Apparel & Textile products	2	1.16
Asset Management	8	4.65
Automotive	4	2.33
Banking	17	9.88
Biotech & Pharma	1	0.58
Commercial Services	2	1.16
Consumer Products	2	1.16
Consumer Services	2	1.16
Electrical Equipment	1	0.58
Gaming & Lodging & Restaurants	5	2.91
Hardware	9	5.24
Healthcare Facilities & Services	4	2.33
Institutional Financial Services	6	3.49
Media	28	16.28
Oil & Gas & Coal	1	0.58
Passenger Transportation	3	1.74
Retail – Consumer	3	1.74

Staples		
Retail – Discretionary	13	7.56
Semiconductors	1	0.58
Software	14	8.14
Specialty Finance	11	6.40
Technology Services	9	5.24
Telecom	17	9.88
Transportation Logistics	7	4.07

Table 10 shows the distribution of the privacy related incidents according to the sector of the event related companies. Most of the events have been occurred in communications (%26.12) and financials sector (%24.42). Descriptive statistics of Table 10 is in line with the statistics in the Table 8, which shows the distribution of the number of privacy breaches by the manufacturing or service organizations.

Table 10: Distribution of the number of privacy breaches by the sector

Type of Sector	**Number**	**% of Sample**
Communications	45	26.12
Consumer Goods	36	20.93
Energy	1	0.58
Financials	42	24.42
Healthcare	5	2.91
Industrials	10	5.81
Technology	33	19.19

4.3.2. RESEARCH MODEL

First of all, measurement of abnormal return (AR) is a necessity to be able to assess the impact of the security breach. The abnormal return could be derived from subtracting the normal stock return over the event window from the actual stock return (observed after the event) (Aytes et al., 2006). For being able to calculate the abnormal performance there is a need for a model for normal returns. To estimate the effect of the security breach incidents, first the firm's stock return should have been calculated without considering the effect of the event. The normal return is estimated in a time period where the security breach incident could not impact the return (in this dissertation, day -250 to -30 relative to the event data). To estimate normal return of a firm, a statistical model should be used that relates the return of any stock's return to the market portfolio. In literature, there are 3 different models followed for the calculation of expected return on the stock: the market model, the market adjusted model and mean adjusted model (Campbell et al., 1997; Hendricks and Singhal, 1996). First model that is going to be used for that aim is the market model which is the most common model used for estimation the expected return MacKinlay (1997). The market model assumes a stable linear relation between the market return and return on the stock. For verification of the results the other two models will also be used: Market-adjusted Model and Mean-adjusted model. By using all of the 3 models, the results will be compared with each other and the dissertation will be strengthened.

After calculating the normal return, event window should be selected because the impact is observed on the event window. The event window is a time period which overlaps the date of the event announcement. The smallest event window is 1 day, which is the day of the announcement or day 0. When the announcement is made on a day when markets are closed, the next day the markets are open will be counted as day 0. Often the event window is expanded to two days, which are day 0 and day 1. Day 1 is defined as the day after the announcement. This expansion is made for capturing the effect of price announcement made after the close of the markets on a particular day. Sometimes researchers include a day before the announcements to incorporate any information leaks about the event (Acquisti et al., 2006).

The typical timeline for an event study could be shown in Figure 3 below:

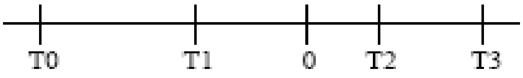


Figure 3: Timeline for an Event Study

Where:

T0 – T1 interval is the estimation period,

T1 – T2 interval is the event window,

0 is the day of the event,

T2 – T3 interval is the post-event window.

So, the event window could be explained as the time window that takes into account T1 days before and T2 days after the announcement date (which is defined as zero). 5 days before and 10 days after (-5, +10) the event is focused in the dissertation, with the purpose of taking before of the event activities into account in a more detailed manner and being able to analyze after the event activities in a more comprehensive way.

The abnormal returns and cumulative abnormal returns are calculated by using three different models (Market Model, Market-Adjusted Model, Mean-Adjusted Model). In addition, for all of these 3 models, three different test statistics are used: Mean Abnormal Return, Median Abnormal Return, and Percent Less than Zero.

The models used for quantifying the impact of the event could be seen as follows:

The Market Model

Investors want to know the level of risk they are taking before they buy a stock. Beta provides them a value which represents the volatility of a stock compared to the stock market.

The first step of calculating the impact of the event is estimating the normal return of the share prices without considering the existence of the event.

The market model used is based on the Capital Asset Pricing Model (CAPM) is widely used and accepted in the literature and the expected return estimations is based on ordinary least squares (OLS) regression. This regression includes the independent variable as the market index for date t and dependent variable as the return of security i at date t.

The single index market model is used to estimate the returns for a firm i at the date t is as follows:

$$R_{it} = a_i + b_i R_{mt} + e_{it} \tag{1}$$

Where;

Rit denotes the normal return for firm i on day t

Rmt denotes the return on the market index on day t

ai denotes the intercept for firm i (y-intercept),

bi is a proxy for the systematic risk of the firm i (slope that measures the sensitivity of Rmt) and,

$eit$is the error term (disturbance term with OLS properties) for the firm i on day t.

Value weighted index is used depending on which market the stock of interest is traded as the proxy for the market portfolio and estimated the parameters of the market model: ai, bi, and eit during the estimation period. The collection of weighted indices for each sample country, their components and descriptions are represented below:

Table 11: Information about indices

Country	**Index**	**Ticker**	**Components**
USA	S&P 500	SPX	500
Germany	DAX	GDAXI	30
Japan	Nikkei 225	N225	225
United Kingdom	FTSE 100	FTSE	100
Italy	FTSE MIB	FTMIB	40
South Korea	KOSPI	KS11	741
India	BSE Sensex 30	BSESN	30
Brazil	Bovespa	BVSP	59

The market index choice reveals the wide set of firms in the sample. The expected return estimation is based on OLS regression. The Ordinary Least Squares (OLS) regression is used to estimate the regression parameters $\propto$ and β. OLS assumes the error terms from regression are independent and identically distributed and they have a mean of zero and are homoscedastic (Campbell et al., 2003). The estimation window varies from one study to another. The shortest estimation period which commonly accepted is 120 days. An estimation period that starts 250 days, a full calendar year, before the event announcement and ends 30 days before the announcement date (day -250 to day -30) is used. This period is used for being able to observe the effects in a broader sense. The 30-day gap between the regression window and the event window is selected to produce robust parameters as a result of the regression estimation.

Based on the estimates of the regression parameters from the market model, abnormal returns could be calculated for the event period. The abnormal return (AR) during the event window for firm i on day t is estimated according to the market model as follows:

$$AR_{it} = R_{it} - \propto_i - \beta_i R_{mt} \tag{2}$$

Where;

i denotes the event ($i = 1,2, \dots, N$),

AR_{it} denotes the abnormal return of event $i$at time t,

R_{it} denotes the normal return for firm i on day t,

$\propto$ and β are the OLS (Ordinary Least Squares) estimates from the market model,

m denotes the market,

t denotes the event day (i.e. t=0 denotes the day of the announcement about the incident),

R_{mt} denotes the market return at time period t.

The abnormal returns are accumulated for each event window to obtain cumulative abnormal returns (CARs).

The Market Adjusted Model

In the Market Adjusted Model, the event window returns are compared to an expected return of the market only over the event period. The abnormal returns are calculated as follows:

$$AR_{it} = R_{it} - R_{mt} \tag{3}$$

Where;

i denotes the event $(i = 1,2, \dots, N)$

AR_{it} denotes the abnormal return of event $i$at time t,

R_{it} denotes the normal return for firm i on day t,

R_{mt} denotes the market return at time period t.

The abnormal returns are accumulated for each event window to obtain cumulative abnormal returns (CARs) as in the market model.

The Mean Adjusted Model

In the Mean Adjusted Model, the returns are compared to the mean market return over the event period. Abnormal returns are calculated as:

$$AR_{it} = R_{it} - R_{i} \tag{4}$$

Where,

i denotes the event $(i = 1,2, \dots, N)$

AR_{it} denotes the abnormal return of event $i$at time t,

R_{it} denotes the normal return for firm i on day t,

R_i denotes the mean return on the stock which made an incident announcement during event i, over the duration of the estimation period.

The abnormal returns are accumulated for each event window to obtain cumulative abnormal returns (CARs) as in the market model and market adjusted model.

Cumulative Abnormal Returns

There is a possibility that the markets do not fully incorporate information instantaneously; therefore, multi-day event window calculation is required. During the event window, abnormal returns are accumulated to calculate Cumulative Abnormal Return.

The abnormal returns during the event window (-5, 10) have been accumulated for each event window to get Cumulative Abnormal Return (CAR). Again, this period is chosen for having estimation in a broader sense.

The CAR for firm i for event window (T1, T2) that begins at day T1 and ends at day T2 is calculated as follows:

$$CAR_i \ [T1, T2] = \sum_{t=T1}^{T2} \mathrm{AR}_{it} \quad \textbf{(5)}$$

Where:

$[T1, T2]$ = the event interval and all other terms are as previously defined.

Then, the CARs are averaged across all firm-events to calculate the mean CAR. For the sample of 172 events the mean announcement effect is calculated as:

$$\overline{CAR}\,[T1, T2] = \frac{1}{N}\sum_{j=1}^{N} \mathrm{CAR}_j[\mathrm{T1}, \mathrm{T2}] \quad \textbf{(6)}$$

Where:

N= the number of events and and all other terms are as previously defined.

The results according to the three models (market model, market adjusted model and mean adjusted model) can be found in the next chapter.

CHAPTER 5: RESULTS & DISCUSSIONS

The results for the Event Study methodology will be explained in this chapter. There are 3 different result sets according to each model used (market model, market-adjusted model and mean-adjusted model) for each research question. Abnormal results and cumulative abnormal results tables are given and t-statistics results for the significance tests of cumulative abnormal results are presented.

5.1. RESULTS

In this chapter, the results are presented for 172 events. The estimation window from -250 to -30 and the event window from -5 to +10 have been used in the analysis.

For having a stronger set of results, all the three models which have been mentioned in the previous chapter (market model, market adjusted model, mean adjusted model) have been tested.

There are five research questions in this dissertation. Three models that have been mentioned have been used to answer all of the research questions.

The research questions and the results of the analysis could be found below.

5.1.1. HAVE THE LISTED FIRMS BEEN AFFECTED FROM INFORMATION TECHNOLOGY RELATED FAILURE?

The first question examines if the listed firms have been affected from IT related failures or not. Overall sample (172 events) has been used to answer this question.

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are presented below. The comparison of the results according to each model can be seen in the last graphic.

ABNORMAL RETURNS

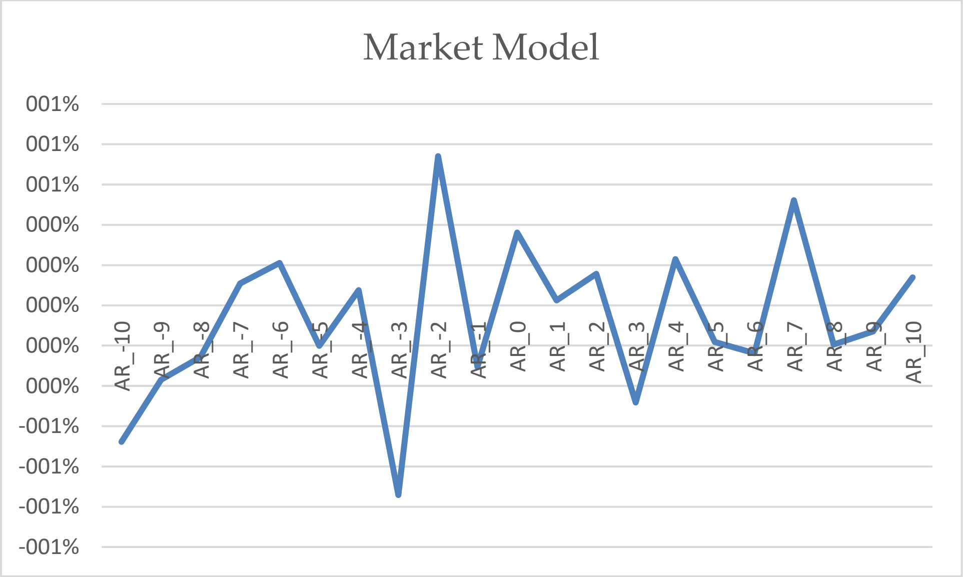


Figure 4: Abnormal returns by market model for all the firms in the sample

Figure 4 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. After the event day (the announcement of the event on day 0) the values showed a slow decrease and then a sharp decrease in day 2. The values showed an unstable stance after the event day.

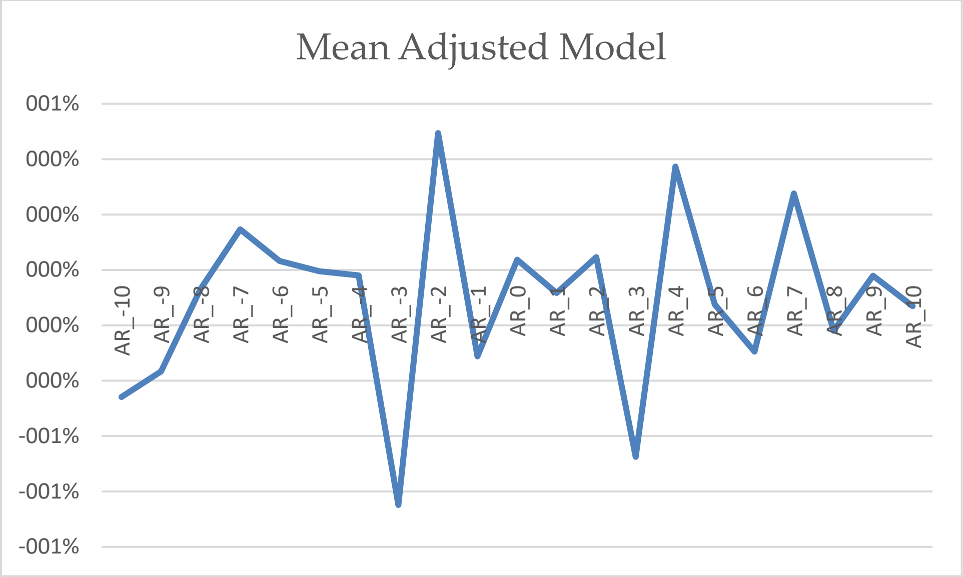


Figure 5: Abnormal returns by mean adjusted model for all the firms in the sample

Figure 5 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. The results become negative one more time on day -1 and increased after day -1. There is another large negative value on day 3.

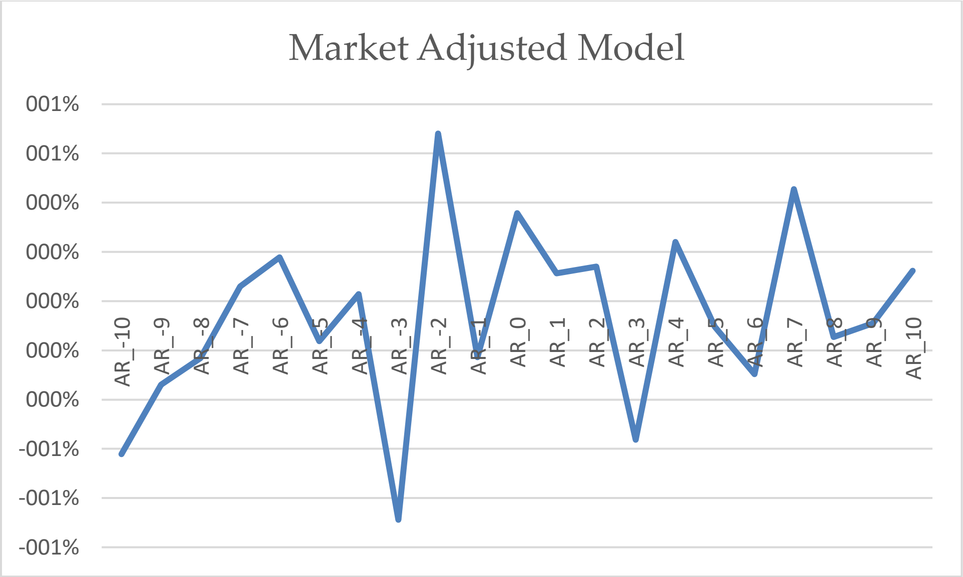


Figure 6: Abnormal returns by market adjusted model for all the firms in the sample

Figure 6 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2 with the largest value in the event window. After day -2, the values have started to decrease and became negative on day -1, i.e. the day before the event announcement day. There is also a sharp decrease in the values on day -3.

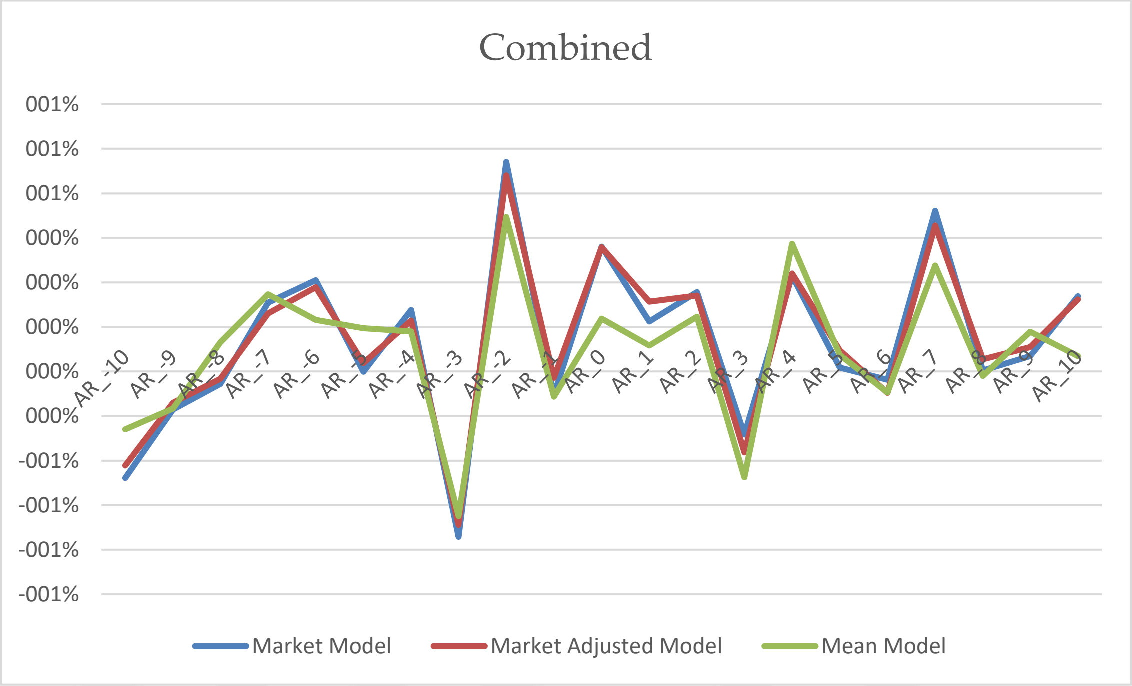


Figure 7: Comparison of the abnormal returns according to the 3 models used in the study for all the firms in the sample

Figure 7 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, a slight difference between the mean adjusted model and the other 2 models on the event day can be observed. According to the mean adjusted model the values are lower than the results of the market model and the market adjusted model on day 0.

Table 12 shows the specific values for the abnormal return on event day for the first research question. There are different and comparable results according to the different models used in the dissertation.

Table 12: Abnormal returns on event day for the overall sample

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	0,36%	0,36%	0,04%
Median Abnormal Return	0,17%	0,19%	-0,08%
Percentage Below Zero	44,35%	42,74%	52,42%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

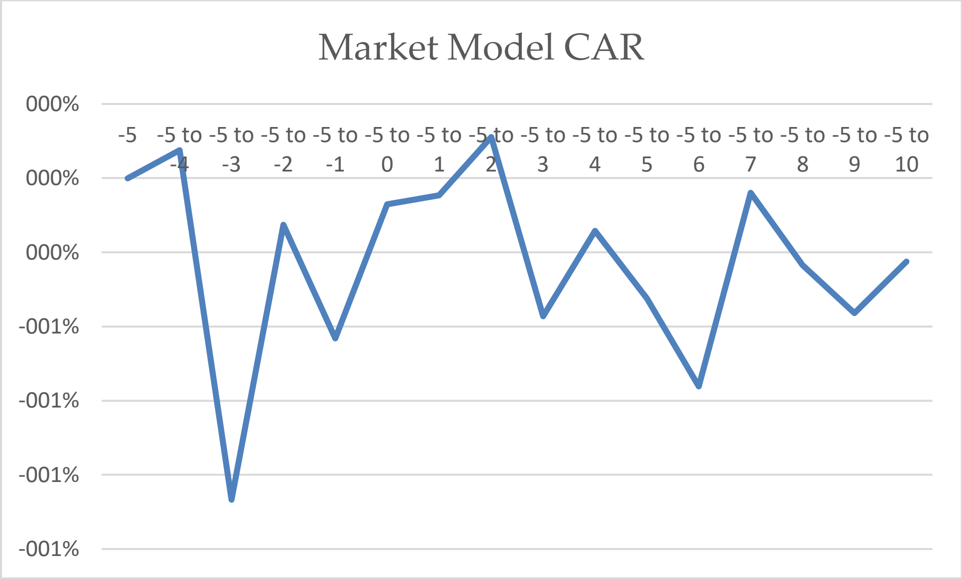


Figure 8: Cumulative abnormal returns by market model for all the firms in the sample

Figure 8 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. Beginning of the sudden drop in returns can be observed more clearly in this figure after day 2. After a slightly increase the values have started to decrease again after day 4.

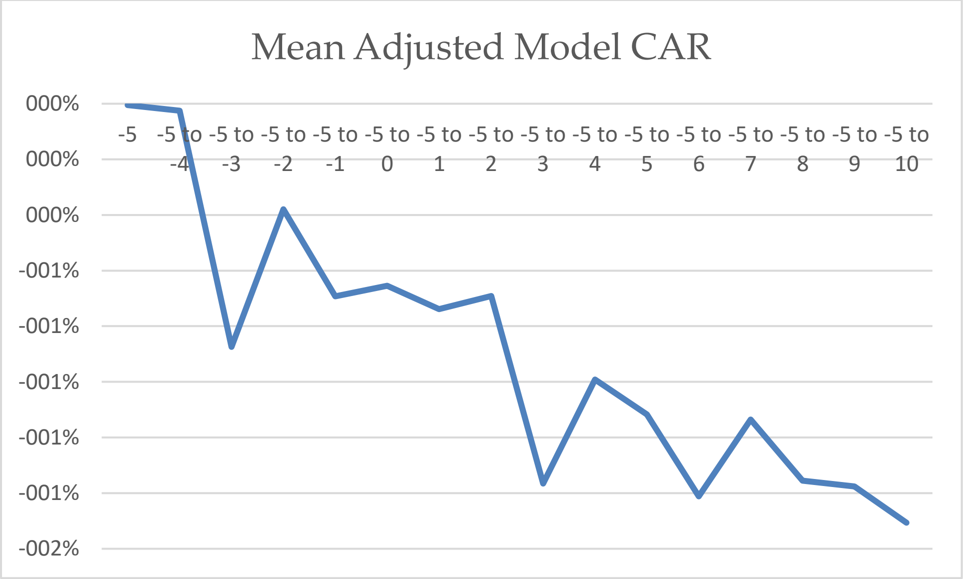


Figure 9: Cumulative abnormal returns by mean adjusted model for all the firms in the sample

Figure 9 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The decrease in the values can be observed starting by day -2. After day 2, there has been one larger decrease.

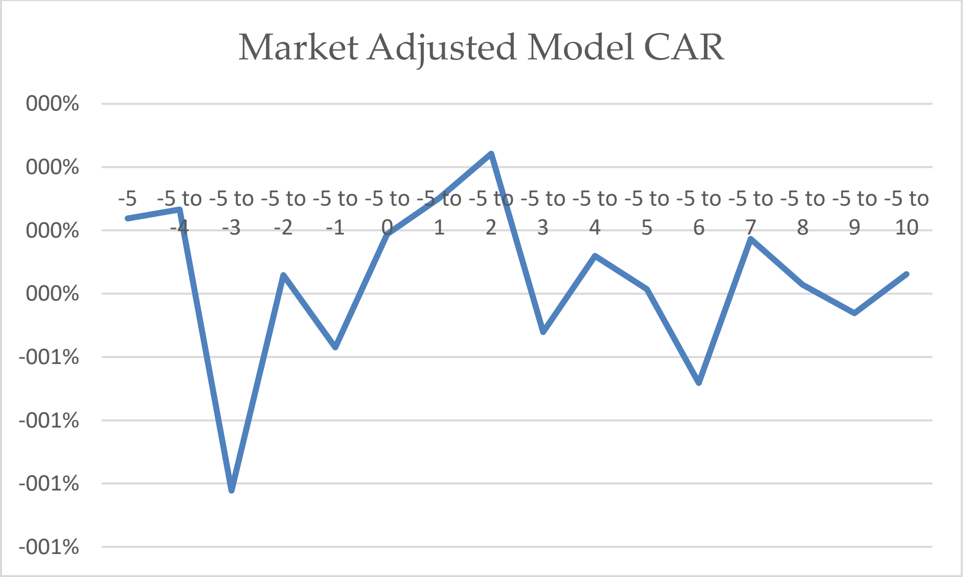


Figure 10: Cumulative abnormal returns by market adjusted model for all the firms in the sample

Figure 10 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. A sudden drop could be observed between the days -4 and -3 and on day -3 values have started to increase again. After a decrease on day -2, the values have started to increase on day -1. The increase state continued until day 2.

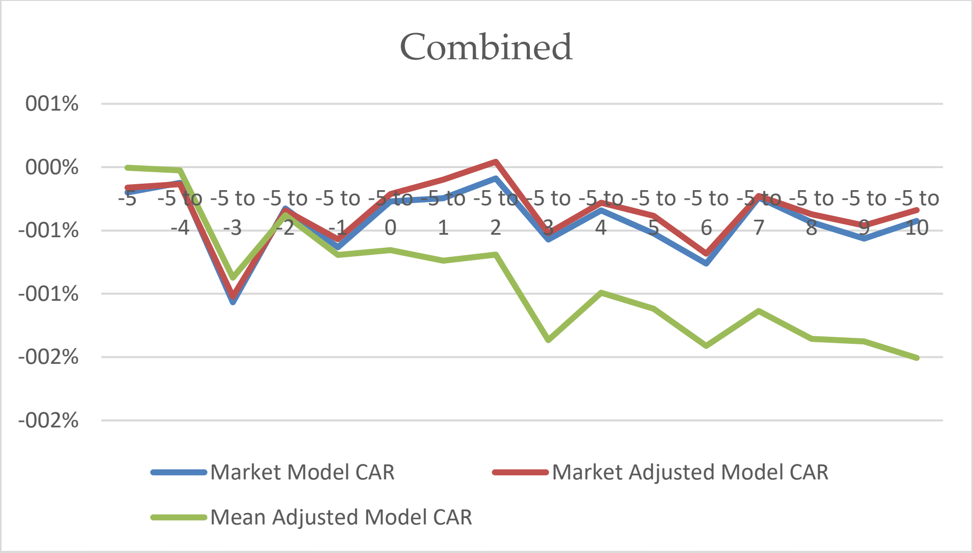


Figure 11: Comparison of the cumulative abnormal returns according to 3 models used in the study for all the firms in the sample

Figure 11 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are matching with each other in general. However, the result of the mean adjusted model is different than the other two models. According to mean adjusted model, the decrease in the values, which began on day -2, is larger than the others.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 13: Cumulative Abnormal Returns for overall sample

Day	Market Model CAR	Market Adjusted Model CAR	Mean Adjusted Model CAR
-5	-0,20%	-0,16%	0,00%
-5 to -4	-0,12%	-0,13%	-0,02%
-5 to -3	-1,07%	-1,02%	-0,87%
-5 to -2	-0,33%	-0,34%	-0,38%
-5 to -1	-0,63%	-0,57%	-0,69%
-5 to 0	-0,27%	-0,21%	-0,65%
-5 to 1	-0,25%	-0,10%	-0,74%
-5 to 2	-0,09%	0,04%	-0,69%
-5 to 3	-0,57%	-0,52%	-1,37%
-5 to 4	-0,34%	-0,28%	-0,99%
-5 to 5	-0,52%	-0,39%	-1,12%
-5 to 6	-0,76%	-0,68%	-1,41%
-5 to 7	-0,24%	-0,23%	-1,14%
-5 to 8	-0,43%	-0,37%	-1,36%
-5 to 9	-0,56%	-0,46%	-1,38%
-5 to 10	-0,43%	-0,34%	-1,51%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 14: t-statistics for overall sample

Day	Market Model CAR t-stat	Market Adjusted Model CAR t-stat	Mean Adjusted Model CAR t-stat
-5	-0,79	-0,63	-0,01
-5 to -4	-0,49	-0,52	-0,05

-5 to -3	-4,18***	-3,98***	-1,83**
-5 to -2	-1,28	-1,33*	-0,8
-5 to -1	-2,47***	-2,22***	-1,45*
-5 to 0	-1,06	-0,82	-1,37*
-5 to 1	-0,96	-0,38	-1,55*
-5 to 2	-0,35	0,16	-1,45*
-5 to 3	-2,24***	-2,03***	-2,87***
-5 to 4	-1,34*	-1,09	-2,08***
-5 to 5	-2,05***	-1,5*	-2,35***
-5 to 6	-2,98***	-2,65***	-2,96***
-5 to 7	-0,94	-0,88	-2,38***
-5 to 8	-1,7**	-1,45*	-2,85***
-5 to 9	-2,21***	-1,8**	-2,89***
-5 to 10	-1,66**	-1,32*	-3,16***

The hypothesis for this research question was:

$H1_0$: IT related failures do not have statistically significant negative impact on the market value of the publicly listed firms.

For the event window [-5,10], the null hypothesis is rejected.

5.1.2. WHAT ARE THE EFFECTS OF INFORMATION TECHNOLOGY RELATED FAILURES ON MANUFACTURING AND SERVICE FIRMS SEPARATELY?

5.1.2.1. Results for Manufacturing Companies

ABNORMAL RETURNS

Results of the abnormal returns according to the market model, mean adjusted model and market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

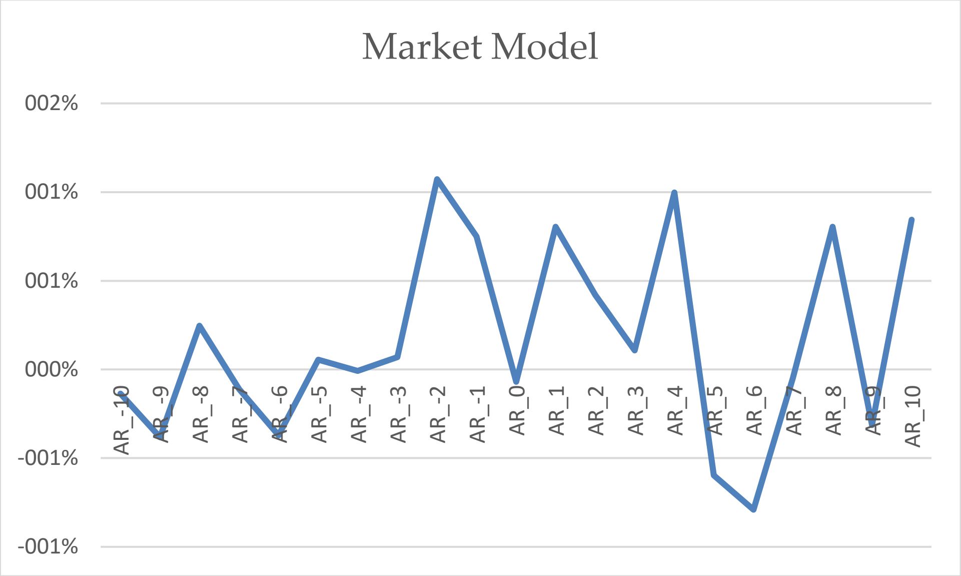


Figure 12: Abnormal returns by market model for manufacturing companies

Figure 12 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The positive values on day -2 are the largest in the considered window. The results show that the values start to decrease right before the event day and start to increase again after the event day. However, there is a sharp decrease in values between days 4 and 6.

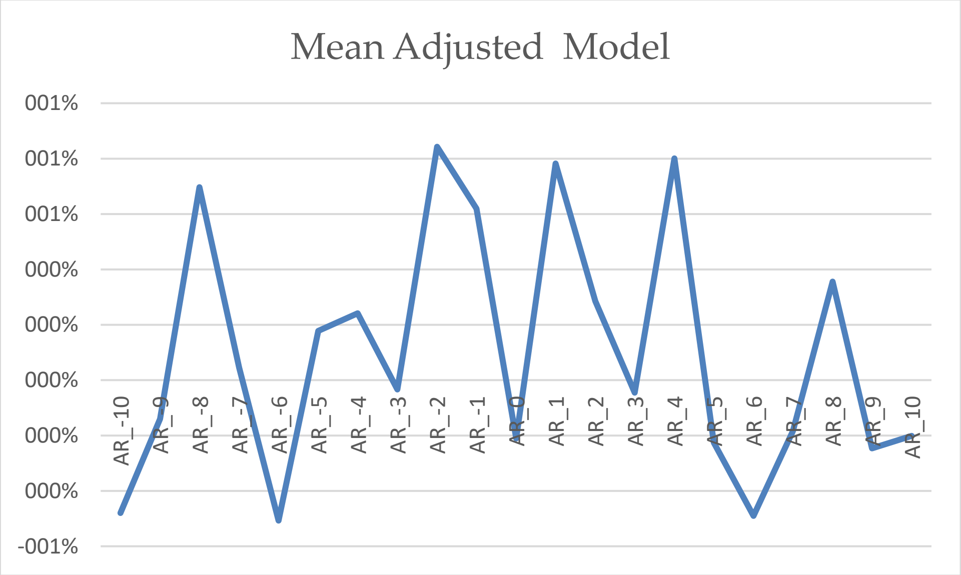


Figure 13: Abnormal returns by mean adjusted model for manufacturing companies

Figure 13 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The positive values on day 2 are the largest in the considered window. After that, the values decreased and the abnormal return became negative in day 0. The increase in the values can be observed after the event day.

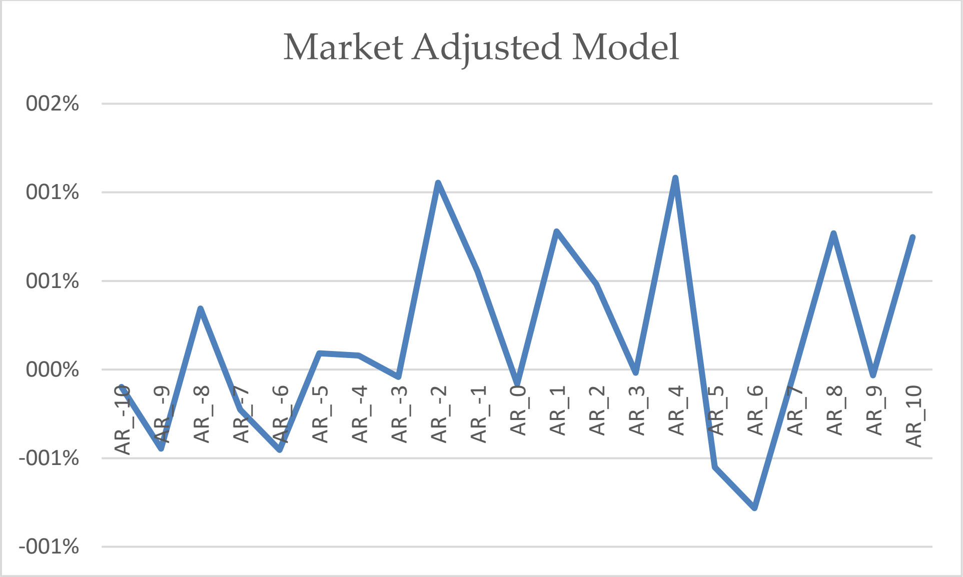


Figure 14: Abnormal returns by market adjusted model for manufacturing companies

Figure 14 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values have started to increase on day -3 and became significantly large on day -2. After day -2 the values started to decrease until the event day. After the event day the values has started to increase again. The largest and the most significant negative value in the event window can be observed on day 6.

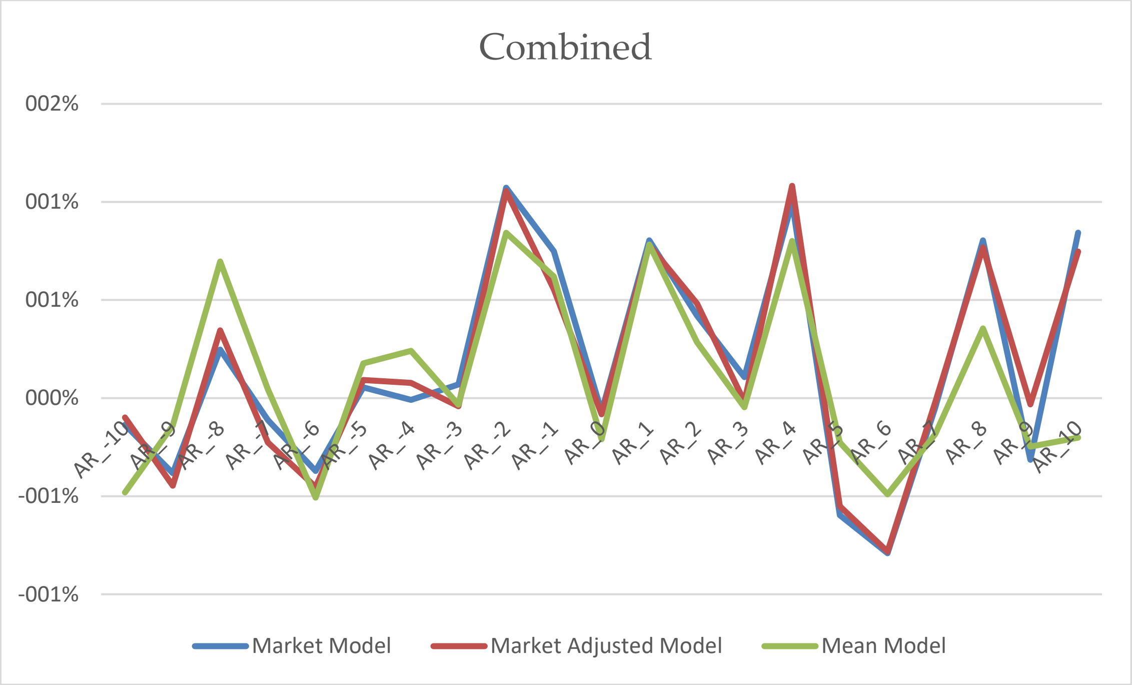


Figure 15: Comparison of the abnormal returns according to the 3 models used in the study for manufacturing companies

Figure 15 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other models around day 6. According to the mean adjusted model the values are higher than the results of the market model and the market adjusted model on day 6.

Table 15 shows the specific values for the abnormal return on event day. The analyses are made specifically for manufacturing companies. There are different and comparable results according to the different models used in the dissertation.

Table 15: Abnormal returns on event day for manufacturing companies

ARt=0	**Market Model**	**Market Adjusted Model**	**Mean Model**
Mean Abnormal Return	-0,07%	-0,08%	-0,21%
Median Abnormal Return	-0,12%	-0,14%	-0,15%
Percentage Below Zero	52,63%	52,63%	52,63%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

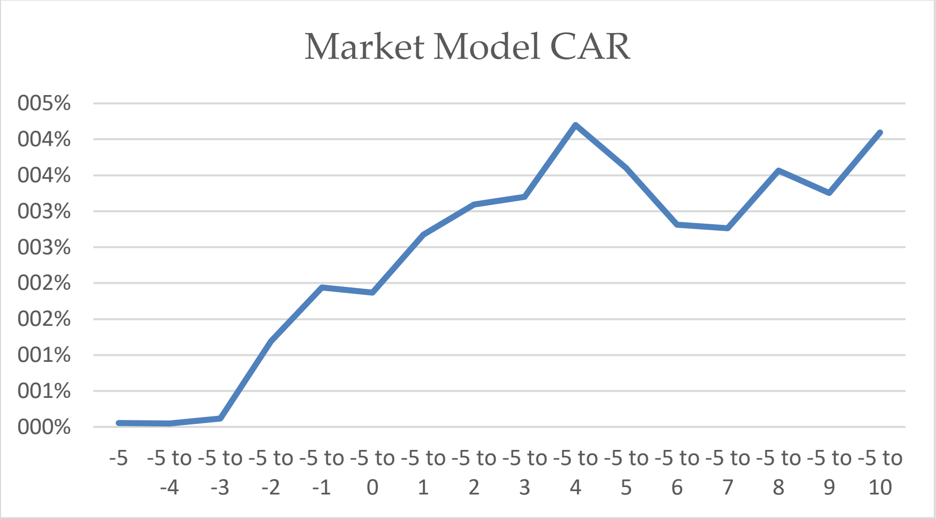


Figure 16: Cumulative abnormal returns by market model for manufacturing companies

Figure 16 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. After the event day the values have started to increase.

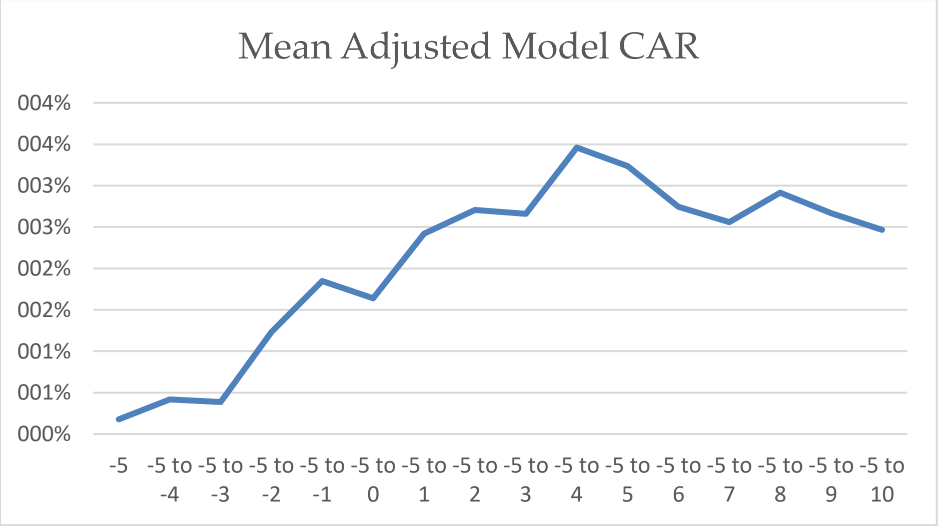


Figure 17: Cumulative abnormal returns by mean adjusted model for manufacturing companies

Figure 17 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to increase on day -2. There has been a small drop in the values on day -1, however the values have started to increase again after the event day.

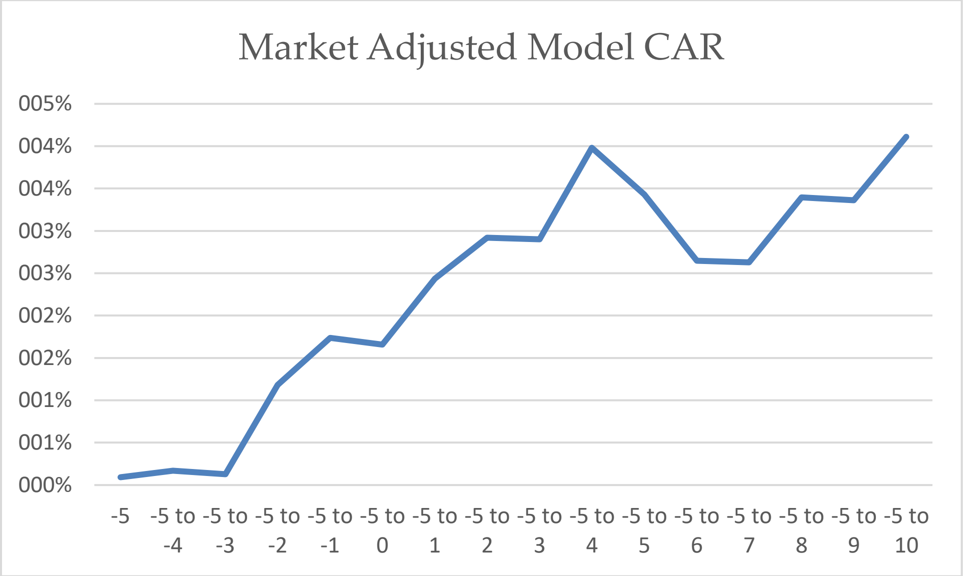


Figure 18: Cumulative abnormal returns by market adjusted model for manufacturing companies

Figure 18 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The values have started to increase on day -3. The increase continued even after the day of event. The only decrease can be observed between the days 4 and 6.

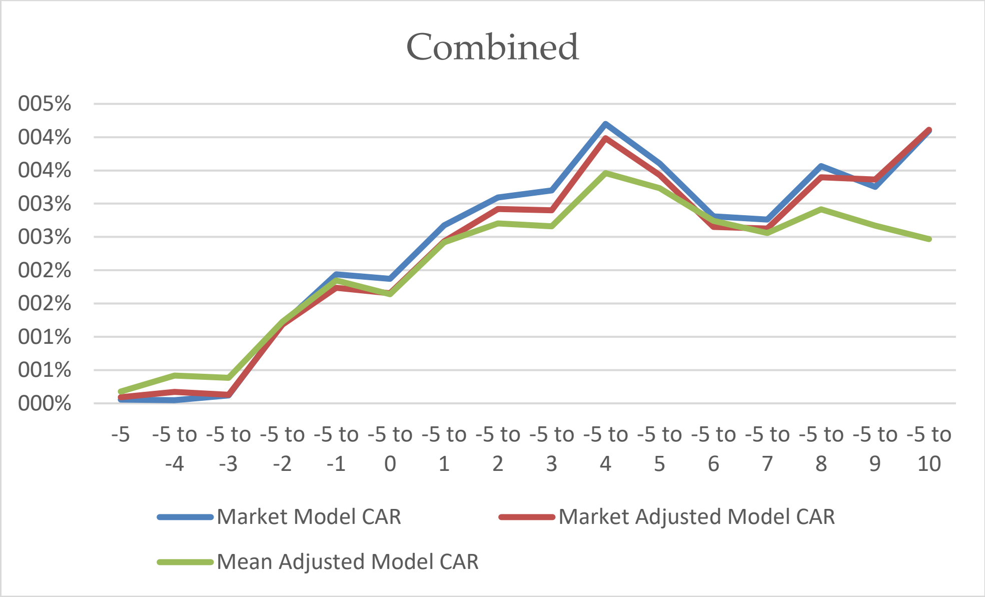


Figure 19: Comparison of the cumulative abnormal returns according to the 3 models used in the study for manufacturing companies

Figure 19 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, the result of the mean adjusted model is slightly different than the other models. According to mean adjusted model the values are slightly less than the market model and the market adjusted model.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 16: Cumulative Abnormal Returns for manufacturing firm sample

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	0,06%	0,09%	0,18%
-5 to -4	0,05%	0,17%	0,42%
-5 to -3	0,12%	0,13%	0,39%
-5 to -2	1,19%	1,18%	1,23%
-5 to -1	1,94%	1,74%	1,85%
-5 to 0	1,87%	1,66%	1,64%
-5 to 1	2,67%	2,44%	2,42%
-5 to 2	3,09%	2,92%	2,70%

-5 to 3	3,20%	2,90%	2,66%
-5 to 4	4,20%	3,98%	3,46%
-5 to 5	3,60%	3,43%	3,23%
-5 to 6	2,81%	2,65%	2,74%
-5 to 7	2,76%	2,63%	2,56%
-5 to 8	3,57%	3,40%	2,92%
-5 to 9	3,25%	3,36%	2,67%
-5 to 10	4,10%	4,11%	2,47%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 17: t-statistics for manufacturing firm sample

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	0,04	0,07	0,17
-5 to -4	0,03	0,13	0,4
-5 to -3	0,08	0,1	0,37
-5 to -2	0,85	0,89	1,18
-5 to -1	1,39*	1,3*	1,78**
-5 to 0	1,34*	1,24	1,58*
-5 to 1	1,91**	1,82**	2,33***
-5 to 2	2,21***	2,18***	2,61***
-5 to 3	2,29***	2,17***	2,56***
-5 to 4	3***	2,98***	3,33***
-5 to 5	2,58***	2,57***	3,12***
-5 to 6	2,01***	1,98***	2,64***
-5 to 7	1,98***	1,97***	2,47***
-5 to 8	2,55***	2,54***	2,81***

-5 to 9	2,33***	2,52***	2,57***
-5 to 10	2,93***	3,07***	2,38***

The hypothesis for the effect of information security breaches on manufacturing firms sample was:

$H2_0$: IT related failures do not have statistically significant impact on the market value of the manufacturing firms.

For the event window [-5,10], the null hypothesis is rejected.

5.1.2.2. Results for Service Companies

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

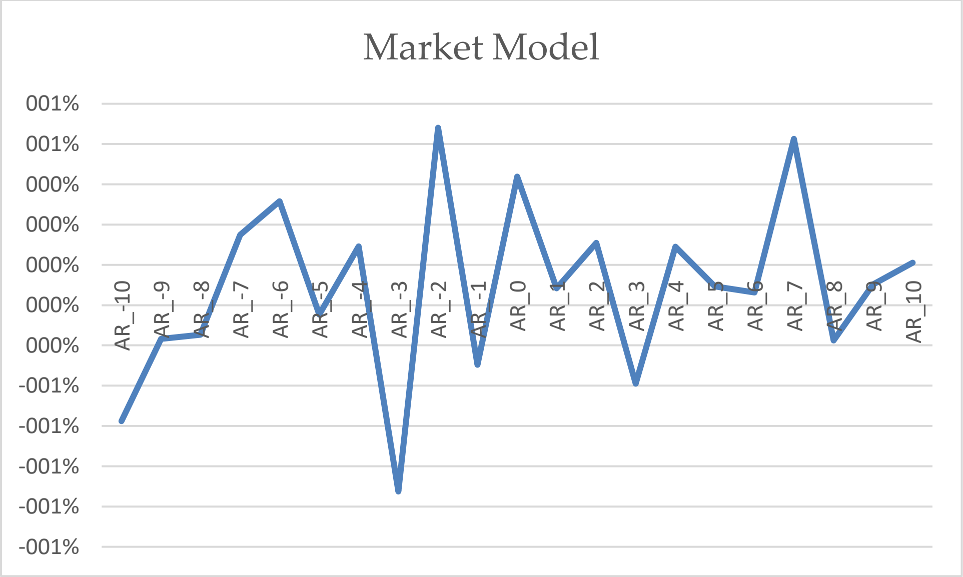


Figure 20: Abnormal returns by market model for service firms

Figure 20 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). There is a sharp decrease on the values on day -3, which is the largest negative value, and then the values start to increase again. There is another decrease on day -1, which is the day before the event. The next decrease in the window is identified as day 3, after that the values have become positive until day 8.

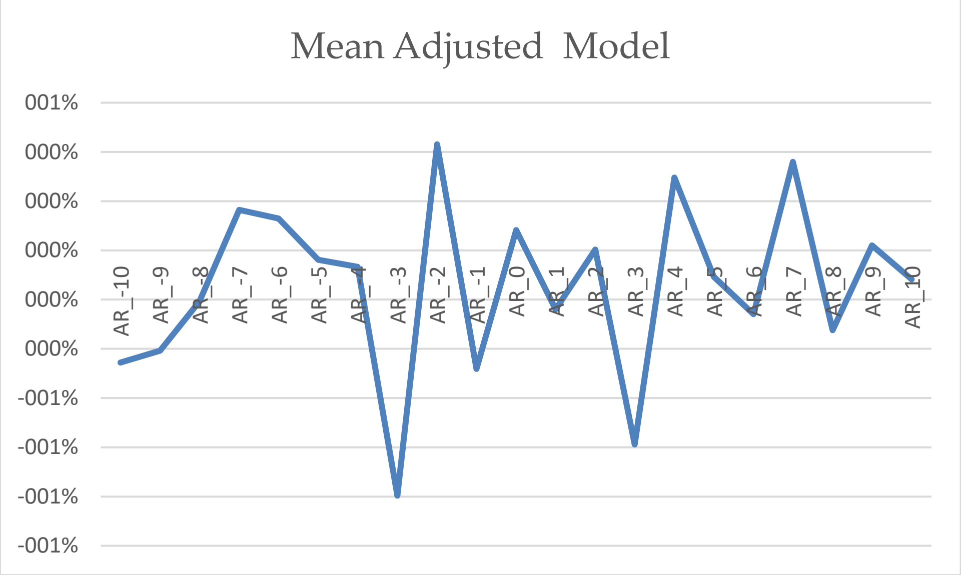


Figure 21: Abnormal returns by mean adjusted model for service firms

Figure 21 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. After the event day (the announcement of the event on day 0) the values showed a slow decrease and then a sharp decrease in day 2.

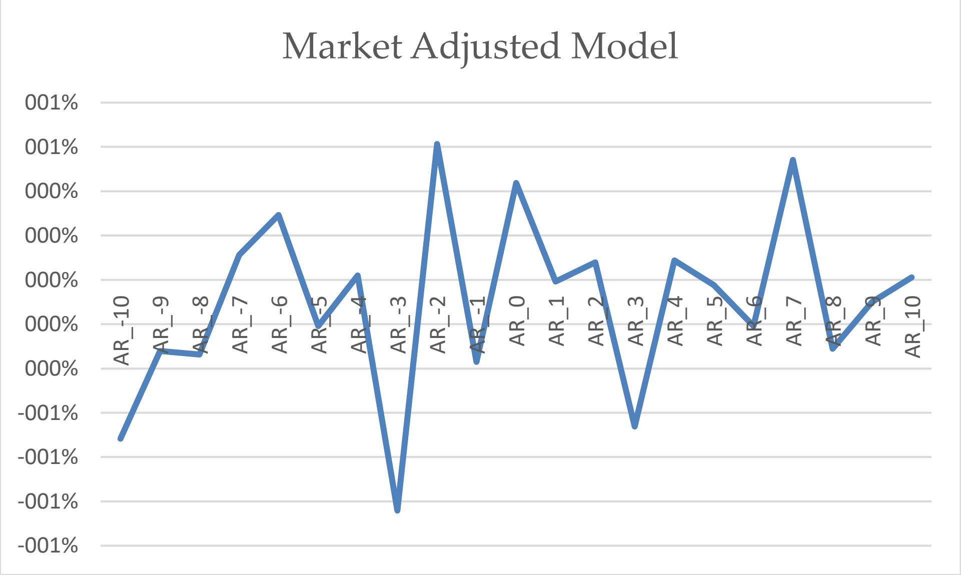


Figure 22: Abnormal returns by market adjusted model for service firms

Figure 22 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2 with the largest and most significant value in the event window. After day -2, the values have started to decrease and became negative on day -1, i.e. the day before the event announcement day. The values have started to increase before day 0 and decrease again after that day.

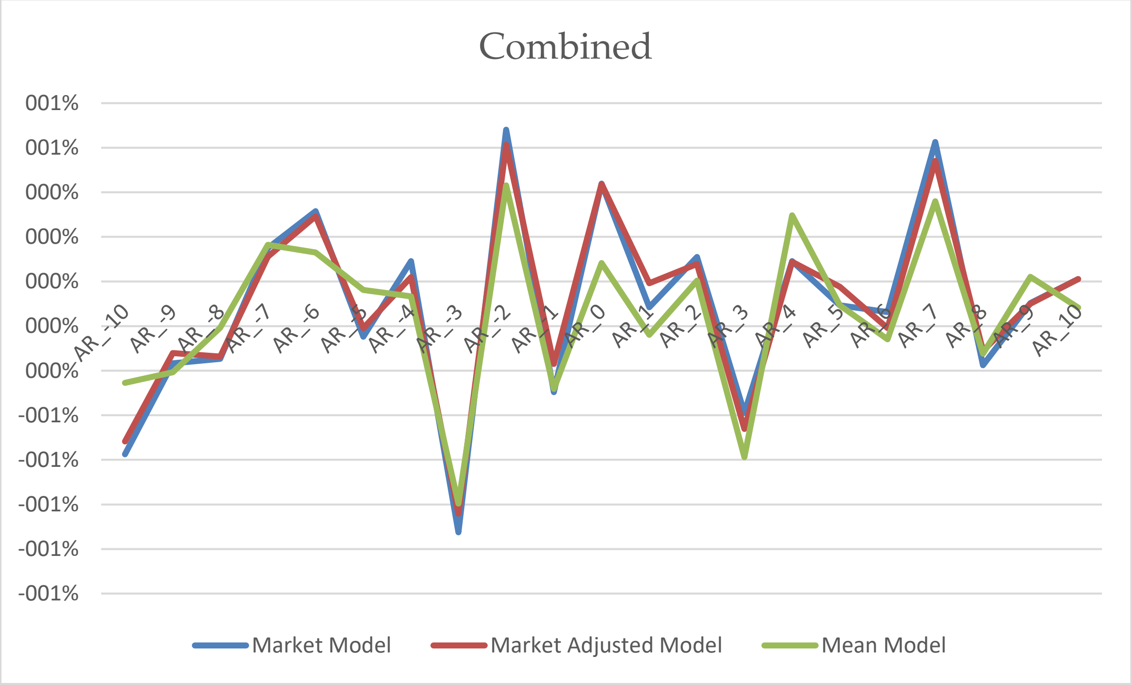


Figure 23: Comparison of the abnormal returns according to the 3 models used in the study for service firms

Figure 23 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other models on day 0. According to the mean adjusted model the values are lower than the results of the market model and the market adjusted model on the event day.

Table 18 shows the specific values for the abnormal return on event day. The analyses are made specifically for service firms. There are different and comparable results according to the different models used in the dissertation.

Table 18: Abnormal returns on event day for service firms

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	0,44%	0,44%	0,08%
Median Abnormal Return	0,20%	0,21%	-0,08%
Percentage Below Zero	42,86%	40,95%	52,38%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

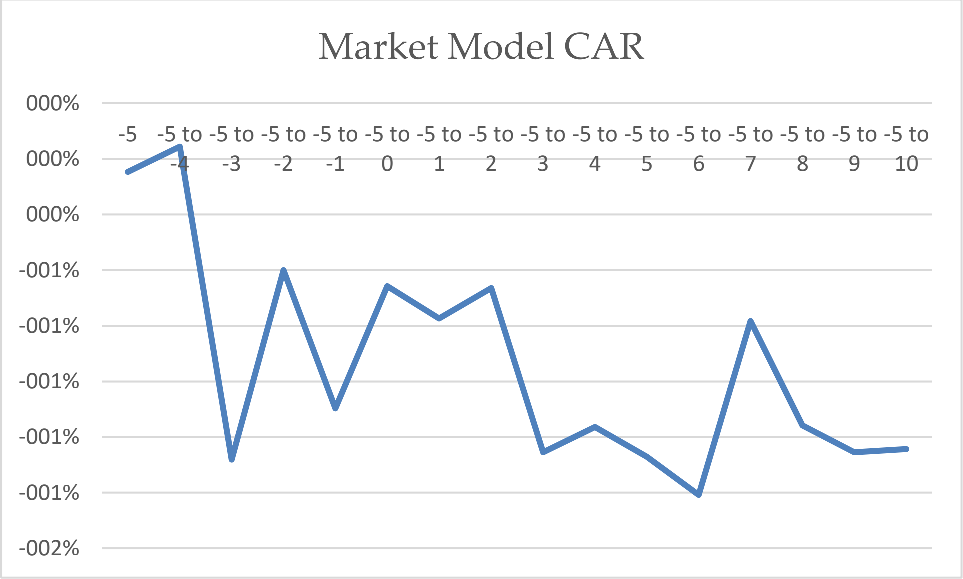


Figure 24: Cumulative abnormal returns by market model for service firms

Figure 24 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. There could be seen a slight decrease in the returns after the event day. However, beginning of the sudden drop in returns can be observed more clearly after day 2. A sharp increase in values can be observed after day 6.

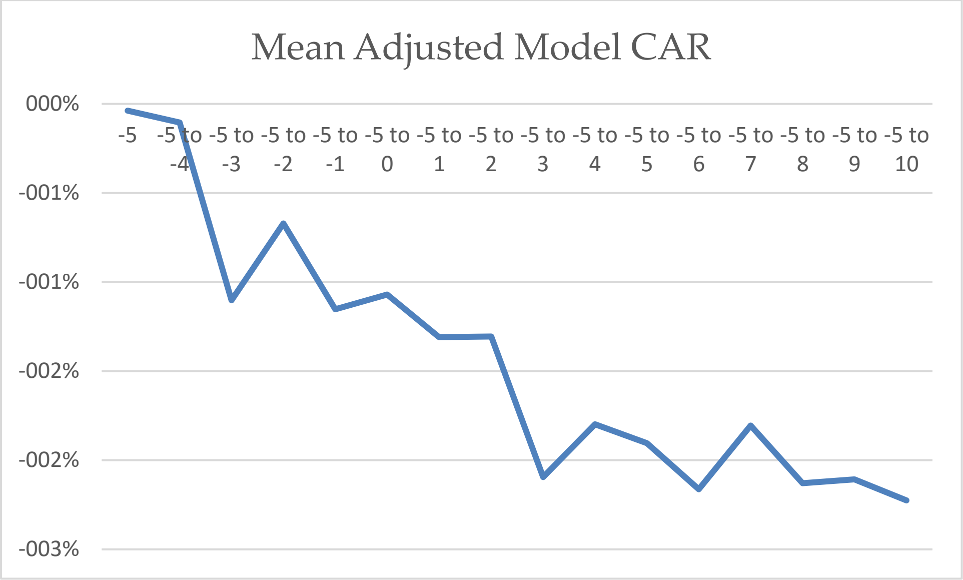


Figure 25: Cumulative abnormal returns by mean adjusted model for service firms

Figure 25 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to decrease on day -2. After the event day, decrease in the values continued until day 3.

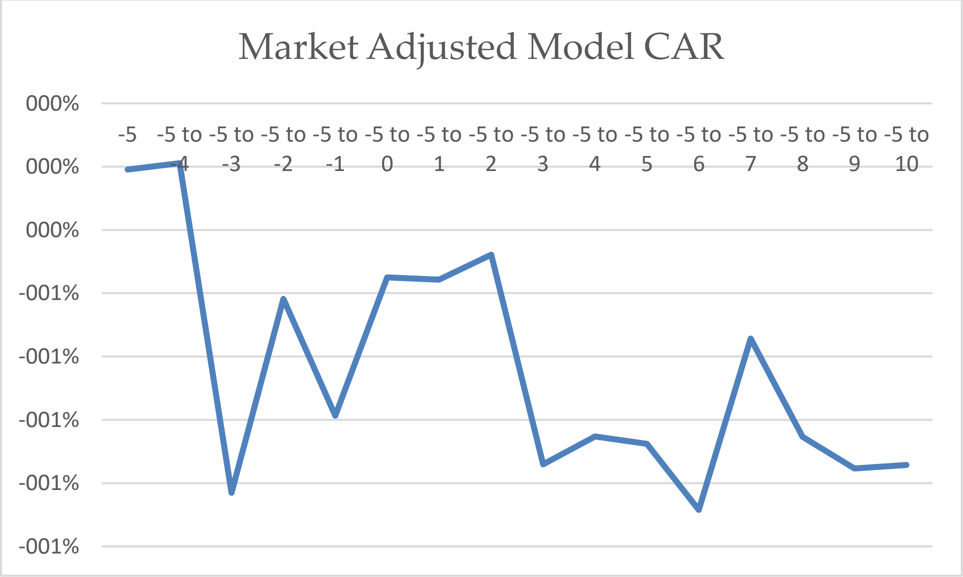


Figure 26: Cumulative abnormal returns by market adjusted model for service firms

Figure 26 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The values have started to decrease on day -2. After an increase in the values on day -1, the values have started to decrease again on day 2.

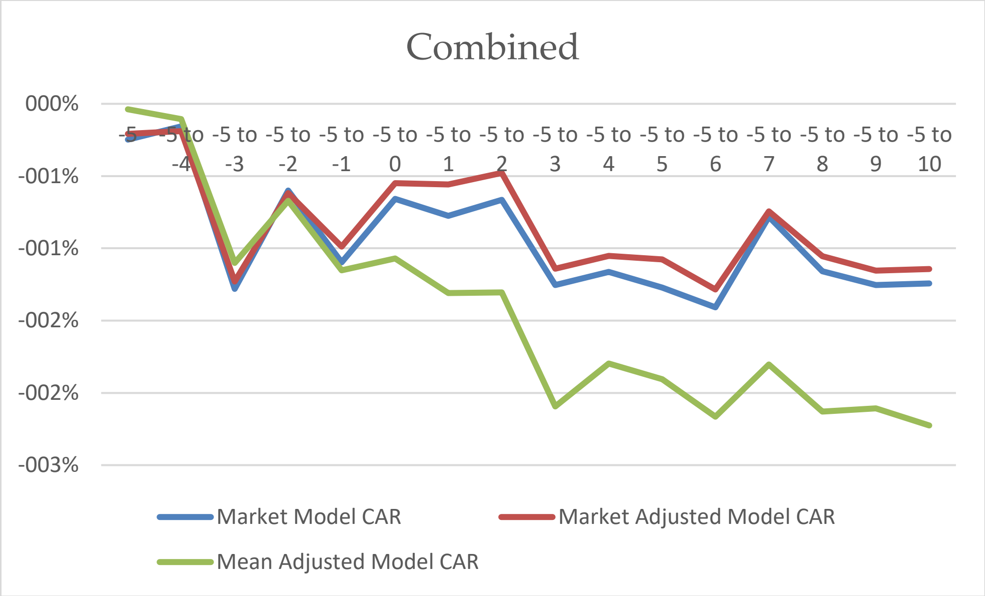


Figure 27: Comparison of the cumulative abnormal returns according to the 3 models used in the study for service firms

Figure 27 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are matching with each other in general. However, the result of the mean adjusted model is different than the other two models. The big difference of the results of mean adjusted model began on day -1.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 19: Cumulative Abnormal Returns for service firms sample

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,25%	-0,21%	-0,04%
-5 to -4	-0,16%	-0,19%	-0,11%
-5 to -3	-1,28%	-1,23%	-1,10%
-5 to -2	-0,60%	-0,62%	-0,67%
-5 to -1	-1,10%	-0,99%	-1,15%

-5 to 0	-0,66%	-0,55%	-1,07%
-5 to 1	-0,77%	-0,56%	-1,31%
-5 to 2	-0,67%	-0,48%	-1,31%
-5 to 3	-1,25%	-1,14%	-2,09%
-5 to 4	-1,16%	-1,05%	-1,80%
-5 to 5	-1,27%	-1,08%	-1,90%
-5 to 6	-1,41%	-1,28%	-2,16%
-5 to 7	-0,78%	-0,74%	-1,80%
-5 to 8	-1,16%	-1,05%	-2,13%
-5 to 9	-1,25%	-1,15%	-2,11%
-5 to 10	-1,24%	-1,14%	-2,23%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 20: t-statistics for service firms sample

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	-0,63	-0,58	-0,05
-5 to -4	-0,4	-0,52	-0,15
-5 to -3	-3,29***	-3,39***	-1,54*
-5 to -2	-1,54*	-1,7**	-0,94
-5 to -1	-2,82***	-2,72***	-1,61*
-5 to 0	-1,69**	-1,51*	-1,5*
-5 to 1	-1,99***	-1,53*	-1,83**
-5 to 2	-1,71**	-1,32*	-1,83**
-5 to 3	-3,22***	-3,14***	-2,93***
-5 to 4	-2,99***	-2,9***	-2,51***

-5 to 5	-3,26***	-2,97***	-2,66***
-5 to 6	-3,62***	-3,54***	-3,03***
-5 to 7	-2,01***	-2,05***	-2,52***
-5 to 8	-2,97***	-2,9***	-2,98***
-5 to 9	-3,22***	-3,18***	-2,95***
-5 to 10	-3,19***	-3,15***	-3,11***

The hypothesis for the effect of information security breaches on service firms sample was:

$H3_0$: IT related failures do not have statistically significant impact on the market value of the service firms.

For the event window [-5,10], the null hypothesis is rejected.

5.1.3. WHICH SECTOR IS AFFECTED THE MOST FROM THE INFORMATION TECHNOLOGY RELATED FAILURES?

5.1.3.1. Consumer Goods

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

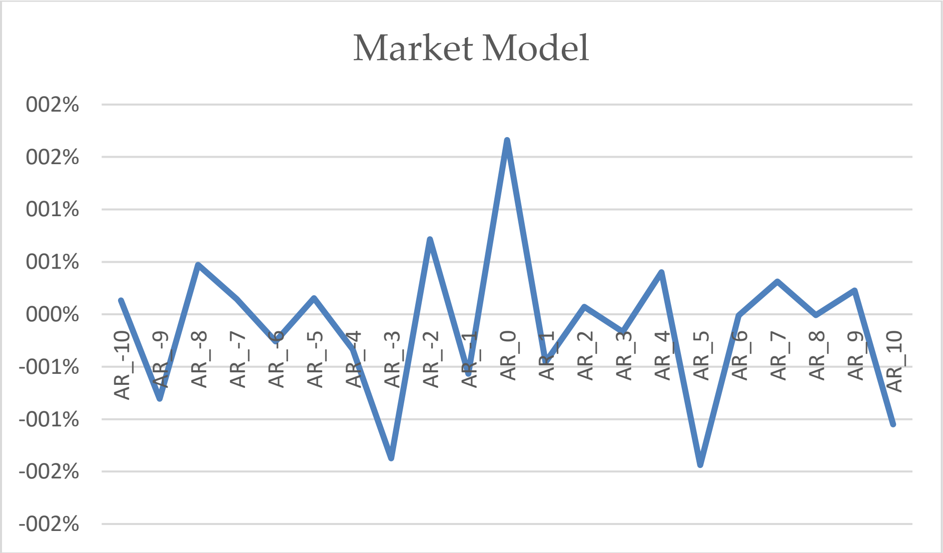


Figure 28: Abnormal returns by market model for consumer goods sector

Figure 28 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 and day 5 are the largest in the considered window. The results show that the values start to increase right before the event day sharply and the sharp decrease has been experienced right after day 0.

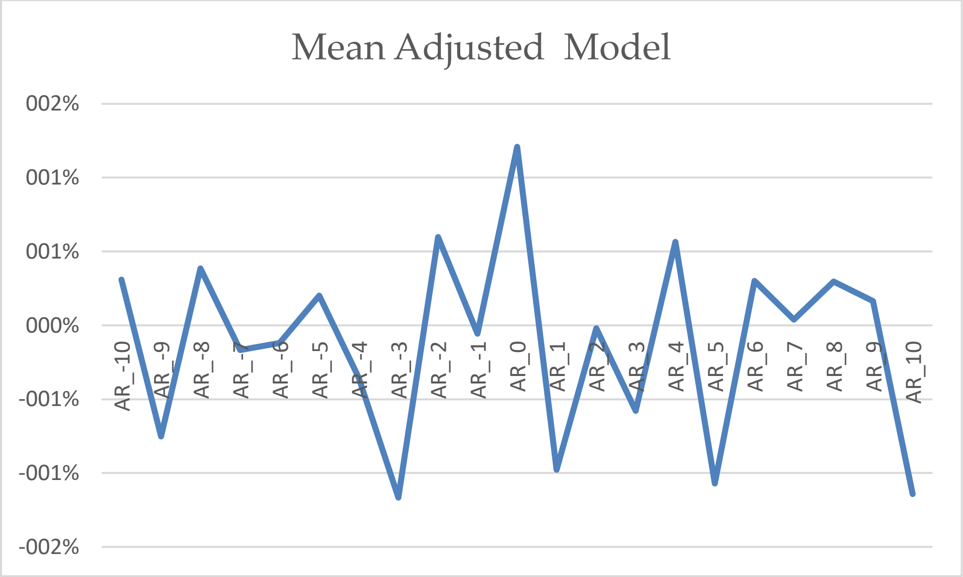


Figure 29: Abnormal returns by mean adjusted model for consumer goods sector

Figure 29 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. After the event day (the announcement of the event on day 0) the values decreased sharply and become positive on day 4.

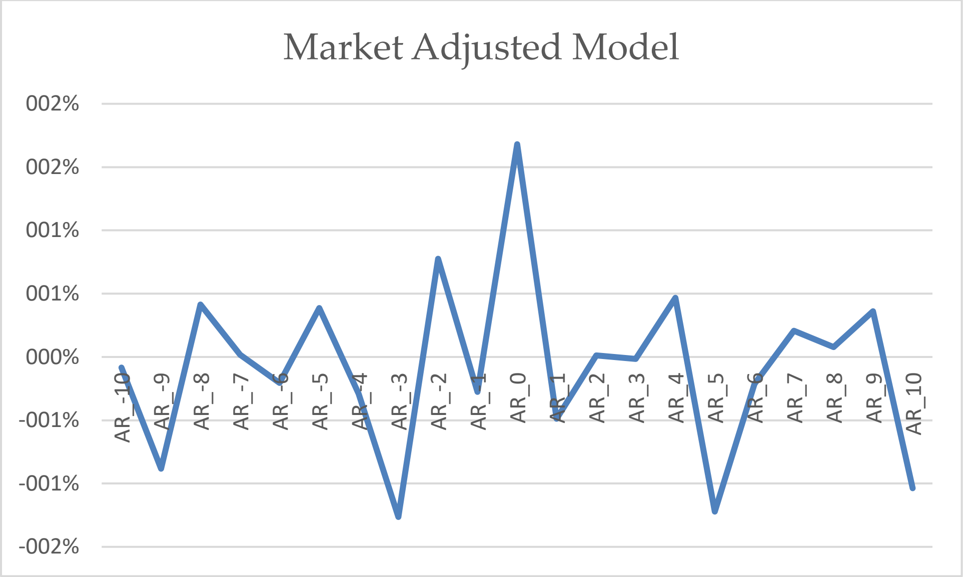


Figure 30: Abnormal returns by market adjusted model for consumer goods sector

Figure 30 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. After day -2, the values have started to decrease and became negative on day -1 and started to increase again after day -1. The positive values are the largest on the event day. A sharp decrease in the values can be observed after the event day.

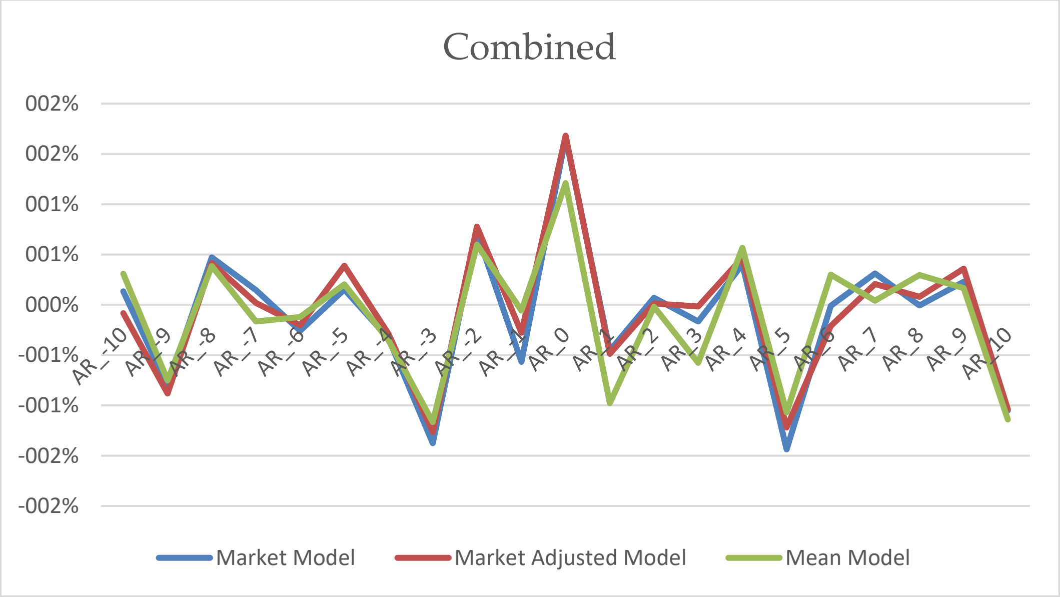


Figure 31: Comparison of the abnormal returns according to the 3 models used in the study for consumer goods sector

Figure 31 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other models on day 0. According to the mean adjusted model the values are slightly lower than the results of the market model and the market adjusted model on the event day. The similar situation is also valid on day 1. The values on day 1 are lower according to the mean adjusted model.

Table 21 shows the specific values for the abnormal return on event day. The analyses are made specifically for the consumer goods sector. There are different and comparable results according to the different models used in the dissertation.

Table 21: Abnormal returns on event day for the consumer goods sector

ARt=0	**Market Model**	**Market Adjusted Model**	**Mean Model**
Mean Abnormal Return	1,66%	1,68%	1,21%
Median Abnormal Return	0,27%	0,30%	0,07%
Percentage Below Zero	36,84%	36,84%	47,37%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

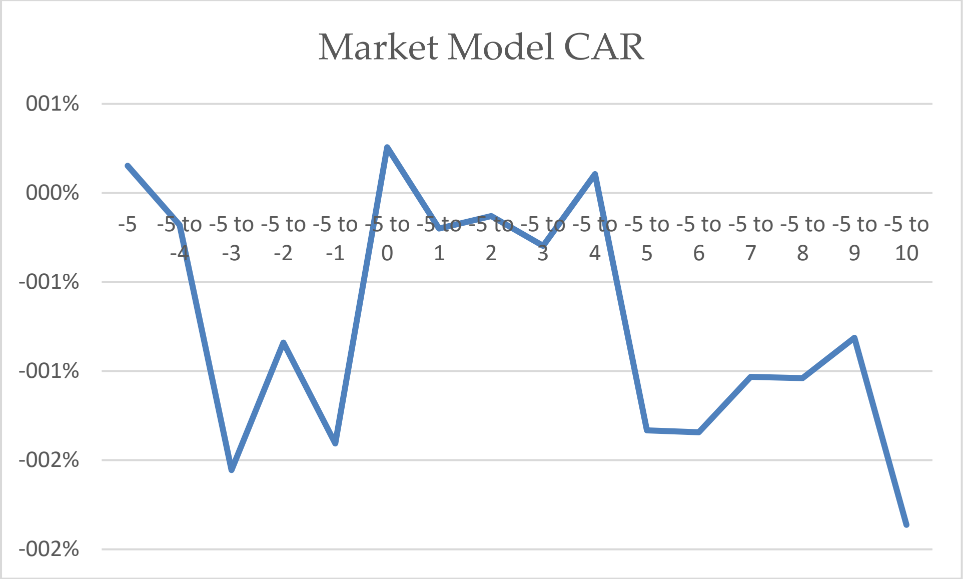


Figure 32: Cumulative abnormal returns by market model for consumer goods sector

Figure 32 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. The results show that there was an increase in the values between the days -1 and 0, however the values started to decrease after the event day. A larger decrease can be observed on day 4.

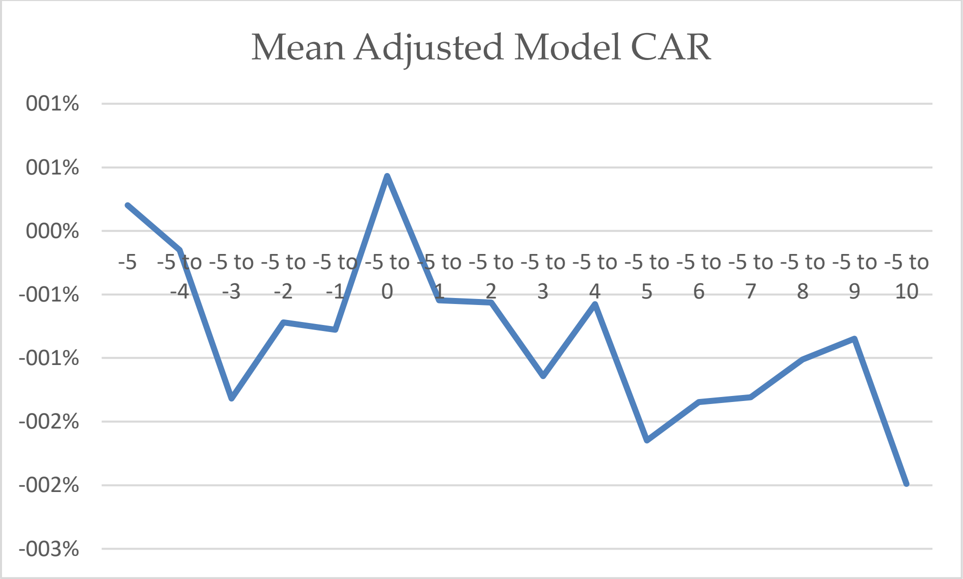


Figure 33: Cumulative abnormal returns by mean adjusted model for consumer goods sector

Figure 33 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The positive values have started to decrease on the event day became negative on 1. After a small increase between the day 3 and day 4, the values decreased again.

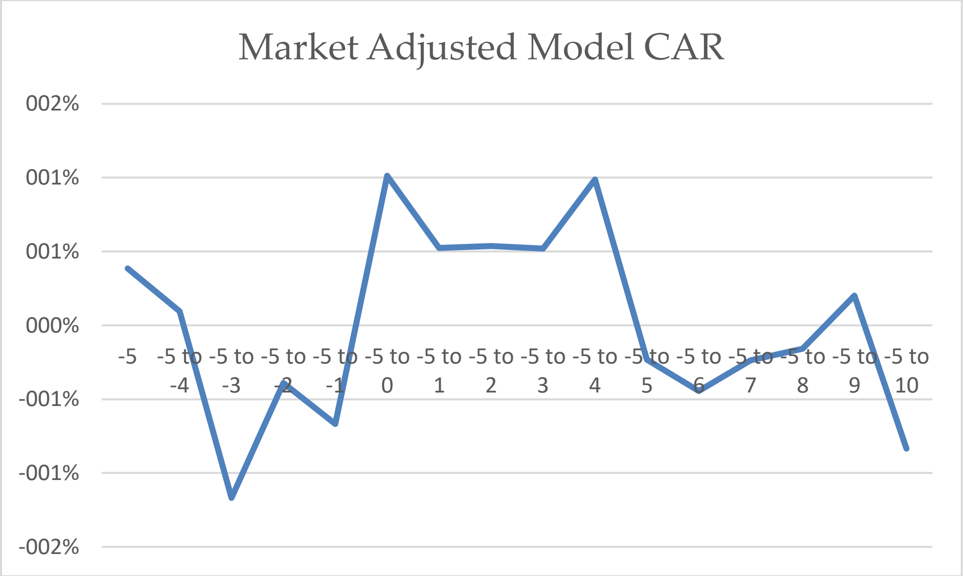


Figure 34: Cumulative abnormal returns by market adjusted model for consumer goods sector

Figure 34 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The values have started to increase on day -1. There has been a small drop in the values on day -1, however the values remained positive. After the decrease on day 4, the values became negative.

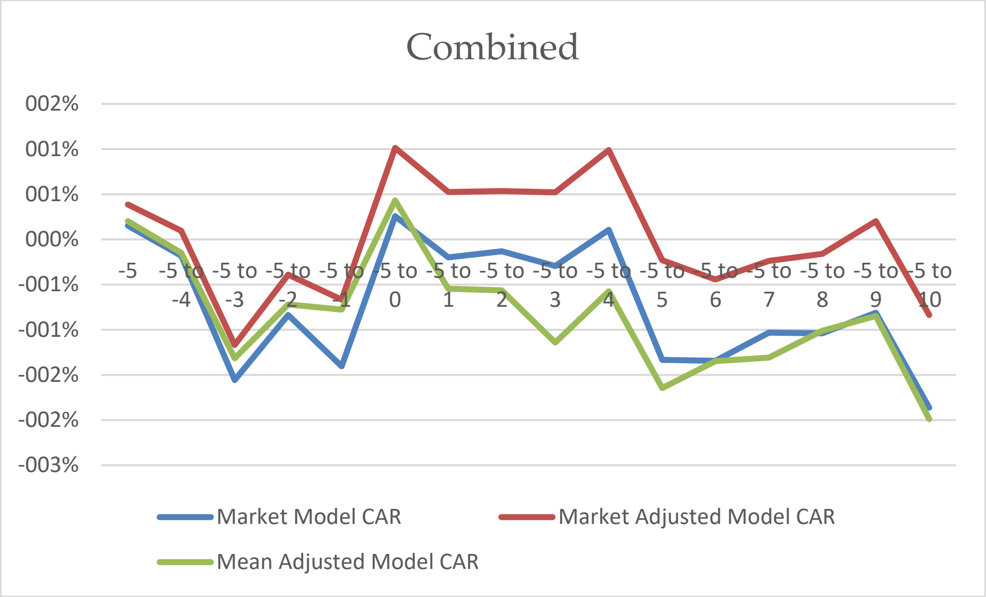


Figure 35: Comparison of the cumulative abnormal returns according to the 3 models used in the study for consumer goods sector

Figure 35 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are slightly different from each other. The market adjusted model shows the highest values on the selected event window. The returns according to the mean adjusted model were higher until the event day. After the event day, the results of the market model are higher than the mean adjustment model.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 22: Cumulative Abnormal Returns for consumer goods sector sample

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	0,15%	0,39%	0,20%
-5 to -4	-0,18%	0,10%	-0,15%
-5 to -3	-1,56%	-1,17%	-1,32%
-5 to -2	-0,84%	-0,39%	-0,72%
-5 to -1	-1,41%	-0,67%	-0,78%
-5 to 0	0,26%	1,01%	0,43%

-5 to 1	-0,20%	0,52%	-0,55%
-5 to 2	-0,13%	0,54%	-0,56%
-5 to 3	-0,30%	0,52%	-1,14%
-5 to 4	0,11%	0,99%	-0,58%
-5 to 5	-1,33%	-0,23%	-1,65%
-5 to 6	-1,34%	-0,44%	-1,35%
-5 to 7	-1,03%	-0,24%	-1,31%
-5 to 8	-1,04%	-0,16%	-1,01%
-5 to 9	-0,81%	0,20%	-0,85%
-5 to 10	-1,86%	-0,84%	-1,99%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 23: t-statistics for consumer goods sector sample

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	0,23	0,61	0,31
-5 to -4	-0,27	0,15	-0,23
-5 to -3	-2,29***	-1,84**	-2,04***
-5 to -2	-1,23	-0,62	-1,12
-5 to -1	-2,06***	-1,05	-1,21
-5 to 0	0,38	1,6*	0,67
-5 to 1	-0,29	0,83	-0,85
-5 to 2	-0,19	0,85	-0,88
-5 to 3	-0,43	0,82	-1,77**
-5 to 4	0,15	1,56*	-0,89
-5 to 5	-1,96**	-0,37	-2,56***

-5 to 6	-1,97***	-0,7	-2,09***
-5 to 7	-1,52*	-0,37	-2,03***
-5 to 8	-1,53*	-0,25	-1,57*
-5 to 9	-1,19	0,32	-1,32*
-5 to 10	-2,74***	-1,32*	-3,09***

The hypothesis for the effect of information security breaches on consumer goods sector was:

H4$_0$: IT related failures do not have statistically significant impact on the market value of the consumer goods sector.

For the event window [-5,10], the null hypothesis is rejected.

5.1.3.2. Financials

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

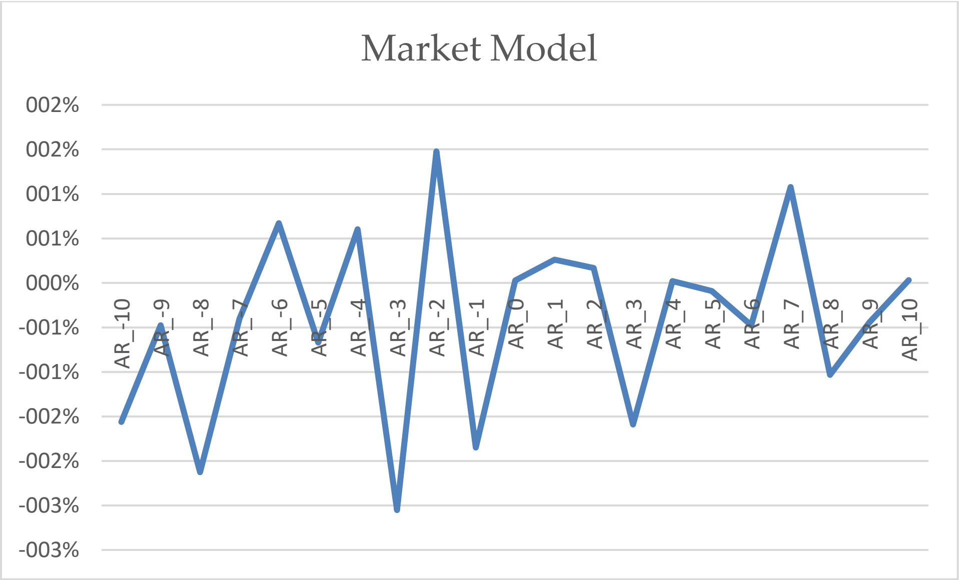


Figure 36: Abnormal returns by market model for financials sector

Figure 36 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After day -3, the values have become positive and there is another sharp decrease on day -1. After the event day the values has become positive for 2 days and the values has become negative again on day 3.

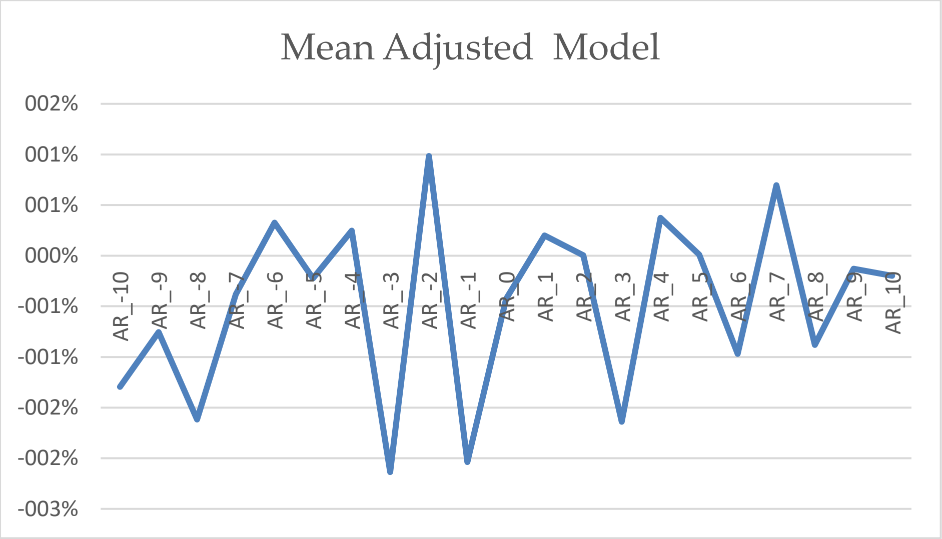


Figure 37: Abnormal returns by mean adjusted model for financials sector

Figure 37 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. The positive values on day -2 are the largest and the most significant in the event window. Before the event day the values decreased again in a significant way. The values became positive on day 1.

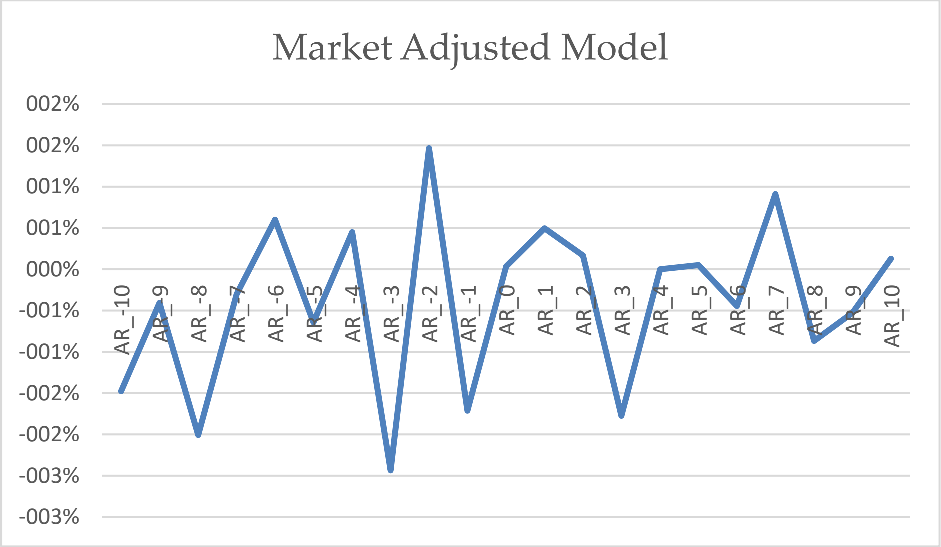


Figure 38: Abnormal returns by market adjusted model for financials sector

Figure 38 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2 with the largest value in the event window. After day -2, the values have started to decrease and became negative on day -1, i.e. the day before the event announcement day. After day -1 the values started to increase, became positive after the event day and started to decrease again after day 1.

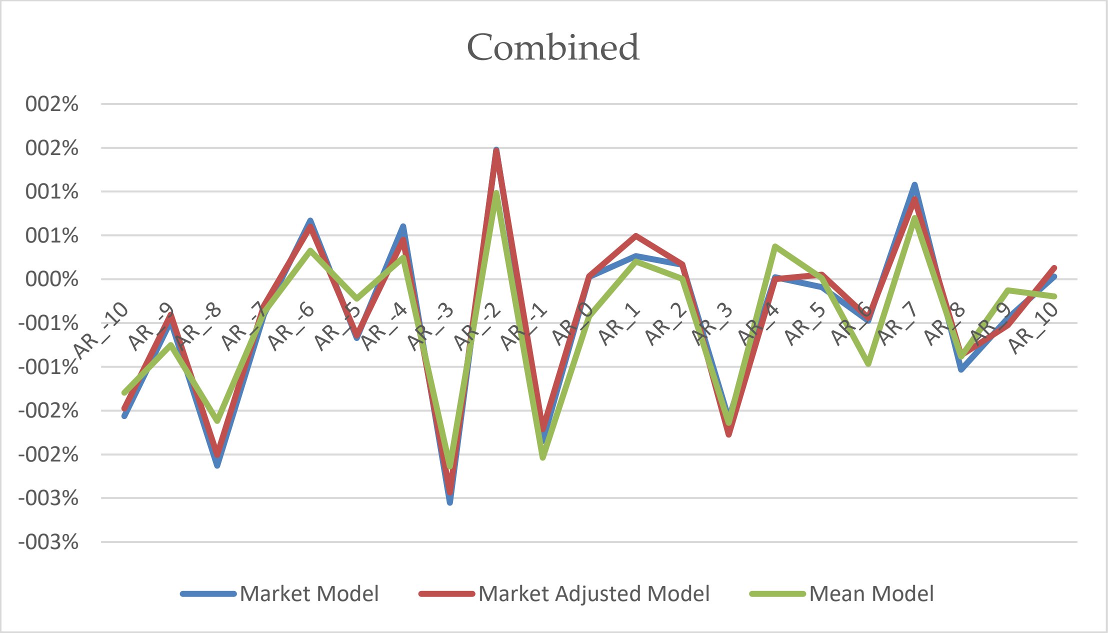


Figure 39: Comparison of the abnormal returns according to the 3 models used in the study for financials sector

Figure 39 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other 2 models on the event day. According to the mean adjusted model the values are lower than the results of the market model and the market adjusted model.

Table 24 shows the specific values for the abnormal return on event day. The analyses are made specifically for the financials sector. There are different and comparable results according to the different models used in the dissertation.

Table 24: Abnormal returns on event day for the financials sector

ARt=0	**Market Model**	**Market Adjusted Model**	**Mean Model**
Mean Abnormal Return	0,03%	0,03%	-0,42%
Median Abnormal Return	0,08%	0,13%	-0,69%
Percentage Below Zero	43,75%	43,75%	62,50%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

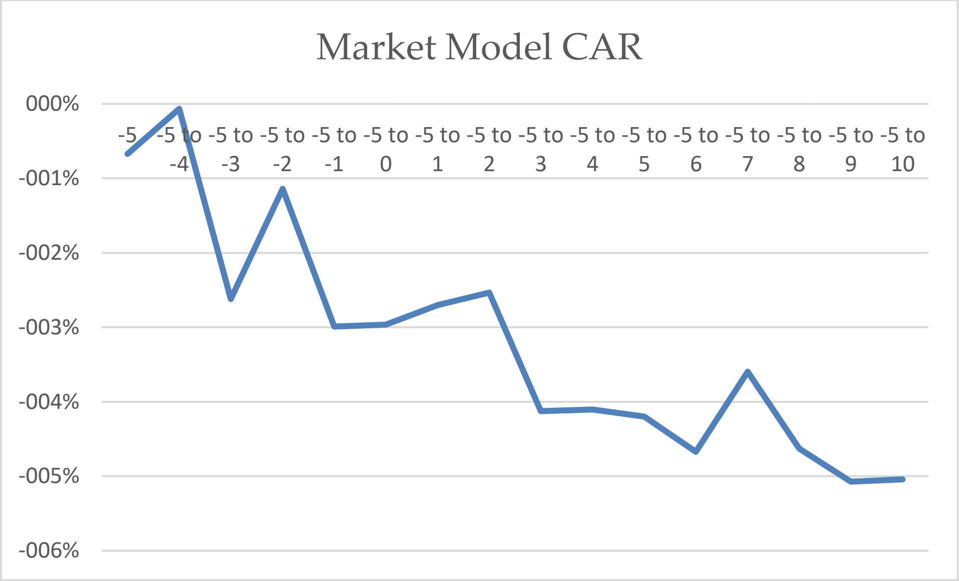


Figure 40: Cumulative abnormal returns by market model for financials sector

Figure 40 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. Beginning of the sudden drop in returns can be observed more clearly after day 2. Following a slightly increase the values on day 6, the values started to decrease again after day 7.

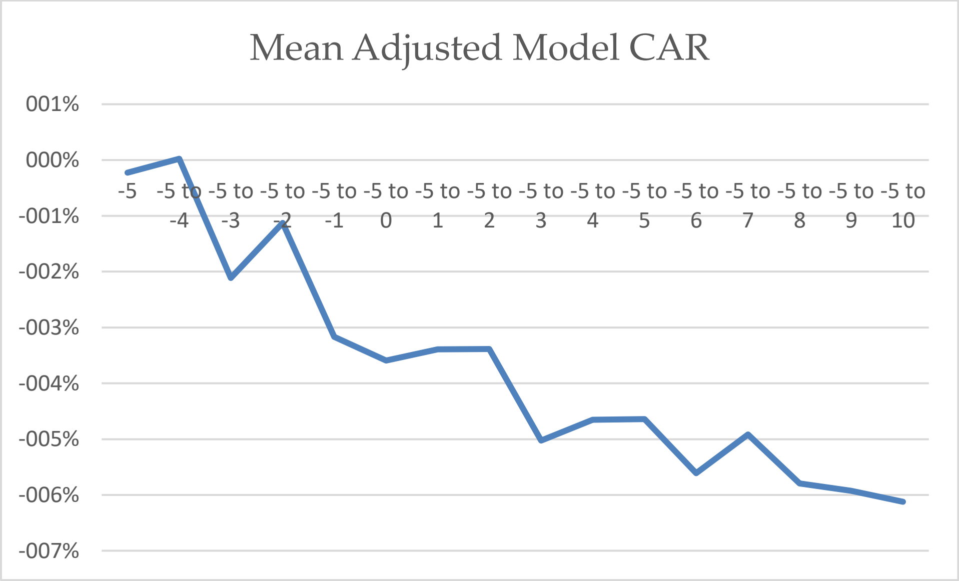


Figure 41: Cumulative abnormal returns by mean adjusted model for financials sector

Figure 41 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to decrease on day -2. The decrease in the values continued after day 0 as well.

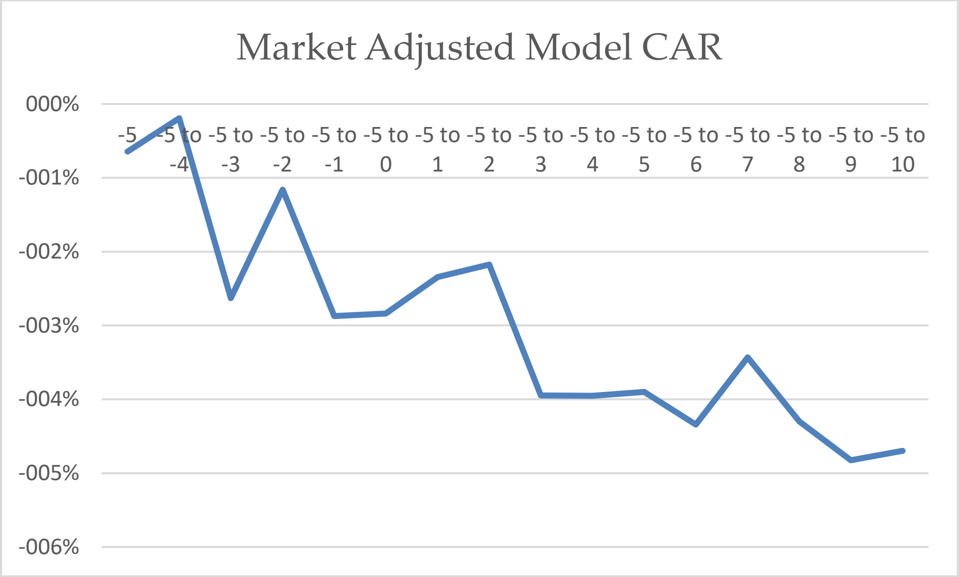


Figure 42: Cumulative abnormal returns by market adjusted model for financials sector

Figure 42 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The values have started to decrease on day -2. After a small increase after day 0, the values have started to decrease again.

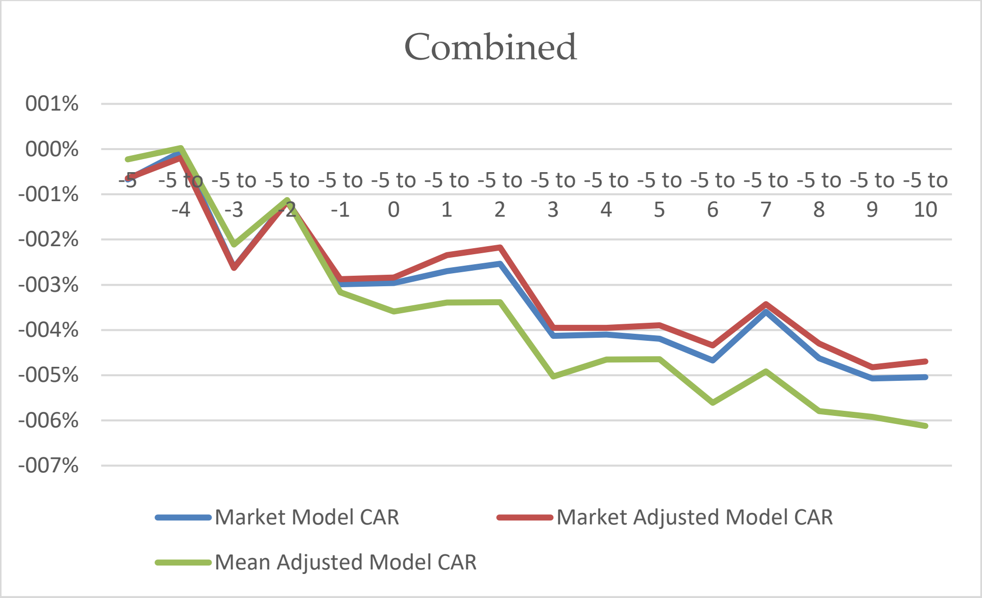


Figure 43: Comparison of the cumulative abnormal returns according to the 3 models used in the study for financials sector

Figure 43 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are matching with each other in general. However, the result of the mean adjusted model is slightly different than the other two models. Mean adjusted model results began to differ from the other two models on day -1.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 25: Cumulative Abnormal Returns for financials sector sample

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,67%	-0,64%	-0,22%
-5 to -4	-0,07%	-0,19%	0,02%
-5 to -3	-2,62%	-2,63%	-2,11%
-5 to -2	-1,14%	-1,16%	-1,13%
-5 to -1	-2,99%	-2,87%	-3,17%
-5 to 0	-2,96%	-2,84%	-3,59%
-5 to 1	-2,70%	-2,34%	-3,39%

-5 to 2	-2,53%	-2,17%	-3,39%
-5 to 3	-4,13%	-3,95%	-5,03%
-5 to 4	-4,10%	-3,95%	-4,65%
-5 to 5	-4,20%	-3,90%	-4,64%
-5 to 6	-4,67%	-4,34%	-5,61%
-5 to 7	-3,60%	-3,43%	-4,91%
-5 to 8	-4,63%	-4,30%	-5,80%
-5 to 9	-5,07%	-4,82%	-5,93%
-5 to 10	-5,04%	-4,70%	-6,12%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 26: t-statistics for financials sector sample

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	-0,44	-0,45	-0,11
-5 to -4	-0,04	-0,14	0,01
-5 to -3	-1,7**	-1,84**	-1,06
-5 to -2	-0,74	-0,81	-0,57
-5 to -1	-1,94**	-2,01***	-1,59*
-5 to 0	-1,93**	-1,99***	-1,8**
-5 to 1	-1,76**	-1,64*	-1,7**
-5 to 2	-1,65**	-1,52*	-1,7**
-5 to 3	-2,68***	-2,77***	-2,52***
-5 to 4	-2,67***	-2,77***	-2,34***
-5 to 5	-2,73***	-2,73***	-2,33***
-5 to 6	-3,04***	-3,04***	-2,82***

-5 to 7	-2,34***	-2,4***	-2,47***
-5 to 8	-3,01***	-3,01***	-2,91***
-5 to 9	-3,3***	-3,38***	-2,98***
-5 to 10	-3,28***	-3,29***	-3,08***

The hypothesis for the effect of information security breaches on financials sector was:

$H5_0$: IT related failures do not have statistically significant impact on the market value of the financials sector.

For the event window [-5,10], the null hypothesis is rejected.

5.1.3.3. Technology

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

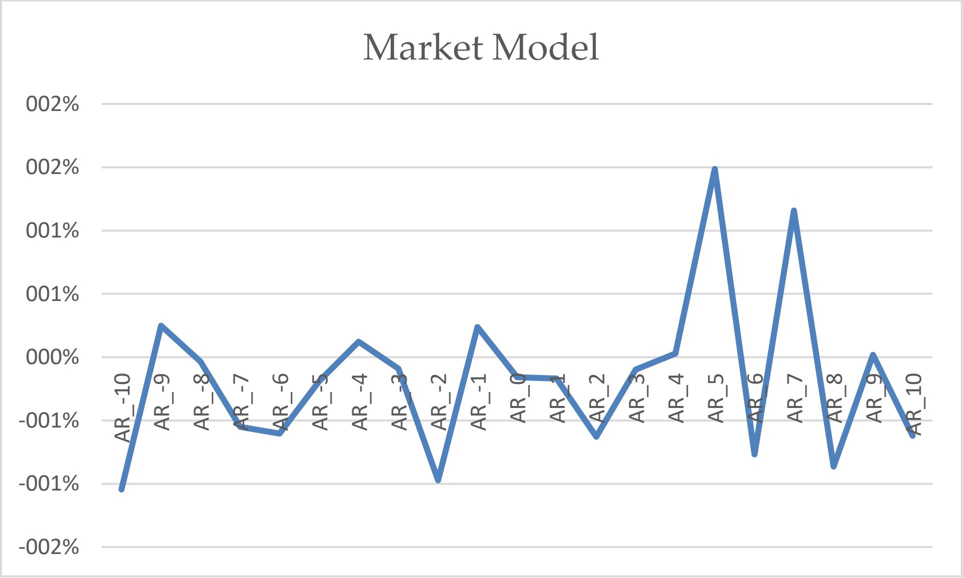


Figure 44: Abnormal returns by market model for technology sector

Figure 44 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -2 are the largest in the considered window. After that, the values start to increase except a decrease to negative value in day -2. The values have been increased sharply in day 5 which has the largest positive value similar to day 7.

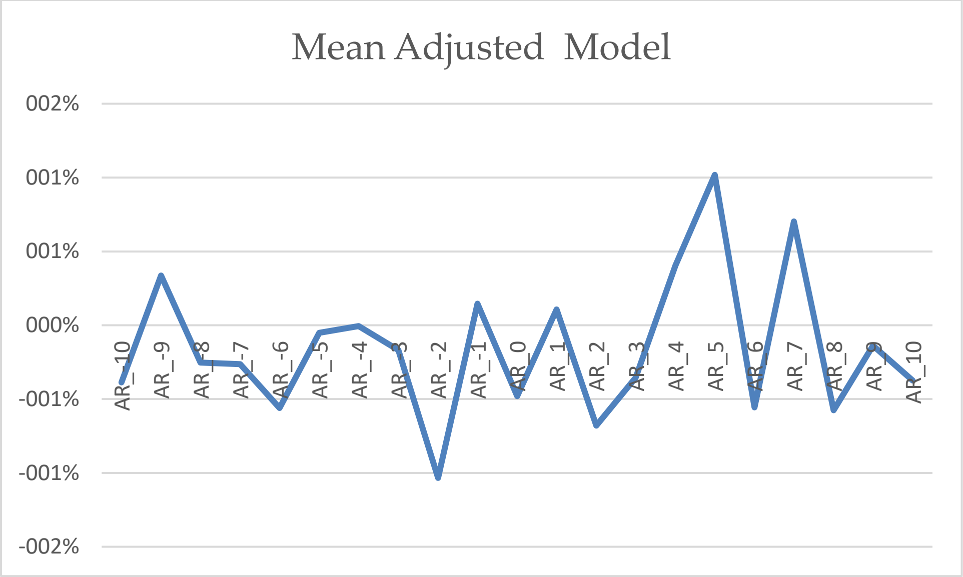


Figure 45: Abnormal returns by mean adjusted model for technology sector

Figure 45 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -2 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -1. The values have started to decrease just before the event and started to increase just after the event. The values started to increase sharply after day 3.

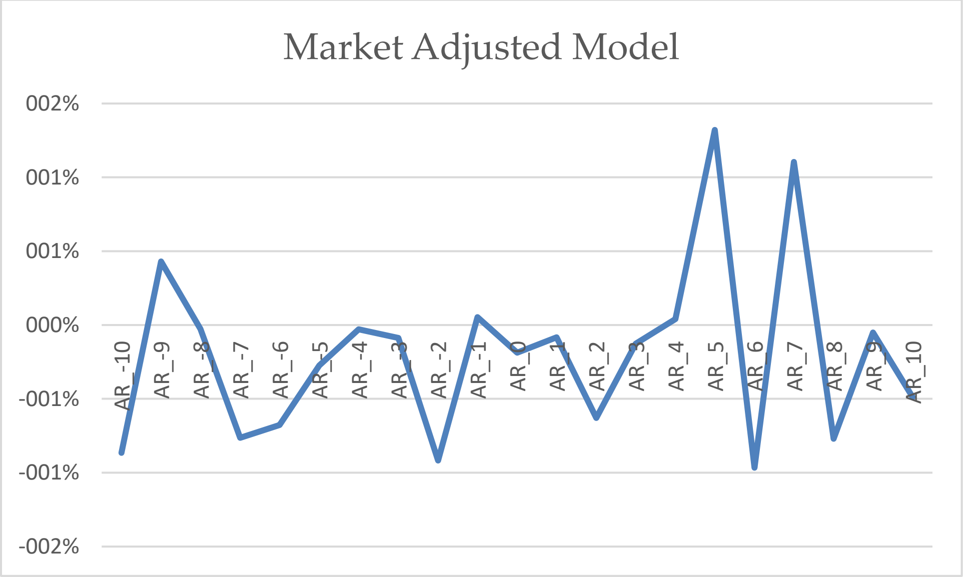


Figure 46: Abnormal returns by market adjusted model for technology sector

Figure 46 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -2 start to increase and became positive on day -1. However, after day -1, the values start to decrease again and a sharp increase can be seen after days 3 and 4.

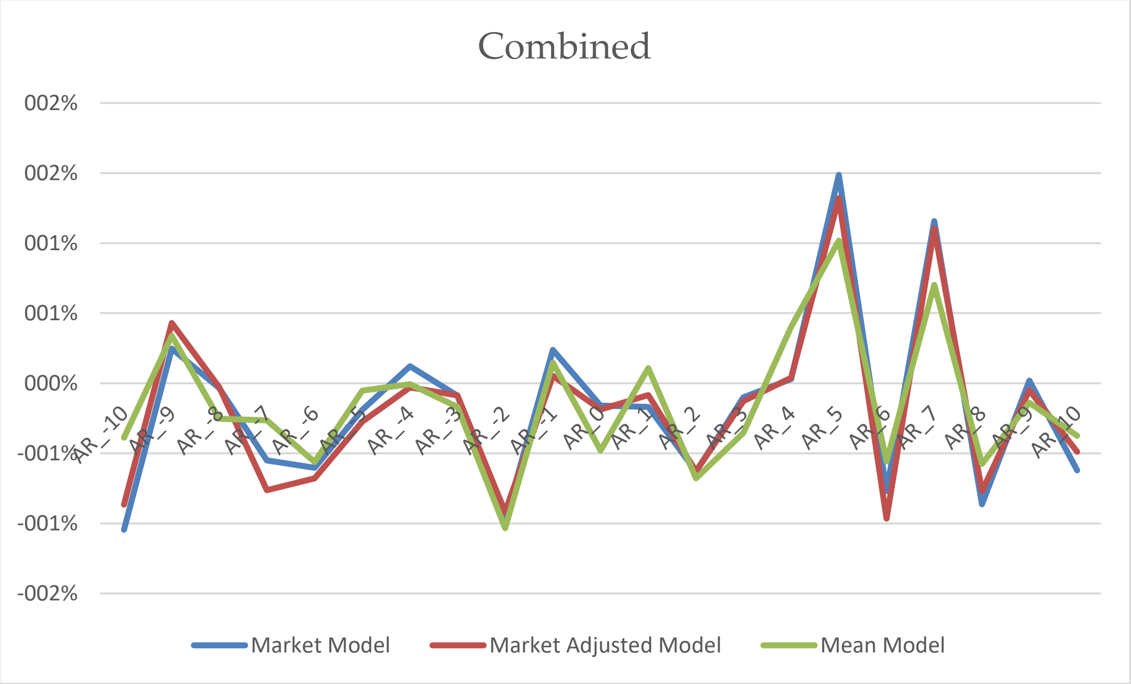


Figure 47: Comparison of the abnormal returns according to the 3 models used in the study for technology sector

Figure 47 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other 2 models on the event day. According to the mean adjusted model the values are slightly lower than the results of the market model and the market adjusted model on the event day.

Table 27 shows the specific values for the abnormal return on event day. The analyses are made specifically for the technology sector. There are different and comparable results according to the different models used in the dissertation.

Table 27: Abnormal returns on event day for the technology sector

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	-0,16%	-0,19%	-0,48%
Median Abnormal Return	-0,68%	-0,57%	-0,64%
Percentage Below Zero	61,54%	61,54%	69,23%

CUMULATIVE ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

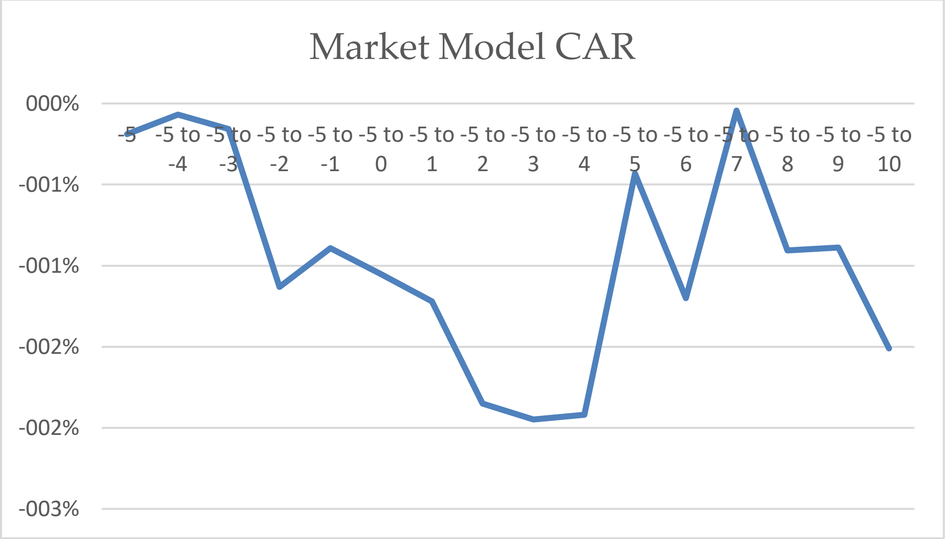


Figure 48: Cumulative abnormal returns by market model for technology sector

Figure 48 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. Beginning of the drop in returns has started on day -1. The values have started to increase after day 4.

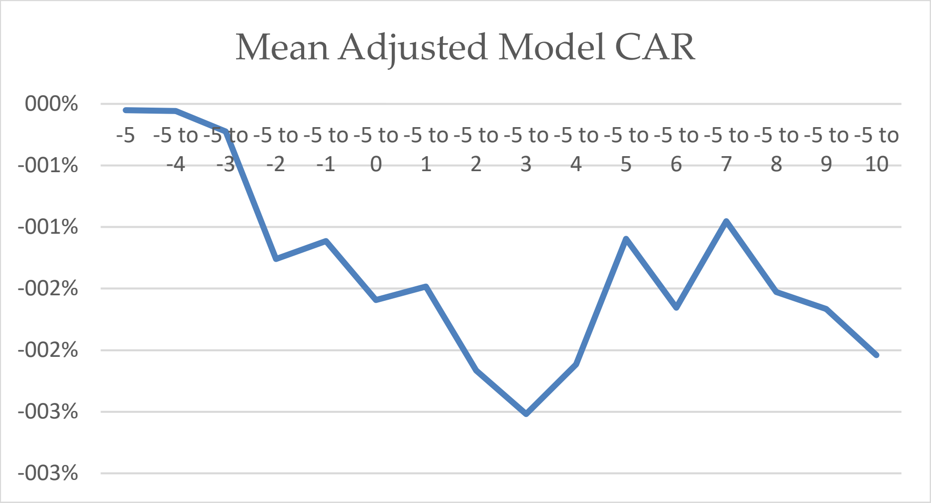


Figure 49: Cumulative abnormal returns by mean adjusted model for technology sector

Figure 49 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to decrease on day -4. The state of decrease could be observed after the event day as well. The return values have started to increase on day 3.

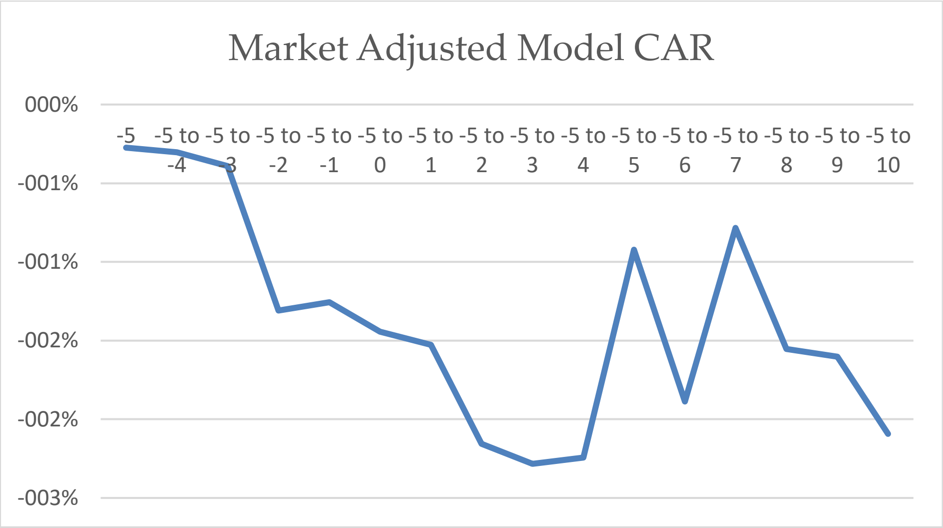


Figure 50: Cumulative abnormal returns by market adjusted model for technology sector

Figure 50 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The values have started to decrease drastically on day -3. After the event day, the values continued to decrease until day 4. The decrease on the days 5 and 7 are not stable because the values decreased again after those increases.

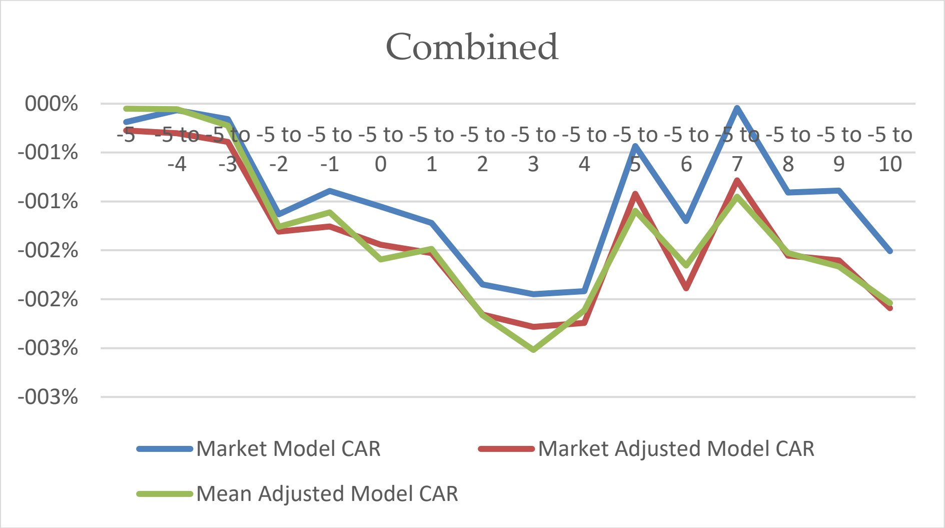


Figure 51: Comparison of the cumulative abnormal returns according to the 3 models used in the study for technology sector

Figure 51 presents the comparison of the results of the three models used in the dissertation. In general, the results coming from the market model are higher than the other two models. The values coming from the mean adjusted models and market adjusted model are matching with each other in general. However, the mean adjusted model results are slightly lower than the results of the market adjusted model a slight difference on the event day. Also, a slight difference can be observed on day 3 between the mean adjusted model and market adjusted model.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 28: Cumulative Abnormal Returns for technology sector sample

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,19%	-0,27%	-0,05%
-5 to -4	-0,07%	-0,30%	-0,06%
-5 to -3	-0,16%	-0,39%	-0,23%

-5 to -2	-1,13%	-1,31%	-1,26%
-5 to -1	-0,89%	-1,26%	-1,11%
-5 to 0	-1,05%	-1,44%	-1,59%
-5 to 1	-1,22%	-1,53%	-1,48%
-5 to 2	-1,85%	-2,16%	-2,16%
-5 to 3	-1,95%	-2,28%	-2,52%
-5 to 4	-1,92%	-2,24%	-2,12%
-5 to 5	-0,43%	-0,92%	-1,10%
-5 to 6	-1,20%	-1,89%	-1,65%
-5 to 7	-0,04%	-0,78%	-0,95%
-5 to 8	-0,91%	-1,55%	-1,53%
-5 to 9	-0,89%	-1,60%	-1,67%
-5 to 10	-1,51%	-2,09%	-2,04%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 29: t-statistics for technology sector sample

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	-0,29	-0,4	-0,07
-5 to -4	-0,1	-0,44	-0,08
-5 to -3	-0,24	-0,57	-0,3
-5 to -2	-1,74**	-1,92**	-1,69**
-5 to -1	-1,37*	-1,84**	-1,5*
-5 to 0	-1,62*	-2,12***	-2,14***
-5 to 1	-1,88**	-2,24***	-2***
-5 to 2	-2,85***	-3,16***	-2,91***
-5 to 3	-3***	-3,35***	-3,39***

-5 to 4	-2,96***	-3,29***	-2,84***
-5 to 5	-0,67	-1,35*	-1,47*
-5 to 6	-1,85**	-2,77***	-2,22***
-5 to 7	-0,07	-1,15	-1,28
-5 to 8	-1,4*	-2,28***	-2,05***
-5 to 9	-1,37*	-2,35***	-2,24***
-5 to 10	-2,33***	-3,07***	-2,74***

The hypothesis for the effect of information security breaches on technology sector was:

$H6_0$: IT related failures do not have statistically significant impact on the market value of the technology sector.

For the event window [-5,10], the null hypothesis is rejected.

5.1.3.4. Communications

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

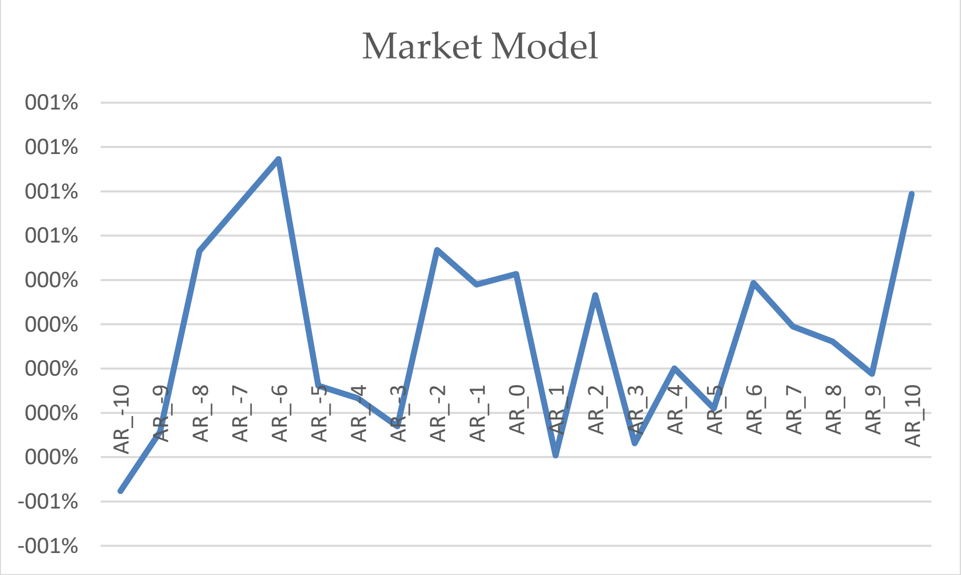


Figure 52: Abnormal returns by market model for communications sector

Figure 52 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values can be observed on day -3, day and day 3. The positive values have started to decrease on day 0 and the negativity on day 1 is the largest one. After day 9 the values started to increase sharply.

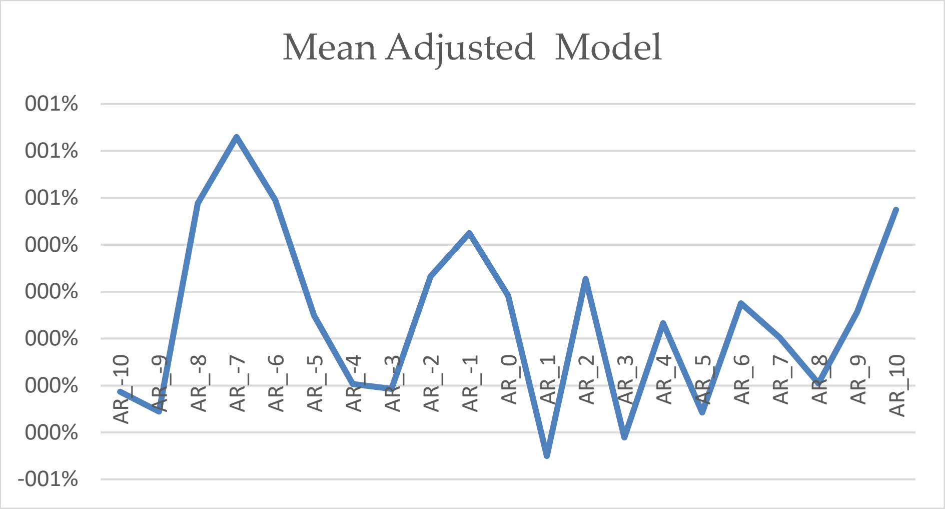


Figure 53: Abnormal returns by mean adjusted model for communications sector

Figure 53 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values show an increase between the days -3 and -1. After that, the values show a decreasing pattern until day 1. The values have started to increase after day 1 and are positive on day 2.

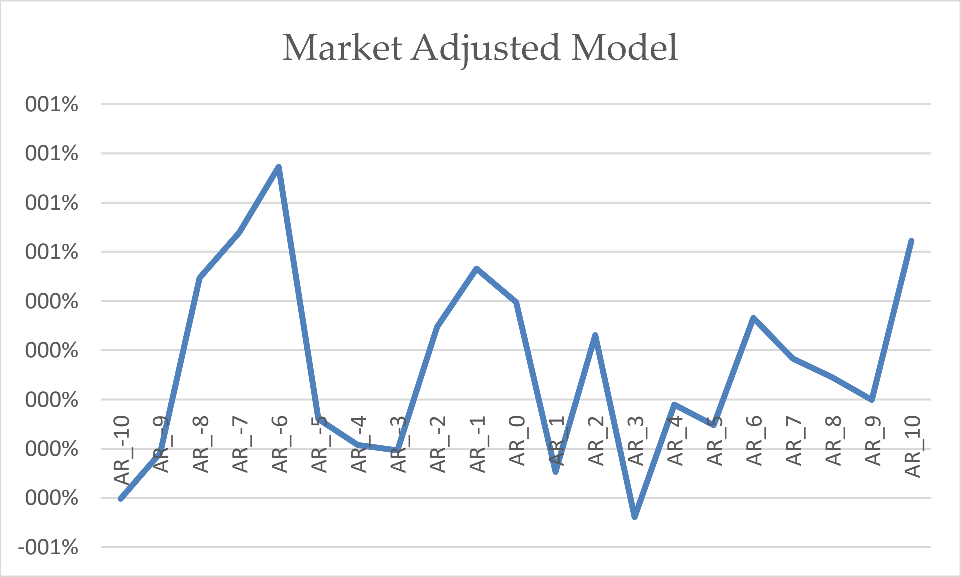


Figure 54: Abnormal returns by market adjusted model for communications sector

Figure 54 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 started to increase until day -1 and decrease after that day until day 1. An increase on the values can be observed after day 1. The negative values on day 3 are the largest in the considered window.

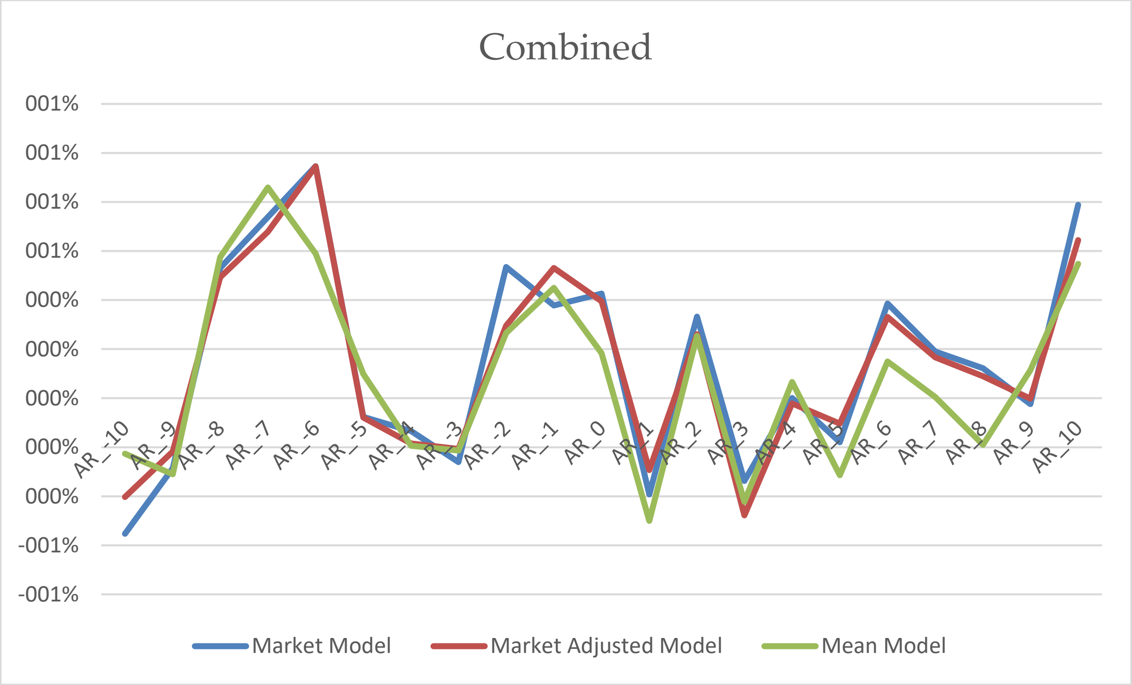


Figure 55: Comparison of the abnormal returns according to the 3 models used in the study for communications sector

Figure 55 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the models on day 0. On the event day, the market adjusted model results shows the largest values and the mean adjusted model shows the lowest values. According to the market adjusted model the values are in between of those two models.

Table 30 shows the specific values for the abnormal return on event day. The analyses are made specifically for the communications sector. There are different and comparable results according to the different models used in the dissertation.

Table 30: Abnormal returns on event day for the communications sector

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	0,43%	0,39%	0,18%
Median Abnormal Return	0,50%	0,56%	0,17%
Percentage Below Zero	37,14%	34,29%	42,86%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. There can be seen the comparison of the results of each model can be seen in the last graphic.

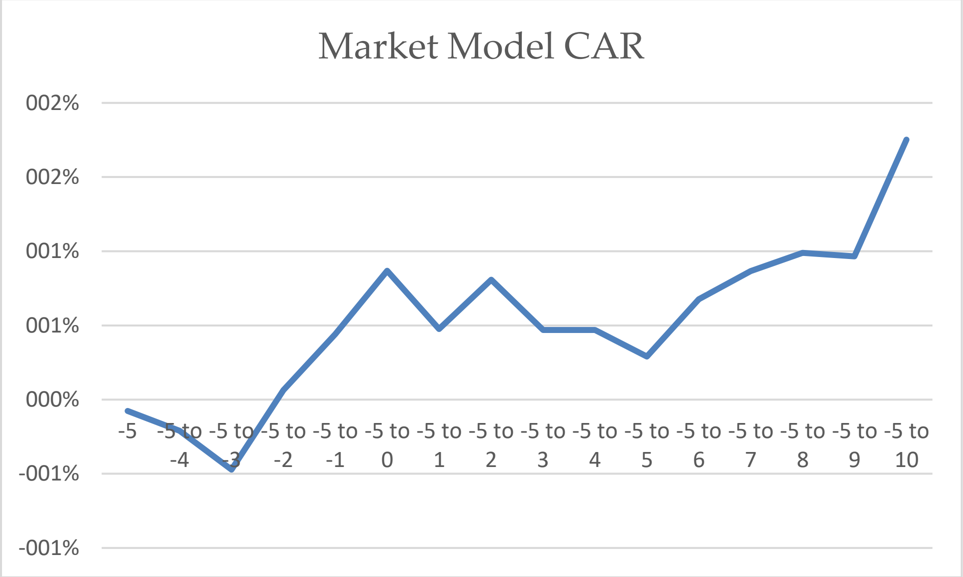


Figure 56: Cumulative abnormal returns by market model for communications sector

Figure 56 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. There is decrease in the values after the event day; however, the values have started to increase on day 2. After day 2, the values have decreased again.

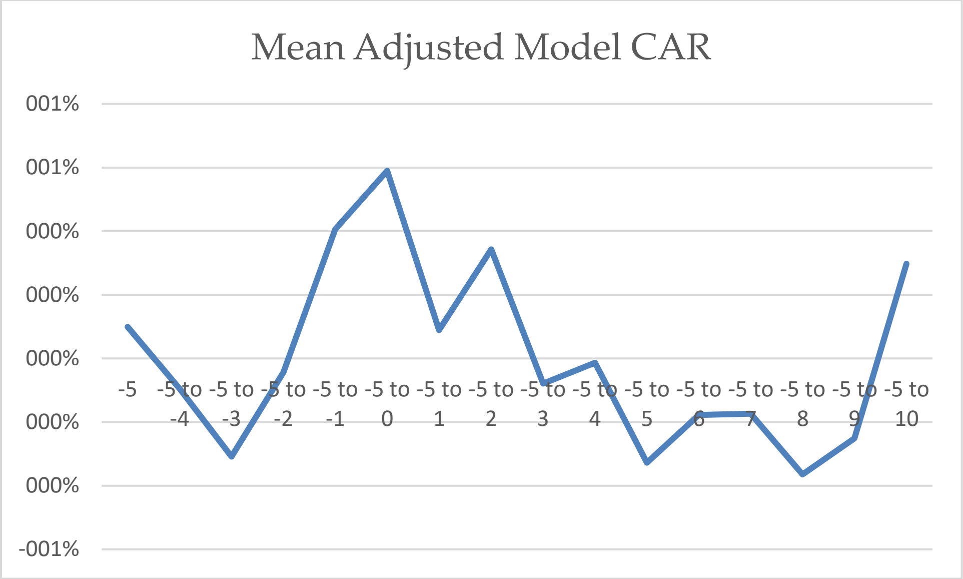


Figure 57: Cumulative abnormal returns by mean adjusted model for communications sector

Figure 57 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to increase on day -3. However, the decrease state could be observed on day 0 and the values have become negative on day 3.

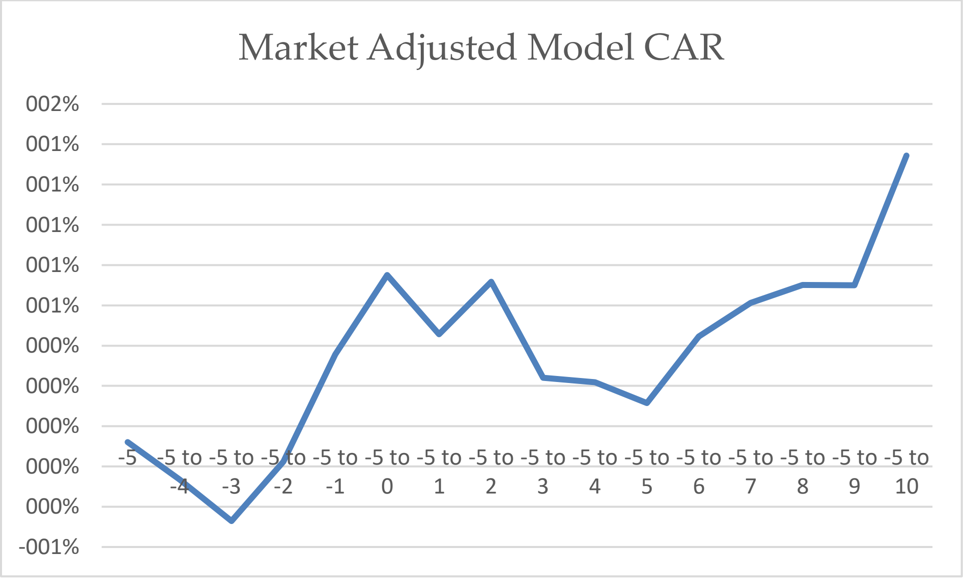


Figure 58: Cumulative abnormal returns by market adjusted model for communications sector

Figure 58 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The values have started to increase on day -3. There has been a small drop in the values on the event day and a larger decrease could be observed beginning on day 3.

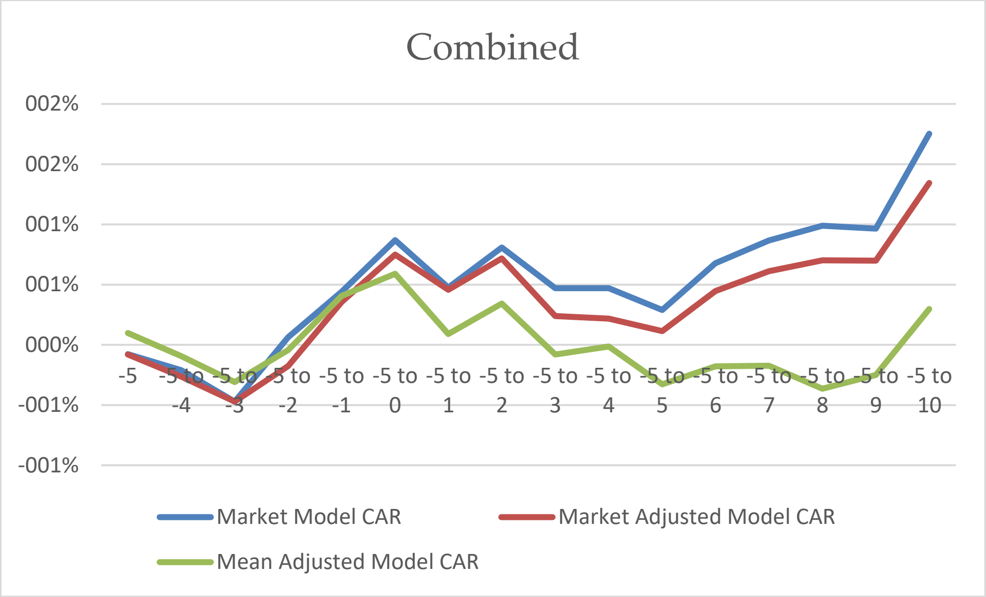


Figure 59: Comparison of the cumulative abnormal returns according to the 3 models used in the study for communications sector

Figure 59 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are matching with each other in general. However, the result of the mean adjusted model is different than the other two models. According to the mean adjusted model, the values are lower than the market model and market adjusted model. Also, the values have started to decrease on day 5 according to mean adjusted model; however, they started to increase according to the other models.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 31: Cumulative Abnormal Returns for communications sector sample

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,08%	-0,08%	0,10%
-5 to -4	-0,21%	-0,26%	-0,09%
-5 to -3	-0,47%	-0,47%	-0,31%
-5 to -2	0,06%	-0,18%	-0,04%
-5 to -1	0,44%	0,36%	0,41%
-5 to 0	0,87%	0,75%	0,59%
-5 to 1	0,48%	0,46%	0,09%
-5 to 2	0,81%	0,72%	0,34%
-5 to 3	0,47%	0,24%	-0,08%
-5 to 4	0,47%	0,22%	-0,01%
-5 to 5	0,29%	0,11%	-0,33%
-5 to 6	0,68%	0,45%	-0,18%
-5 to 7	0,87%	0,61%	-0,17%
-5 to 8	0,99%	0,70%	-0,36%
-5 to 9	0,96%	0,70%	-0,25%
-5 to 10	1,75%	1,34%	0,30%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 32: t-statistics for communications sector sample

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	-0,14	-0,17	0,35
-5 to -4	-0,39	-0,57	-0,33

-5 to -3	-0,87	-1,02	-1,09
-5 to -2	0,12	-0,38	-0,15
-5 to -1	0,81	0,77	1,43*
-5 to 0	1,6*	1,62*	2,07***
-5 to 1	0,88	0,99	0,31
-5 to 2	1,49*	1,55*	1,2
-5 to 3	0,86	0,52	-0,28
-5 to 4	0,86	0,47	-0,05
-5 to 5	0,53	0,25	-1,15
-5 to 6	1,24	0,96	-0,63
-5 to 7	1,59*	1,32*	-0,61
-5 to 8	1,82**	1,51*	-1,28
-5 to 9	1,77**	1,51*	-0,88
-5 to 10	3,22***	2,9***	1,05

The hypothesis for the effect of information security breaches on communications sector was:

$H7_0$: IT related failures do not have statistically significant impact on the market value of the communications sector.

For the event window [-5,10], the null hypothesis is rejected.

5.1.4. DOES THE LOST RECORD SIZE HAVE EFFECT ON THE FAILURE IMPACT?

For assessing the impacts of the data breaches according to the lost record size the sample has been divided into 4 groups. The reason of grouping the sample in 4 groups is being able to see the effects of privacy breaches on different groups which are affected from privacy breaches on different severity levels.

Group 1 includes the lost record sizes between 100 and 114,000; Group 2 includes the lost record sizes between 125,000 and 1,500,000; Group 3 includes the lost record sizes between 1,600,000 and 11,100,000; Group 4 includes the lost record sizes between 12.367.232 and 152,000,000.

Analyses have been made for these 4 groups separately and the results can be seen below:

5.1.4.1. GROUP 1

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

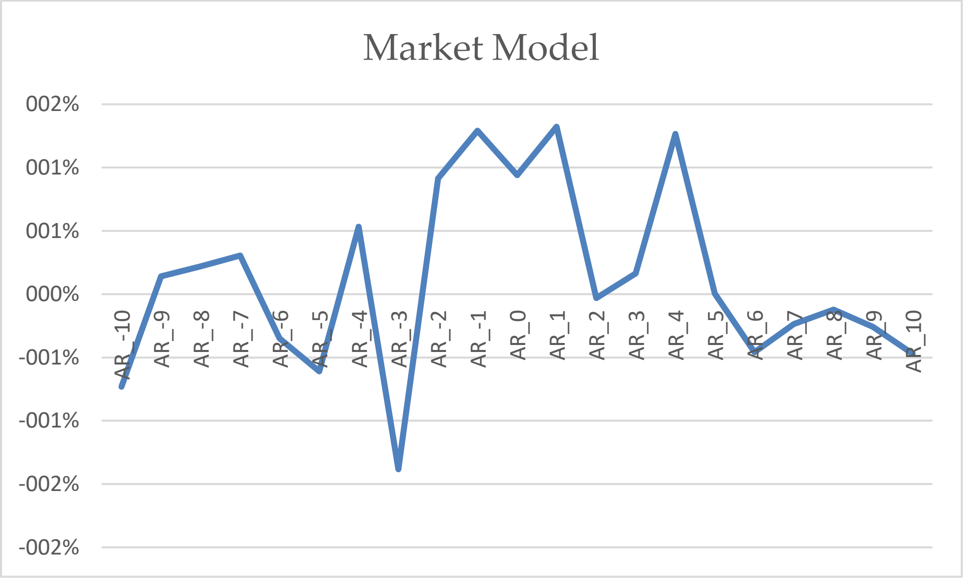


Figure 60: Abnormal returns by market model for group 1

Figure 60 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. The values decreased again on day +1, and an increase is started on day +2. The values showed an unstable stance after the event day.

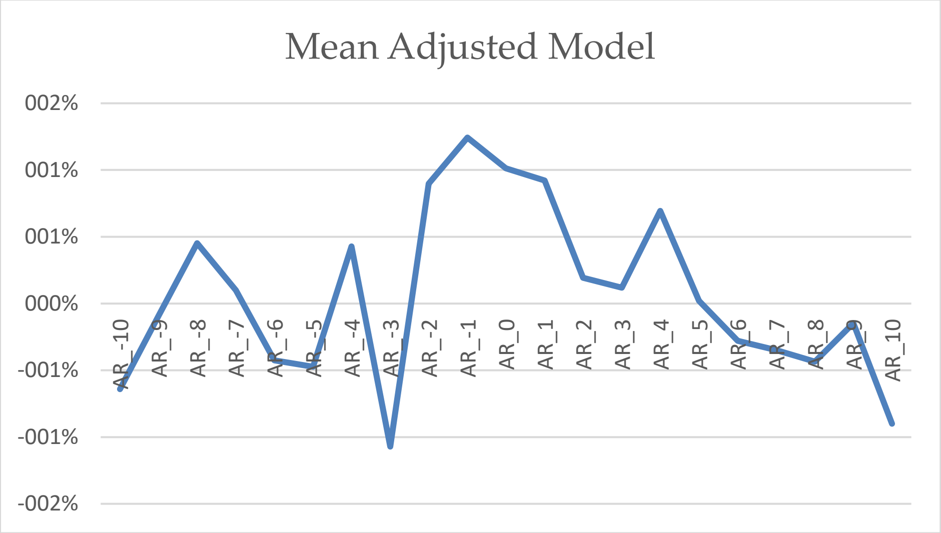


Figure 61: Abnormal returns by mean adjusted model for Group 1

Figure 61 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. The values started to decrease again on day -1, and continued until day +3. After a small increase, the values started to decrease again.

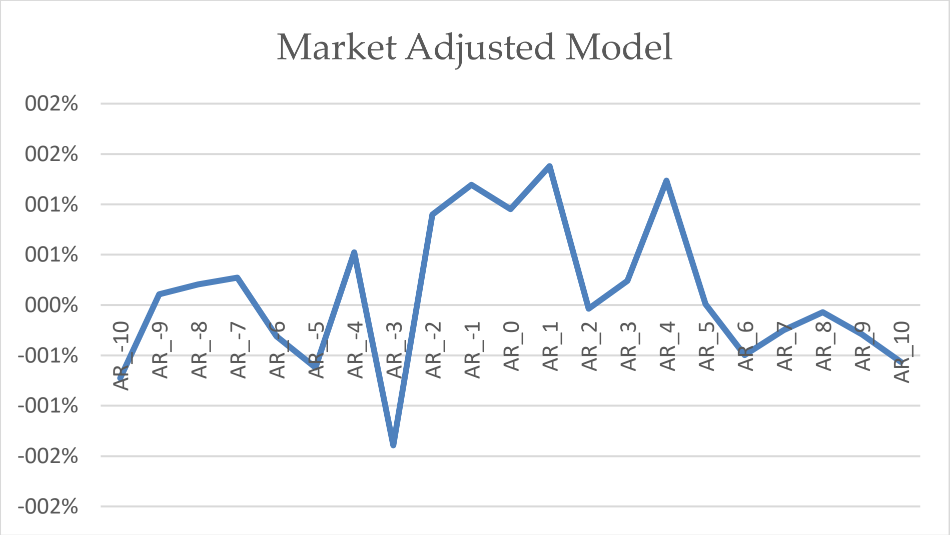


Figure 62: Abnormal returns by market adjusted model for Group 1

Figure 62 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest and the most significant in the window considered. After that, the values increased and the abnormal return became positive in day -2. The values started to decrease again on day +1 and after an increase the values have started to decrease again on day +4.

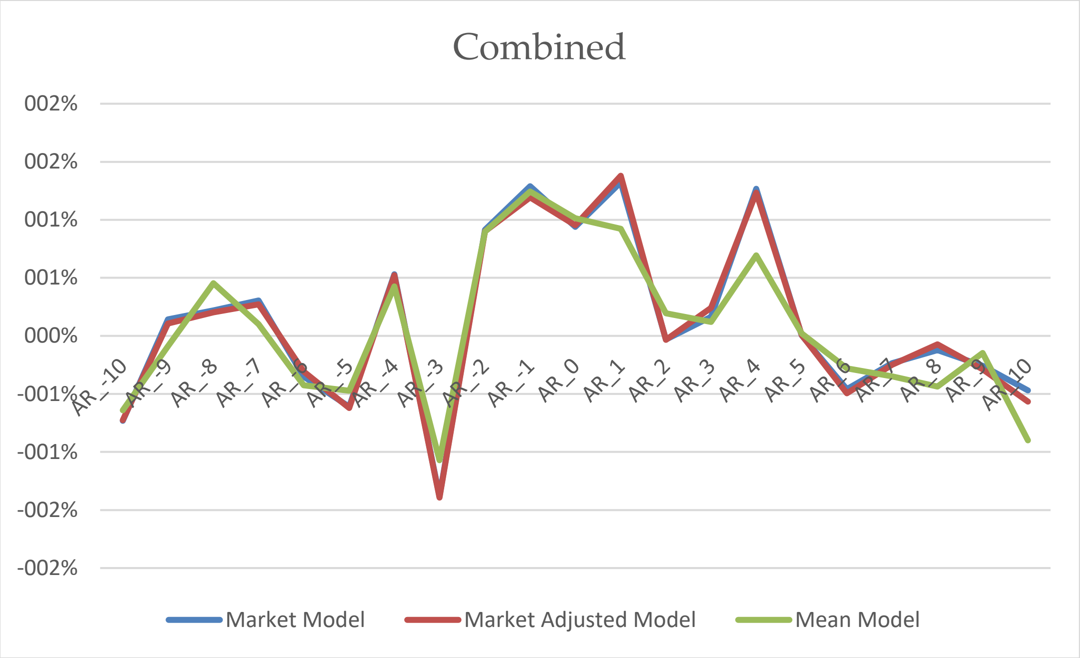


Figure 63: Comparison of the abnormal returns according to the 3 models used in the study for Group 1

Figure 63 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the models between day 0 and day +2. On the event day, the market model and the market adjusted model results show nearly the same values, however, the mean adjusted model shows slightly lower values than the other two models.

Table 33 shows the specific values for the abnormal return on event day for Group 1. There are different and comparable results according to the different models used in the dissertation.

Table 33: Abnormal returns on event day for Group 1

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal	0,94%	0,95%	1,01%

Return			
Median Abnormal Return	-0,12%	0,10%	0,39%
Percentage Below Zero	53,33%	46,67%	40,00%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

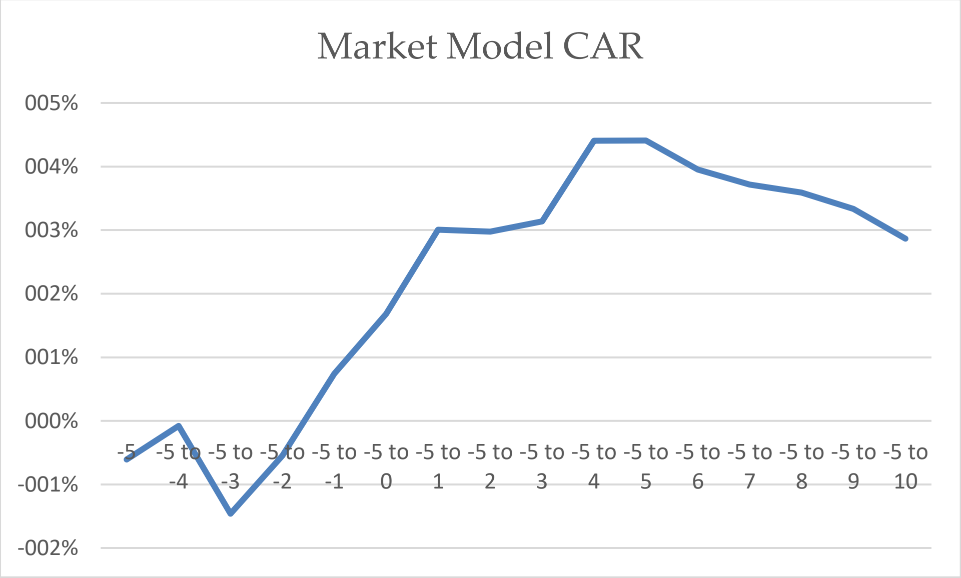


Figure 64: Cumulative abnormal returns by market model for Group 1

Figure 64 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. There is no decrease in the values after the event day; in fact, the values have started to increase on day -3. Only after day 5, the values started to decrease again.

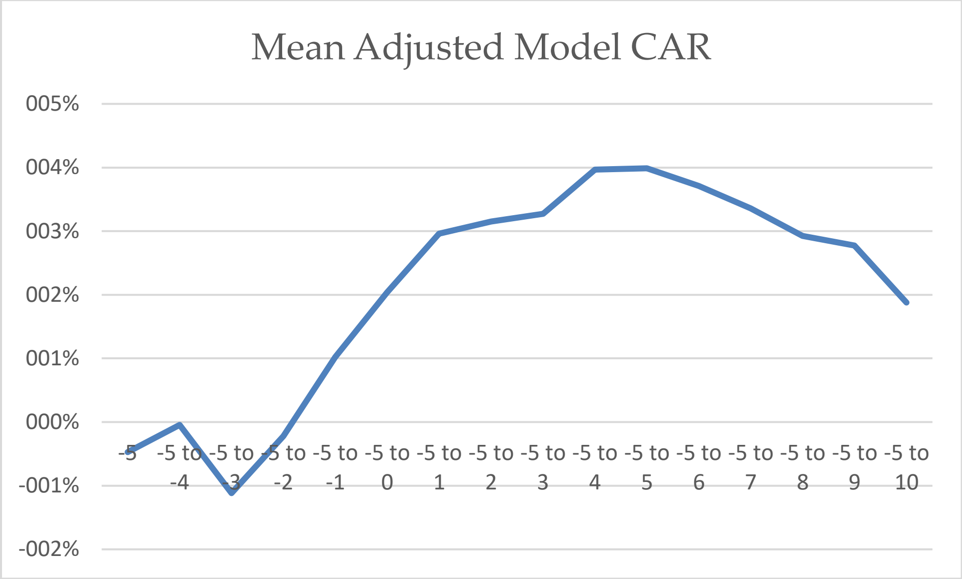


Figure 65: Cumulative abnormal returns by mean adjusted model for Group 1

Figure 65 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. There is no decrease in the values after the event day; in fact, the values have started to increase on day -3. Only after day 5, the values started to decrease again.

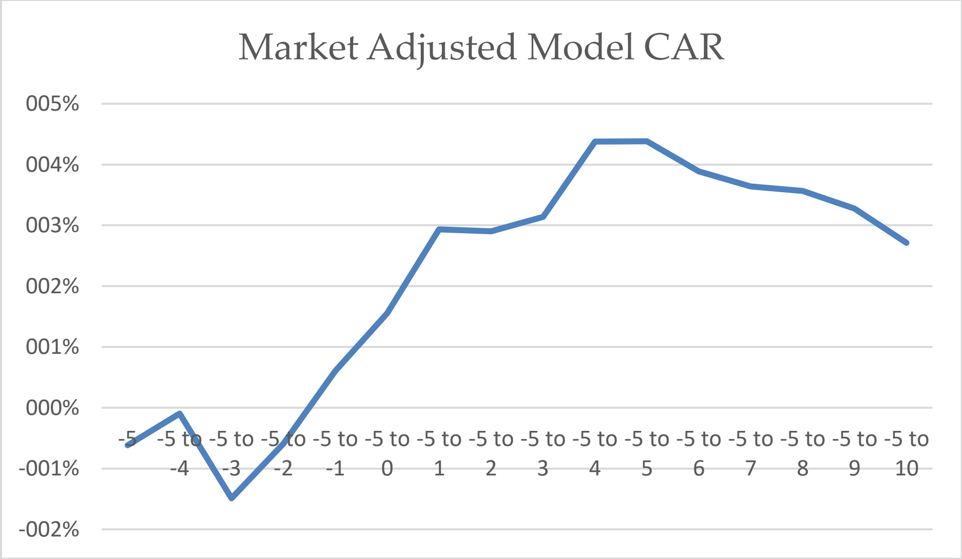


Figure 66: Cumulative abnormal returns by market adjusted model for group 1

Figure 66 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. There is no decrease in the values after the event day; in fact, the values have started to increase on day -3. Only after day 5, the values started to decrease again.

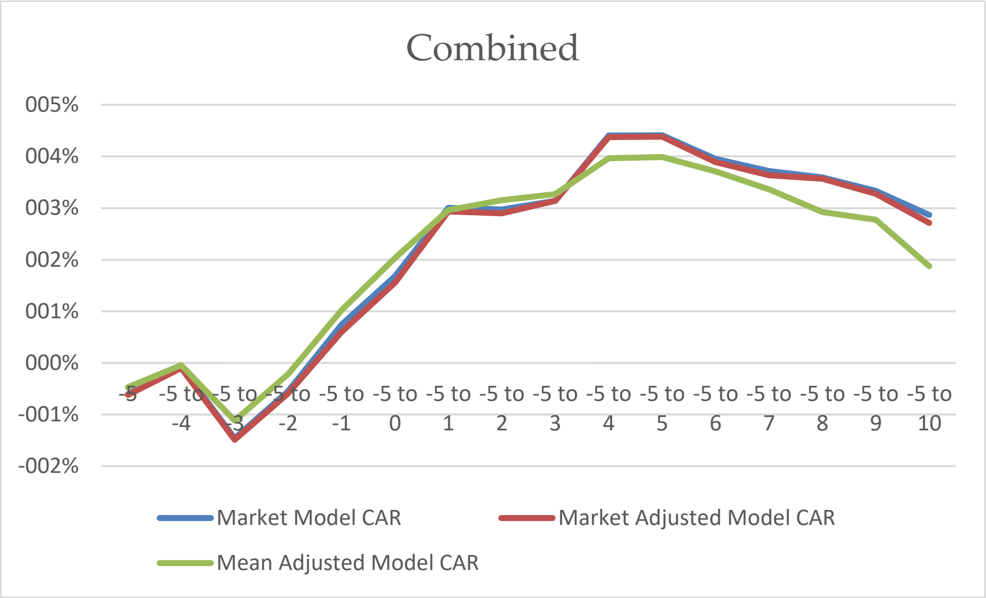


Figure 67: Comparison of the cumulative abnormal returns according to the 3 models used in the study for group 1

Figure 67 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model, market adjusted model and the mean adjusted model are matching with each other in general. However, the result of the mean adjusted model is slightly different than the other two models. According to the mean adjusted model, the cumulative values are slightly lower than the market model and market adjusted model.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 34: Cumulative Abnormal Returns for Group 1

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,61%	-0,62%	-0,47%
-5 to -4	-0,08%	-0,10%	-0,05%
-5 to -3	-1,46%	-1,49%	-1,12%
-5 to -2	-0,55%	-0,59%	-0,22%

-5 to -1	0,74%	0,60%	1,02%
-5 to 0	1,68%	1,56%	2,04%
-5 to 1	3,01%	2,94%	2,96%
-5 to 2	2,97%	2,90%	3,15%
-5 to 3	3,14%	3,14%	3,27%
-5 to 4	4,41%	4,38%	3,97%
-5 to 5	4,41%	4,38%	3,99%
-5 to 6	3,95%	3,89%	3,71%
-5 to 7	3,71%	3,64%	3,36%
-5 to 8	3,59%	3,57%	2,92%
-5 to 9	3,34%	3,28%	2,78%
-5 to 10	2,86%	2,71%	1,88%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 35: t-statistics for Group 1

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	-0,31	-0,32	-0,28
-5 to -4	-0,04	-0,05	-0,03
-5 to -3	-0,75	-0,76	-0,65
-5 to -2	-0,28	-0,3	-0,13
-5 to -1	0,38	0,31	0,6
-5 to 0	0,86	0,8	1,19
-5 to 1	1,54*	1,5*	1,73**
-5 to 2	1,52*	1,49*	1,85**
-5 to 3	1,61*	1,61*	1,92**

-5 to 4	2,25***	2,24***	2,32***
-5 to 5	2,26***	2,25***	2,34***
-5 to 6	2,02***	1,99***	2,17***
-5 to 7	1,9**	1,86**	1,97***
-5 to 8	1,84**	1,83**	1,71**
-5 to 9	1,71**	1,68**	1,63*
-5 to 10	1,47*	1,39*	1,1

The hypothesis for the effect of information security breaches on different group 1 data size loss:

$H8_0$: IT related failures do not have statistically significant impact on Group 1 data size loss

For the event window [-5,10], the null hypothesis is rejected (For the market model and market adjusted model).

5.1.4.2. GROUP 2

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

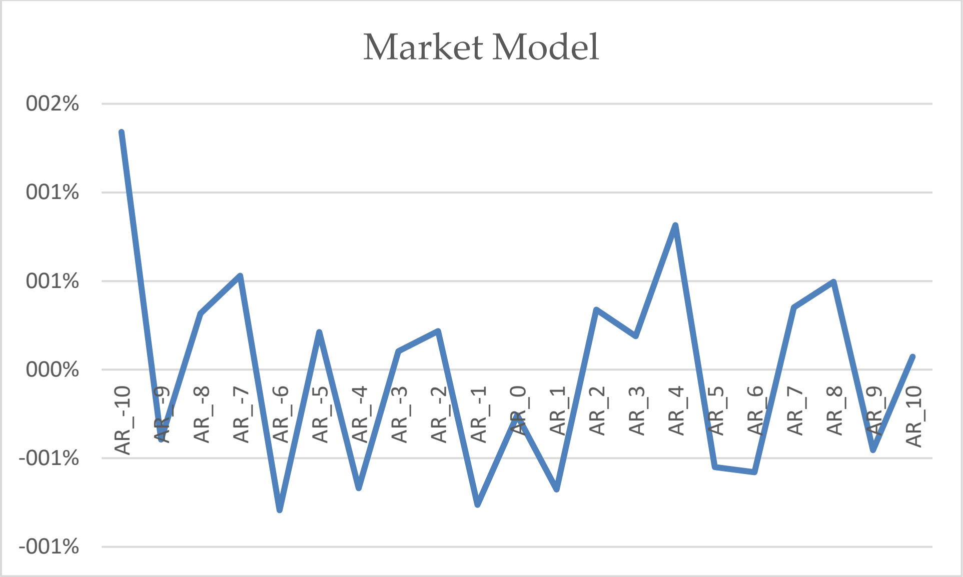


Figure 68: Abnormal returns by market model for Group 2

Figure 68 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. Although values have stayed negatively in a three-day period, including 1 day before the event day, event day and 1 day after the event day. There is a decrease in the values on day 5 and day 6 again.

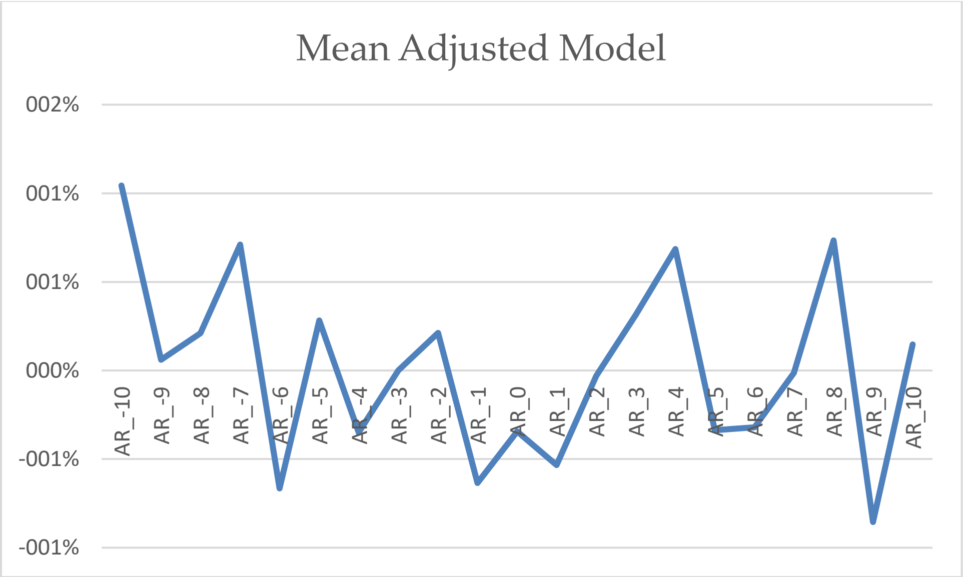


Figure 69: Abnormal returns by mean adjusted model for Group 2

Figure 69 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. The values have stayed negatively between day -2 and day 2. After an increase in the values, the values have started to decrease again on day 4. There is a decrease in the values on day 5 and day 6 again.

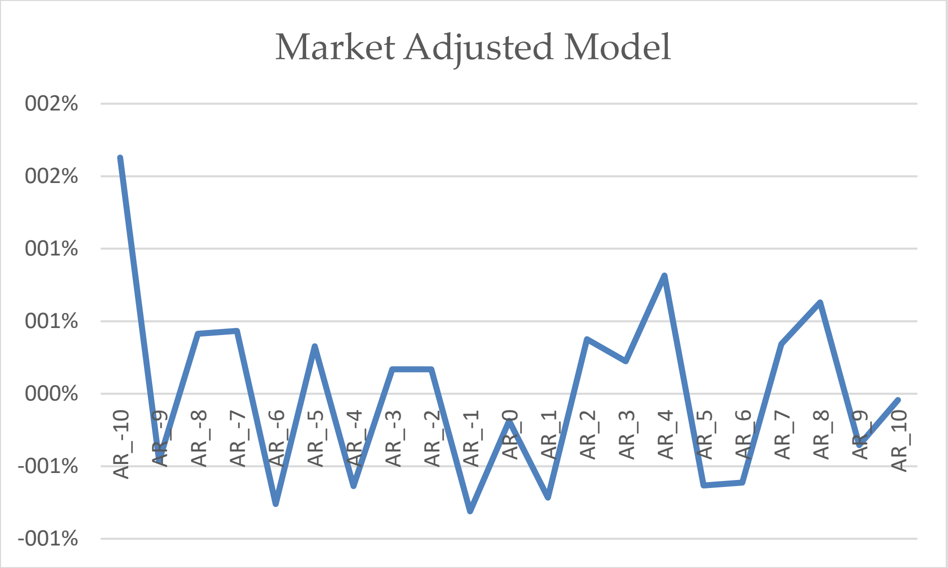


Figure 70: Abnormal returns by market adjusted model for Group 2

Figure 70 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. Although values have stayed negatively in a three-day period, including 1 day before the event day, event day and 1 day after the event day. There is a decrease in the values after day 4.

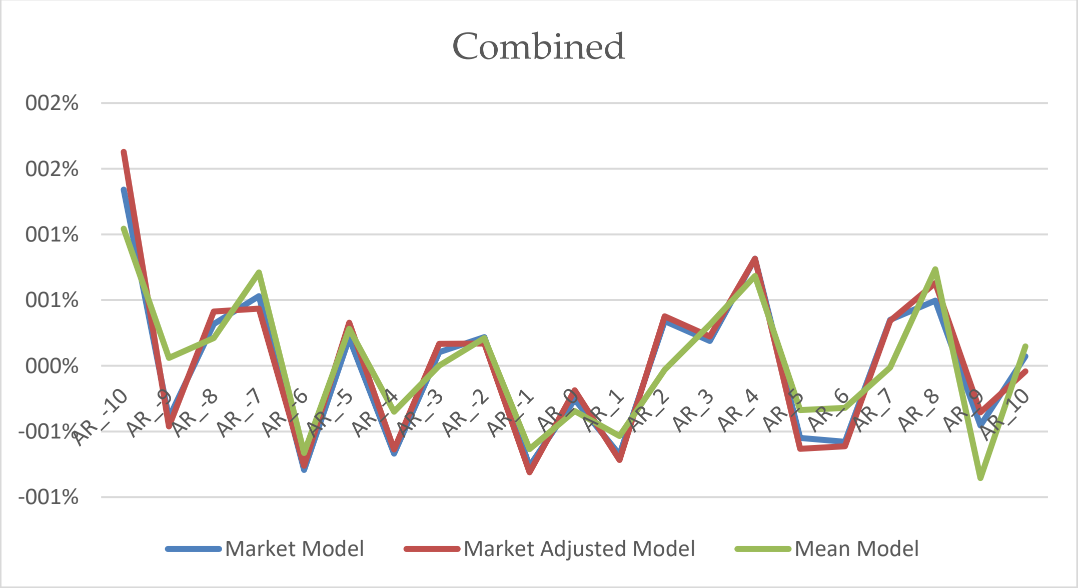


Figure 71: Comparison of the abnormal returns according to the 3 models used in the study for Group 2

Figure 71 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general considering some slight differences in the mean adjusted model.

Table 36 shows the specific values for the abnormal return on event day Group 2. There are different and comparable results according to the different models used in the dissertation.

Table 36: Abnormal returns on event day for the Group 2

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	-0,26%	-0,19%	-0,34%
Median Abnormal Return	0,05%	0,03%	-0,08%
Percentage Below Zero	40,00%	46,67%	53,33%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

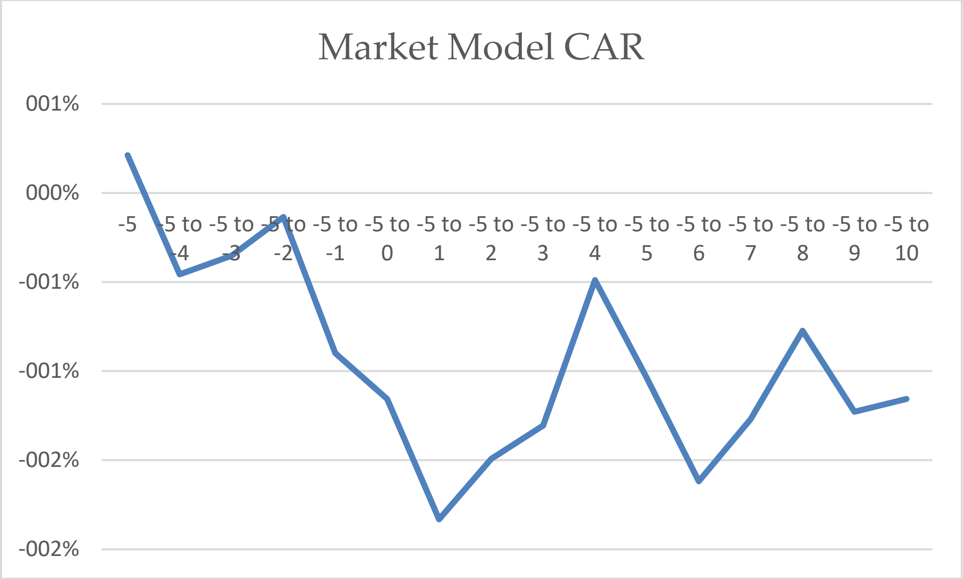


Figure 72: Cumulative abnormal returns by market model for Group 2

Figure 72 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. The decrease in the values started on day -2 and started to increase again after the event day. Although some increase in the values can be observed after the event, they have not been gone into the positive side.

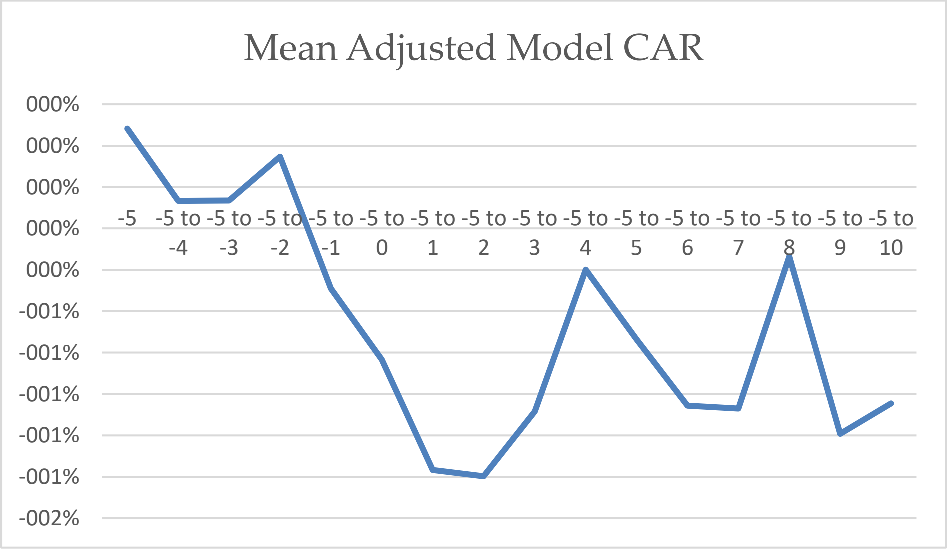


Figure 73: Cumulative abnormal returns by mean adjusted model for Group 2

Figure 73 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. There is a decrease in the values before 2 days of the event day; in fact, the values have started to increase on day -3. Only after day 5, the values started to decrease again. The decrease in the values started on day -2 and started to increase again 2 days after the event day. Although some increase in the values can be observed after the event, they have not been gone into the positive side.

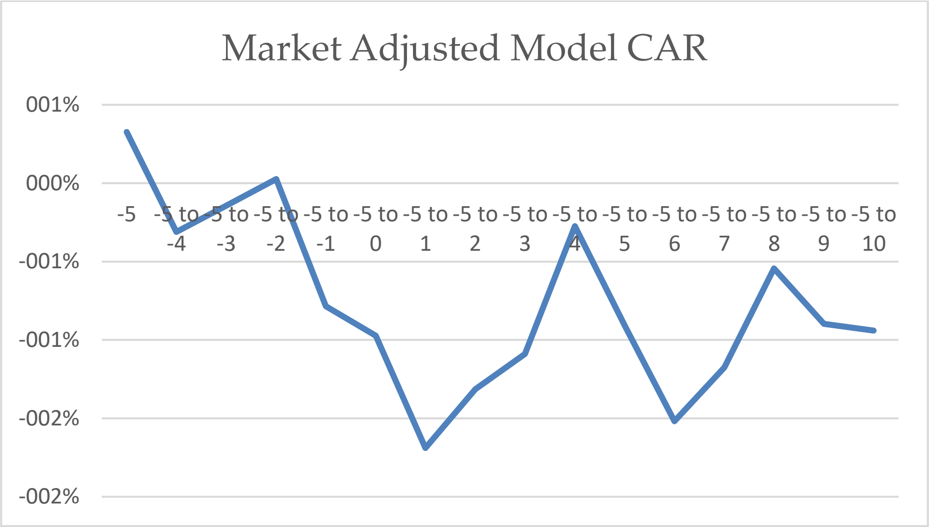


Figure 74: Cumulative abnormal returns by market adjusted model for Group 2

Figure 74 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. There is a decrease in the values before 2 days of the event day and the values have started to increase on day 1. Although some increase in the values can be observed after the event, they have not been gone into the positive side.

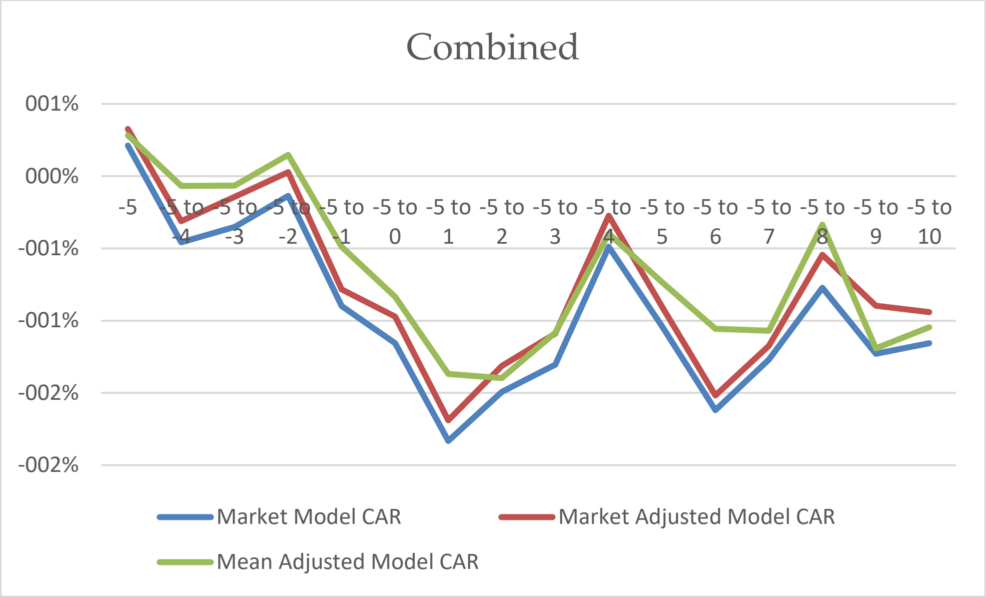


Figure 75: Comparison of the cumulative abnormal returns according to the 3 models used in the study for group 2

Figure 75 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model, market adjusted model and the mean adjusted model are matching with each other in general. However, the result of the market model is slightly different than the other two models. According to the market model, the cumulative values are slightly lower than the market adjusted model and mean adjusted model.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 37: Cumulative Abnormal Returns for Group 2

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	0,21%	0,33%	0,28%
-5 to -4	-0,46%	-0,31%	-0,07%
-5 to -3	-0,35%	-0,14%	-0,07%
-5 to -2	-0,14%	0,03%	0,15%
-5 to -1	-0,90%	-0,78%	-0,49%
-5 to 0	-1,16%	-0,97%	-0,83%

-5 to 1	-1,83%	-1,69%	-1,37%
-5 to 2	-1,49%	-1,31%	-1,40%
-5 to 3	-1,30%	-1,09%	-1,08%
-5 to 4	-0,49%	-0,27%	-0,40%
-5 to 5	-1,04%	-0,91%	-0,74%
-5 to 6	-1,62%	-1,52%	-1,06%
-5 to 7	-1,27%	-1,17%	-1,07%
-5 to 8	-0,77%	-0,54%	-0,34%
-5 to 9	-1,23%	-0,90%	-1,19%
-5 to 10	-1,16%	-0,94%	-1,04%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 38: t-statistics for Group 2

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	0,38	0,58	0,52
-5 to -4	-0,81	-0,55	-0,12
-5 to -3	-0,62	-0,25	-0,12
-5 to -2	-0,24	0,05	0,27
-5 to -1	-1,59*	-1,39*	-0,9
-5 to 0	-2,05***	-1,72**	-1,53*
-5 to 1	-3,25***	-2,98***	-2,51***
-5 to 2	-2,65***	-2,32***	-2,56***
-5 to 3	-2,31***	-1,92**	-1,99***
-5 to 4	-0,87	-0,48	-0,73
-5 to 5	-1,84**	-1,6*	-1,35*

-5 to 6	-2,87***	-2,68***	-1,94**
-5 to 7	-2,25***	-2,07***	-1,96***
-5 to 8	-1,37*	-0,96	-0,62
-5 to 9	-2,18***	-1,59*	-2,19***
-5 to 10	-2,05***	-1,66**	-1,92**

The hypothesis for the effect of information security breaches on different group 2 data size loss:

H9$_0$: IT related failures do not have statistically significant impact on Group 2 data size loss

For the event window [-5,10], the null hypothesis is rejected.

5.1.4.3. GROUP 3

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

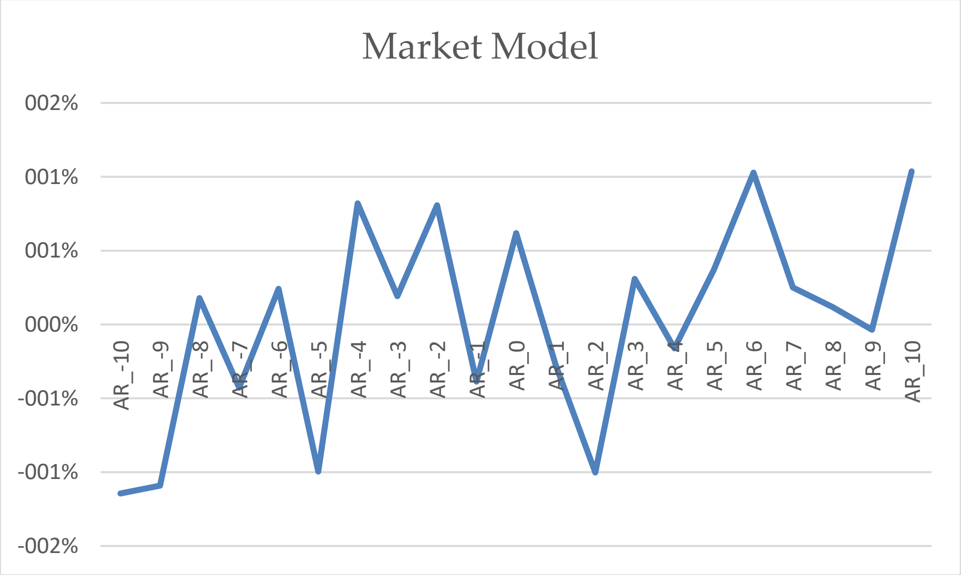


Figure 76: Abnormal returns by market model for Group 3

Figure 76 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. The only striking decrease happens on the announcement date of the event. The values have gone from positive to negative. After day +2, the values increased again and after a slight decrease on day 3, the values have started to increase again on day +4.

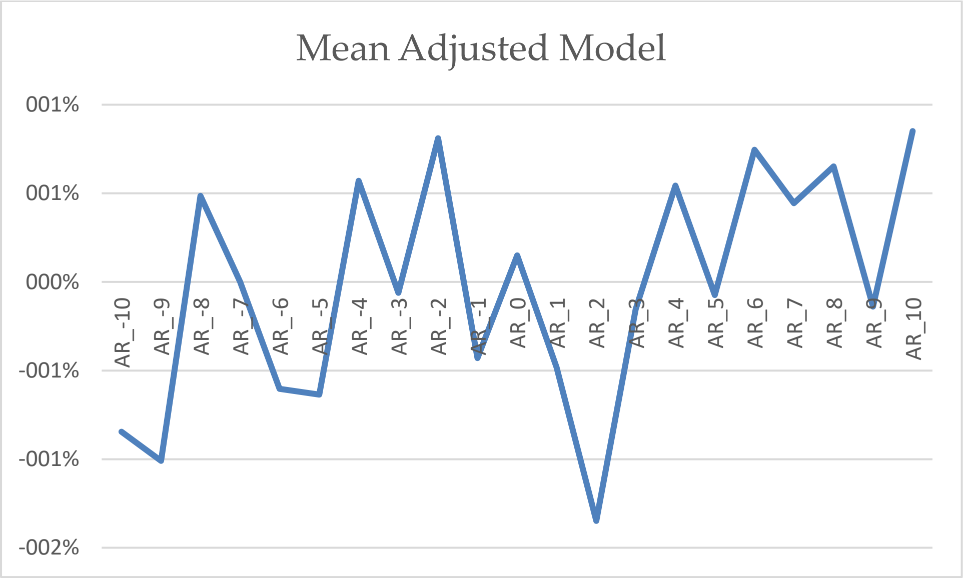


Figure 77: Abnormal returns by mean adjusted model for Group 3

Figure 77 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. There is a striking decrease on the values on the announcement date. The values have decreased sharply from day 0 to day +2. After day +2, the values have started to increase and become positive.

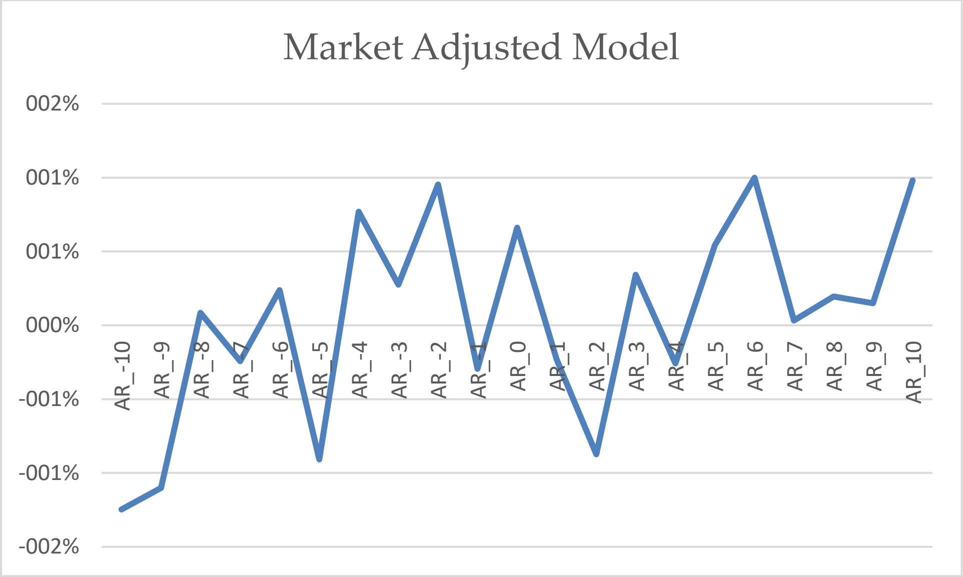


Figure 78: Abnormal returns by market adjusted model for Group 3

Figure 78 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. There is a sharp decrease in the values after the announcement until day +2. After day +4, the values remained positive.

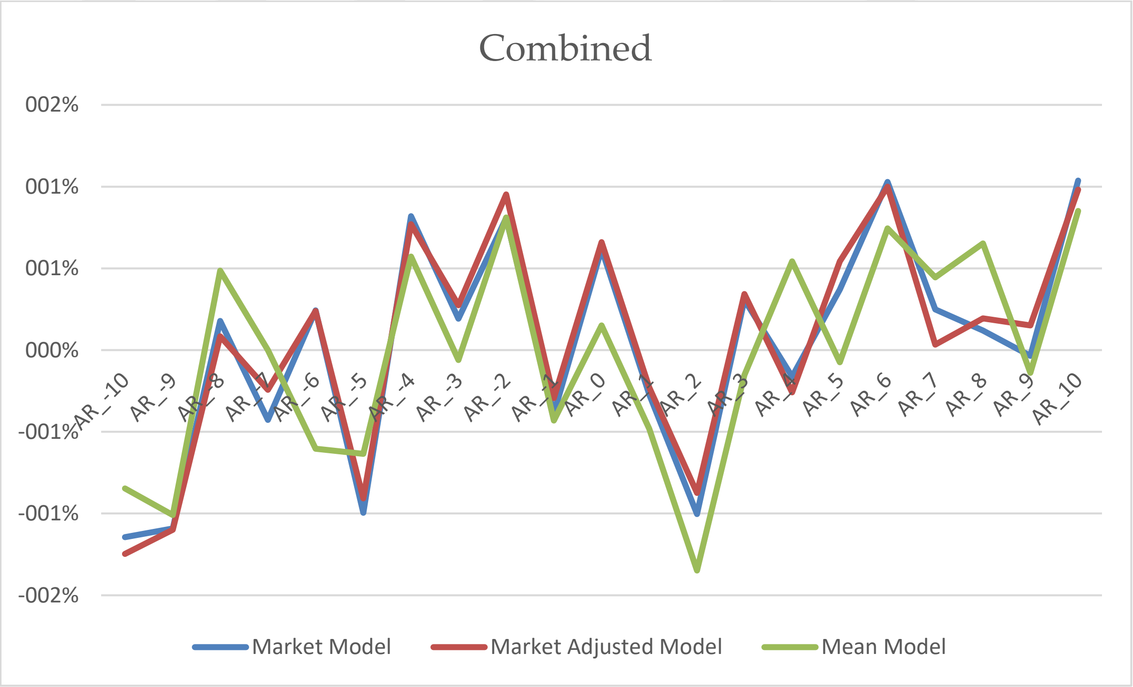


Figure 79: Comparison of the abnormal returns according to the 3 models used in the study for Group 3

Figure 79 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general considering some slight differences in the mean adjusted model. The mean adjusted model results are slightly lower from the other results especially between days -1 and +3.

Table 39 shows the specific values for the abnormal return on event day for Group 3. There are different and comparable results according to the different models used in the dissertation.

Table 39: Abnormal returns on event day for Group 3

ARt=0	**Market Model**	**Market Adjusted Model**	**Mean Model**
Mean Abnormal Return	0,62%	0,66%	0,15%
Median Abnormal Return	0,27%	0,27%	0,29%
Percentage Below Zero	41,18%	47,06%	41,18%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

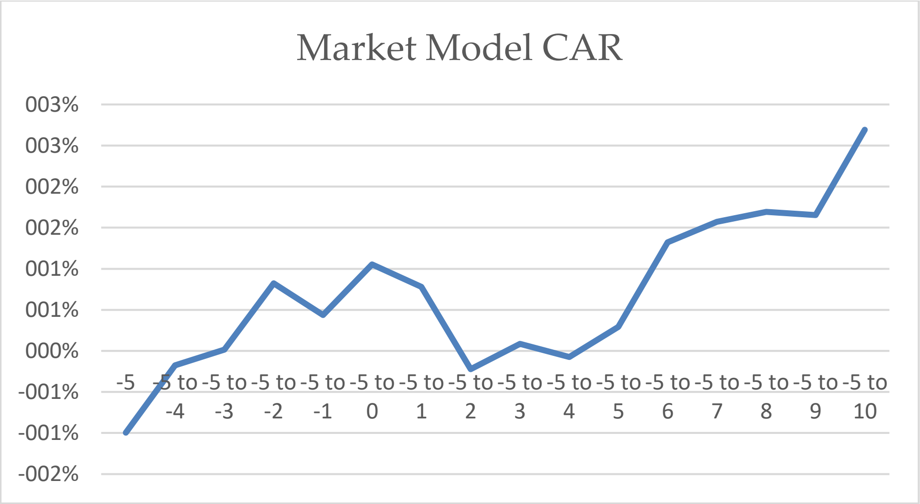


Figure 80: Cumulative abnormal returns by market model for Group 3

Figure 80 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. The decrease in the values started on the announcement date of the event and started to increase again on day +2.

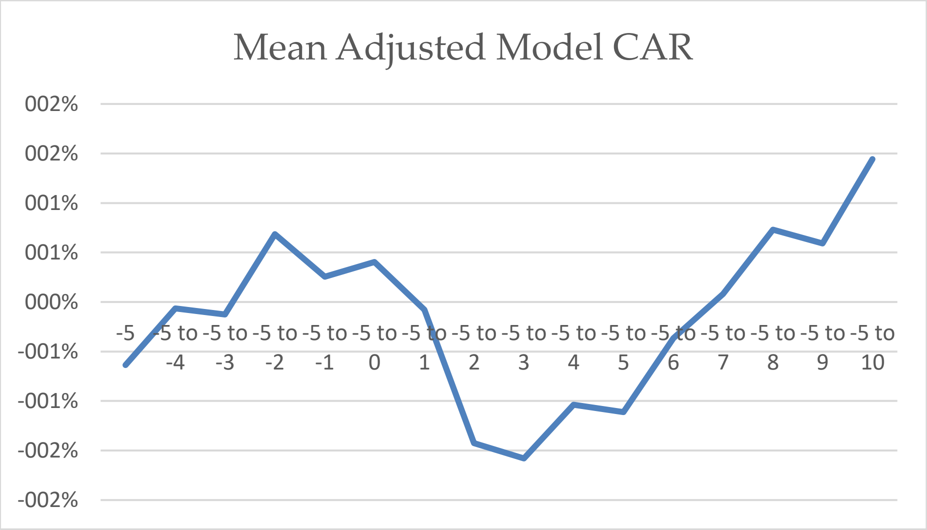


Figure 81: Cumulative abnormal returns by mean adjusted model for Group 3

Figure 81 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The decrease in the values started on day -2, the decrease can be observed as sharper between the days 0 and +3. After that, the values started to increase again; however, the values became positive only after day +7.

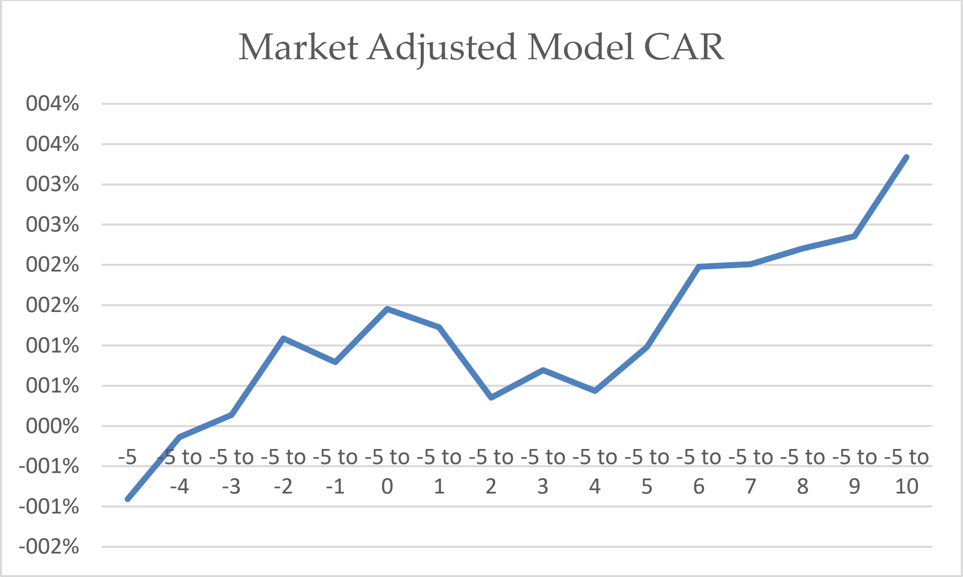


Figure 82: Cumulative abnormal returns by market adjusted model for Group 3

Figure 82 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The decrease in the values started on the announcement date and started to increase again after day +4. Although a decrease can be observed, there were no negative values after the event day on the event window.

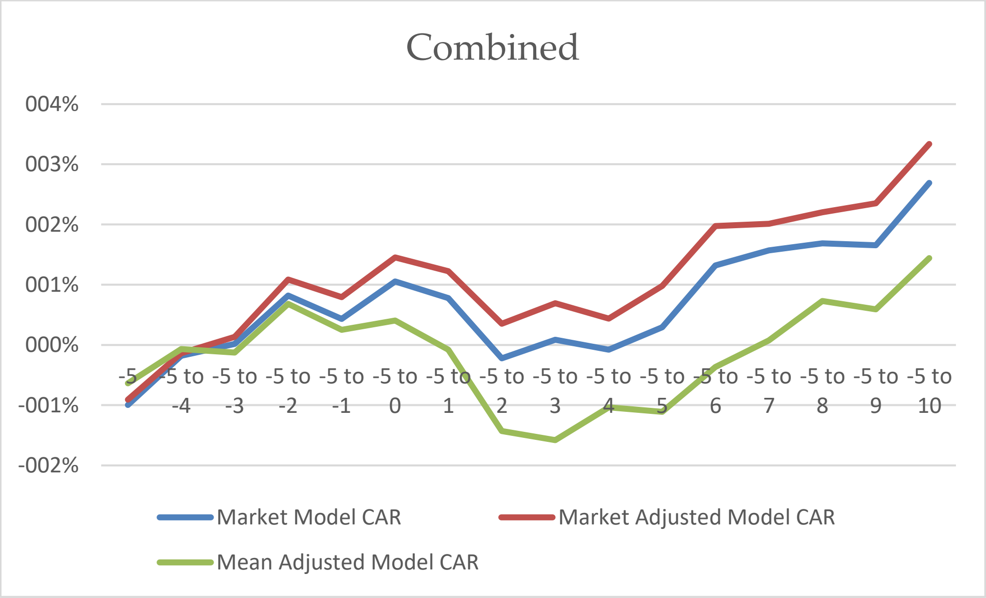


Figure 83: Comparison of the cumulative abnormal returns according to the 3 models used in the study for Group 3

Figure 83 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model, market adjusted model and the mean adjusted model are matching with each other in general. However, the results are slightly different from each other. Especially, the mean adjusted model shows lower results than the other 2 models.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 40: Cumulative Abnormal Returns for Group 3

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-1,00%	-0,91%	-0,64%
-5 to -4	-0,18%	-0,14%	-0,06%
-5 to -3	0,02%	0,14%	-0,13%
-5 to -2	0,82%	1,09%	0,69%
-5 to -1	0,44%	0,79%	0,25%
-5 to 0	1,05%	1,45%	0,40%
-5 to 1	0,78%	1,23%	-0,08%
-5 to 2	-0,22%	0,35%	-1,43%
-5 to 3	0,09%	0,69%	-1,58%
-5 to 4	-0,08%	0,44%	-1,04%
-5 to 5	0,29%	0,98%	-1,11%
-5 to 6	1,32%	1,98%	-0,37%
-5 to 7	1,57%	2,01%	0,08%
-5 to 8	1,69%	2,21%	0,73%
-5 to 9	1,66%	2,36%	0,59%
-5 to 10	2,69%	3,34%	1,44%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 41: t-statistics for Group 3

Day	Market Model CAR t-stat	Market Adjusted Model CAR t-stat	Mean Adjusted Model CAR t-stat
-5	-1,06	-0,84	-0,75
-5 to -4	-0,19	-0,13	-0,08
-5 to -3	0,02	0,13	-0,15
-5 to -2	0,87	1,01	0,81
-5 to -1	0,46	0,74	0,3
-5 to 0	1,12	1,35*	0,48
-5 to 1	0,83	1,14	-0,09
-5 to 2	-0,23	0,33	-1,68**
-5 to 3	0,09	0,65	-1,86**
-5 to 4	-0,08	0,41	-1,22
-5 to 5	0,31	0,91	-1,31*
-5 to 6	1,4*	1,84**	-0,43
-5 to 7	1,67**	1,87**	0,09
-5 to 8	1,79**	2,05***	0,86
-5 to 9	1,76**	2,19***	0,7
-5 to 10	2,86***	3,11***	1,7**

The hypothesis for the effect of information security breaches on different group 3 data size loss:

$H10_0$: IT related failures do not have statistically significant impact on Group 3 data size loss

For the event window [-5,10], the null hypothesis is rejected.

5.1.4.4. GROUP 4

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

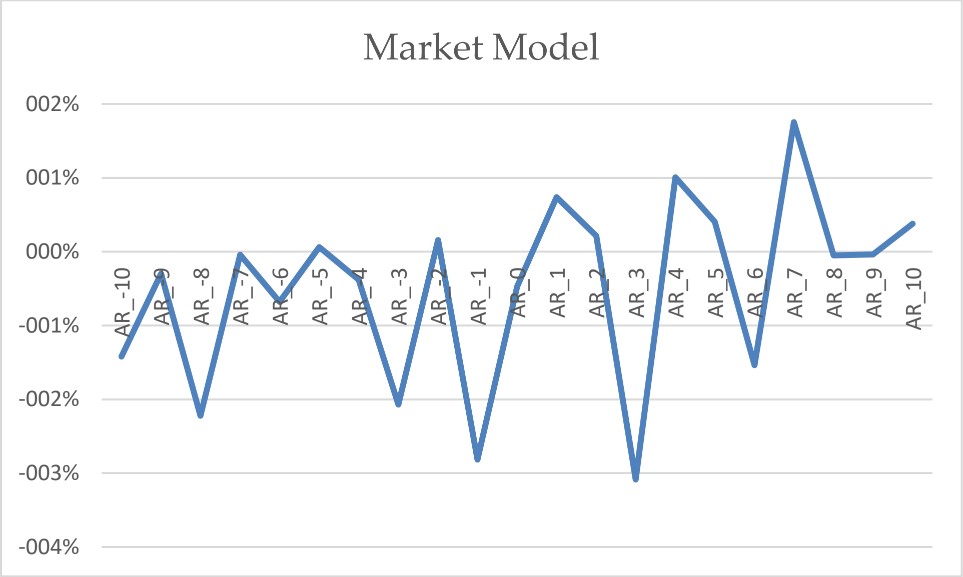


Figure 84: Abnormal returns by market model for Group 4

Figure 84 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. Values have stayed negatively in a three-day period, between days -2 and 0. In addition, there is also a strong decrease on the values between day +1 and day +3. The values have increased again on day +6.

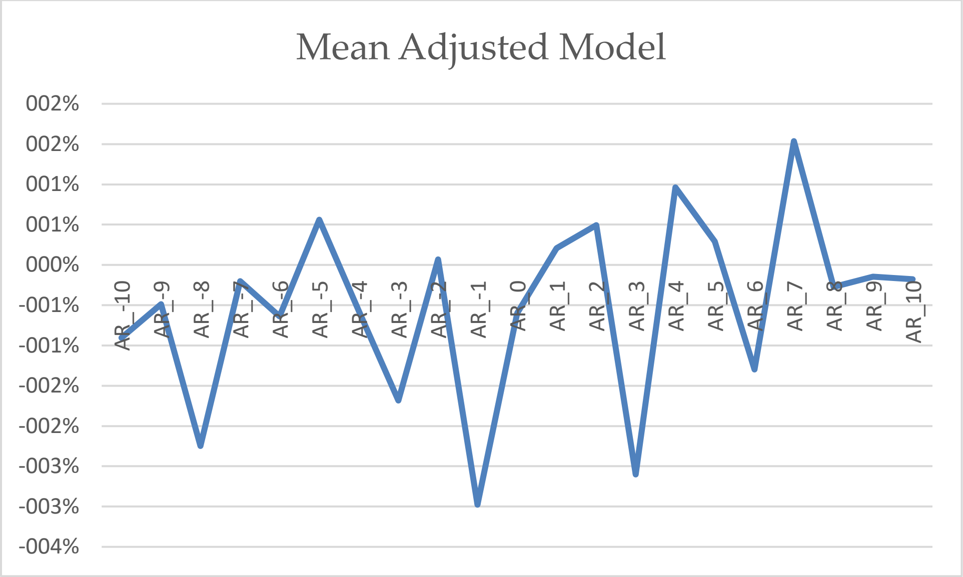


Figure 85: Abnormal returns by mean adjusted model for Group 4

Figure 85 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. Although values have stayed positive for 2 days after the event announcement, there was a sharp decrease on day +2 and there was a decrease on day +4 as well.

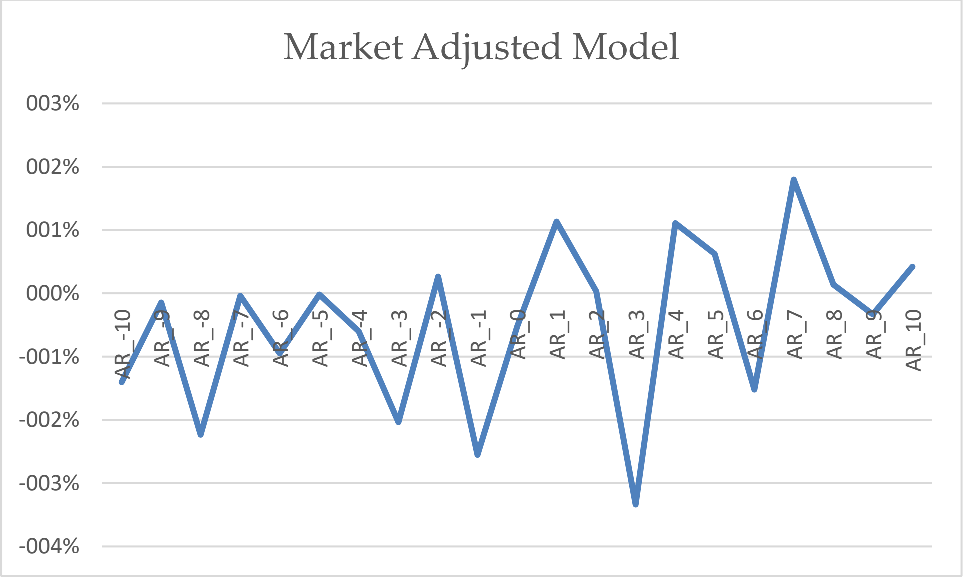


Figure 86: Abnormal returns by market adjusted model for Group 4

Figure 86 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The values are not stable during the t-10 to t+10 window. There was an increase on the values between the days -1 and 1, the values decreased sharply between days +1 and +3.

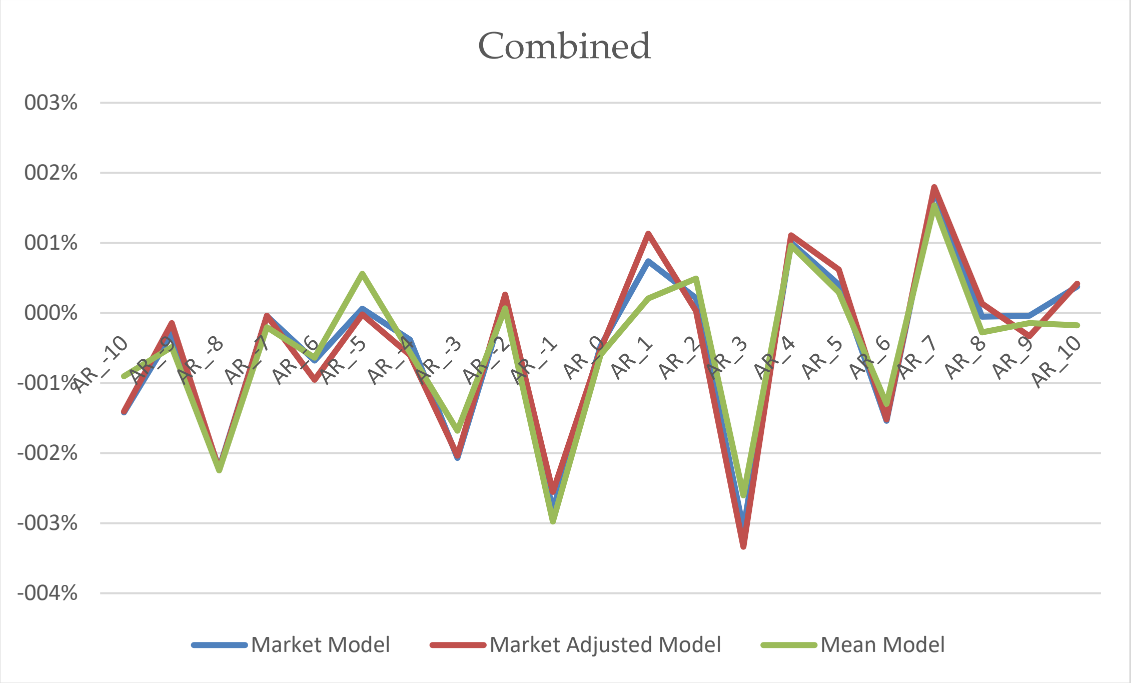


Figure 87: Comparison of the abnormal returns according to the 3 models used in the study for Group 4

Figure 87 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general considering some very slight differences in the results of the mean adjusted model.

Table 42 shows the specific values for the abnormal return on event day for Group 4. There are different and comparable results according to the different models used in the dissertation.

Table 42: Abnormal returns on event day for Group 4

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	-0,47%	-0,53%	-0,60%
Median Abnormal	-0,37%	-0,39%	-0,53%

Return			
Percentage Below Zero	52,94%	52,94%	64,71%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

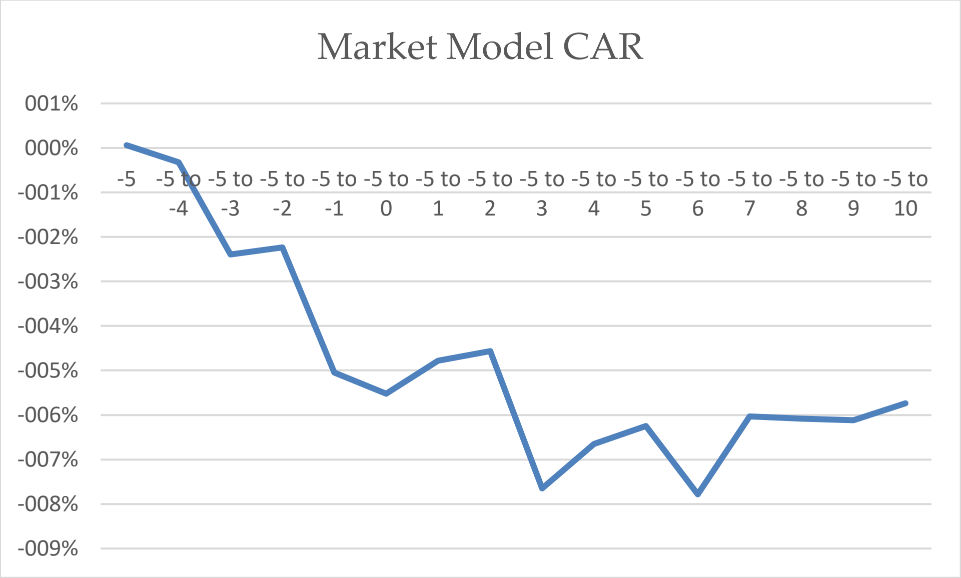


Figure 88: Cumulative abnormal returns by market model for Group 4

Figure 88 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. The decrease in the values started 4 days before the announcement date and showed a stable decrease until day 0. After the announcement date there has only been a small increase until day 2 but the values started to decrease again sharply after day +2.

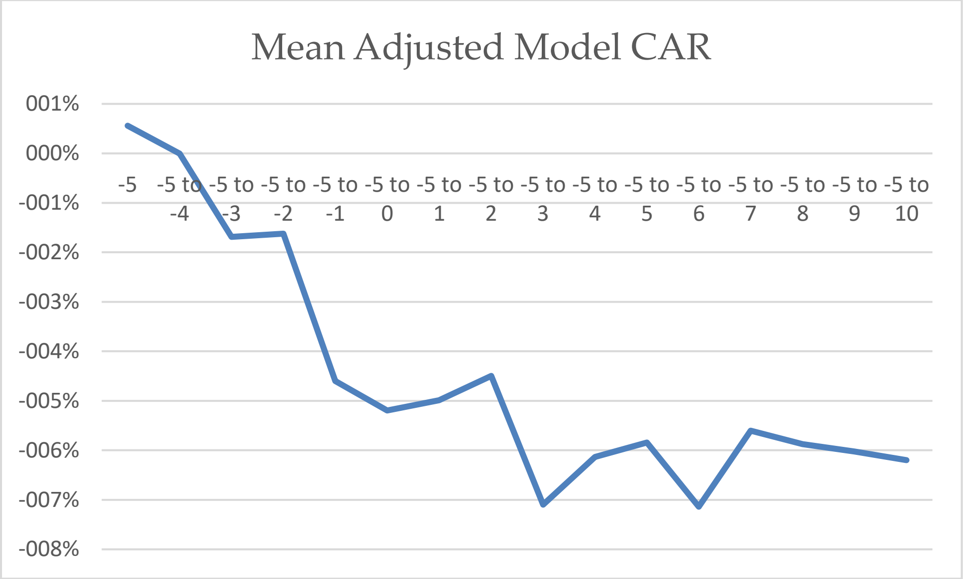


Figure 89: Cumulative abnormal returns by mean adjusted model for Group 4

Figure 89 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The decrease in the values started at day -4 and showed a stable decrease until the announcement date. After the announcement date there has only been a small increase until day 2 but the values started to decrease again sharply after day +2.

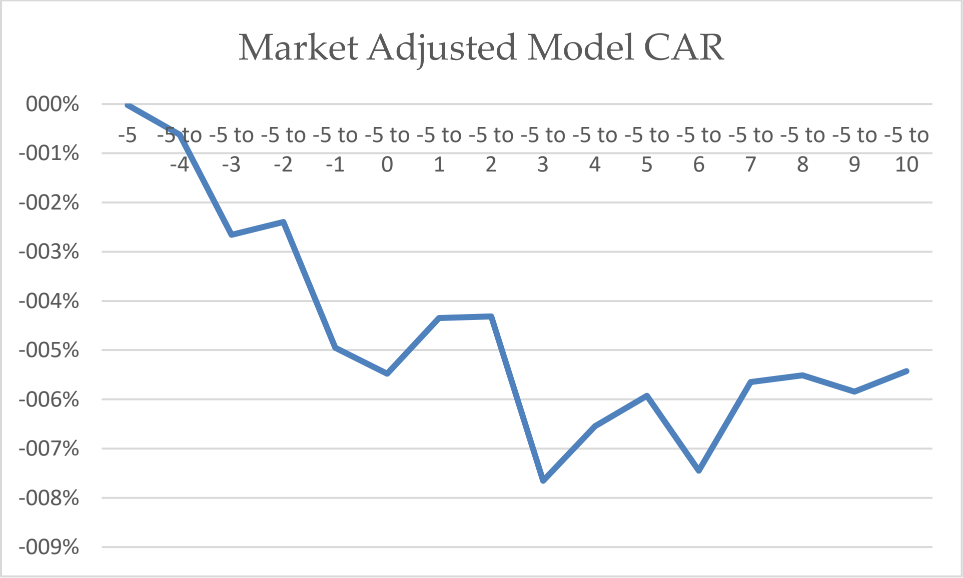


Figure 90: Cumulative abnormal returns by market adjusted model for Group 4

Figure 90 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The decrease in the values started 5 days before the announcement date and showed a decrease until the event announcement. After the stabilization of the values between the days 0 and +1, the decrease continued sharply until day +4.

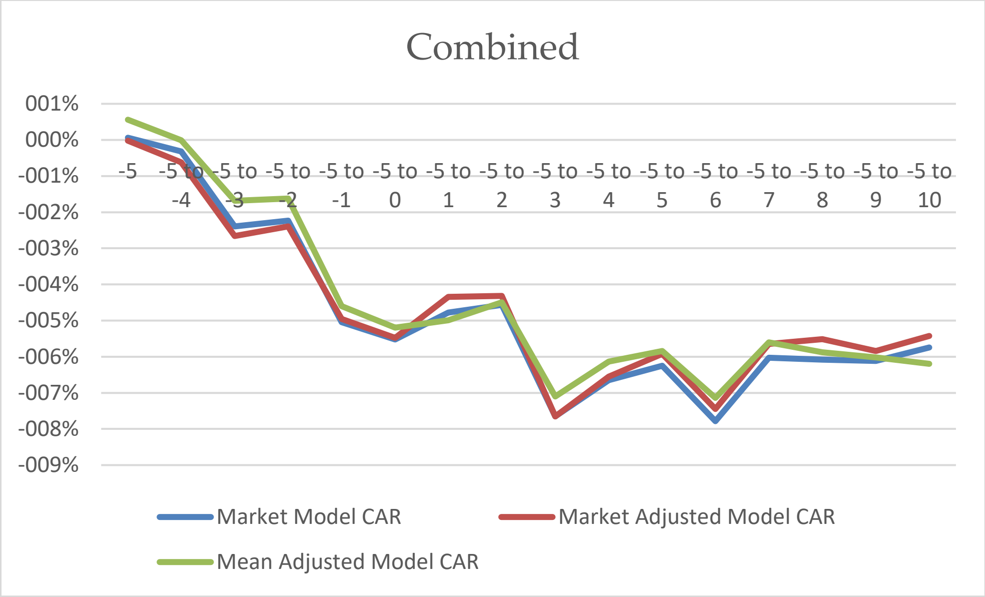


Figure 91: Comparison of the cumulative abnormal returns according to the 3 models used in the study for Group 4

Figure 91 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general other than very slight changes.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 43: Cumulative Abnormal Returns for Group 4

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	0,06%	-0,02%	0,56%
-5 to -4	-0,32%	-0,62%	-0,01%
-5 to -3	-2,39%	-2,66%	-1,69%

-5 to -2	-2,23%	-2,40%	-1,62%
-5 to -1	-5,05%	-4,95%	-4,60%
-5 to 0	-5,52%	-5,48%	-5,19%
-5 to 1	-4,78%	-4,34%	-4,99%
-5 to 2	-4,57%	-4,32%	-4,49%
-5 to 3	-7,65%	-7,65%	-7,10%
-5 to 4	-6,65%	-6,55%	-6,14%
-5 to 5	-6,25%	-5,93%	-5,84%
-5 to 6	-7,78%	-7,45%	-7,14%
-5 to 7	-6,03%	-5,65%	-5,60%
-5 to 8	-6,08%	-5,51%	-5,88%
-5 to 9	-6,12%	-5,84%	-6,02%
-5 to 10	-5,74%	-5,42%	-6,20%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 44: t-statistics for Group 4

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	0,03	-0,01	0,23
-5 to -4	-0,13	-0,28	0
-5 to -3	-1	-1,2	-0,69
-5 to -2	-0,94	-1,08	-0,66
-5 to -1	-2,12***	-2,24***	-1,88**
-5 to 0	-2,32***	-2,47***	-2,13***
-5 to 1	-2,01***	-1,96***	-2,04***
-5 to 2	-1,92**	-1,95**	-1,84**

-5 to 3	-3,21***	-3,46***	-2,91***
-5 to 4	-2,79***	-2,96***	-2,52***
-5 to 5	-2,62***	-2,68***	-2,4***
-5 to 6	-3,27***	-3,36***	-2,93***
-5 to 7	-2,53***	-2,55***	-2,3***
-5 to 8	-2,55***	-2,49***	-2,41***
-5 to 9	-2,57***	-2,64***	-2,47***
-5 to 10	-2,41***	-2,45***	-2,54***

The hypothesis for the effect of information security breaches on different group 4 data size loss:

$H11_0$: IT related failures do not have statistically significant impact on Group 4 data size loss

For the event window [-5,10], the null hypothesis is rejected.

5.1.5. AMONG ALL THE OTHER IT RISKS, IS “HACKING” THE GREATEST RISK FOR BUSINESSES?

5.1.5.1. Results of the companies which are “hacked” by the intruders

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

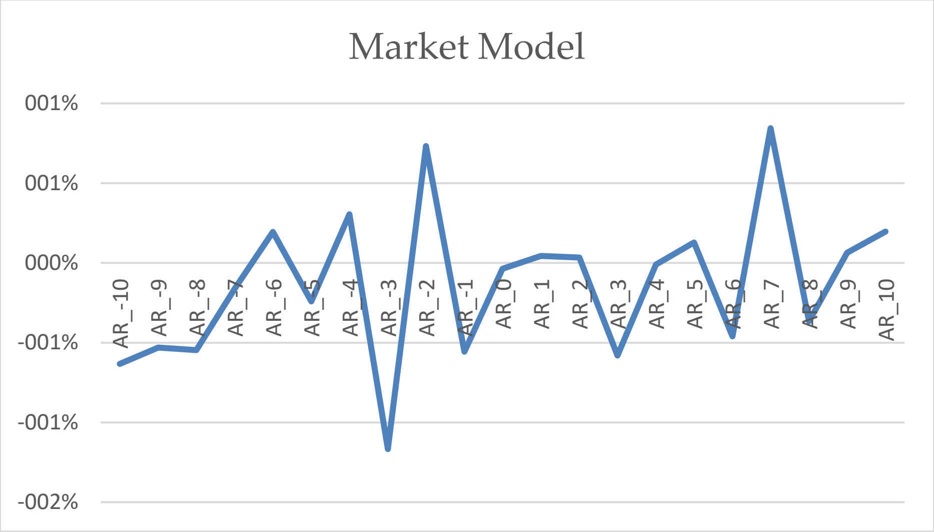


Figure 92: Abnormal returns by market model for "hacked" companies

Figure 92 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased and the abnormal return became positive in day -2. Just before the event announcement day, on day -1, the values are negative and on the event day the values start to increase. A decrease on the values can be seen on day -3.

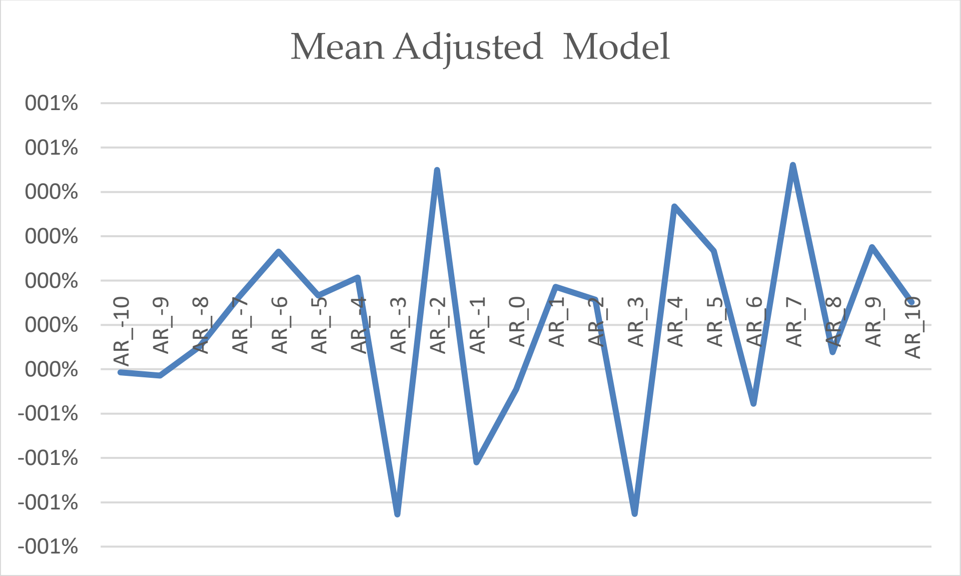


Figure 93: Abnormal returns by mean adjusted model for "hacked" companies

Figure 93 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. The values started to decrease after day -2 and started to increase on day -1 but still negative on the event day. There is also a sharp decrease in the values on day 3.

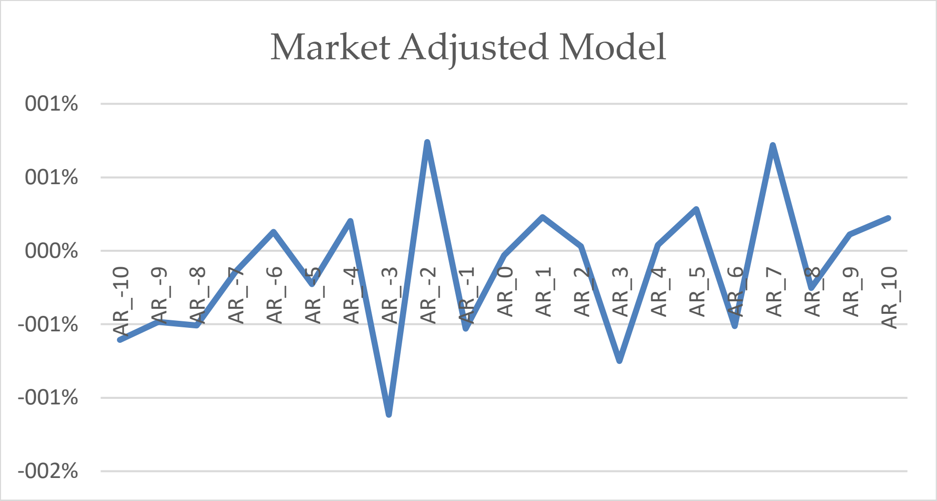


Figure 94: Abnormal returns by market adjusted model for "hacked" companies

Figure 94 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest and in the considered window. After that, the values increased and the abnormal return became positive in day -2 with the largest and most significant value in the event window. After day -2, the values have started to decrease and became negative on day -1. An increase in the values can be observed between the days -1 and 2. The values became negative again on day 3.

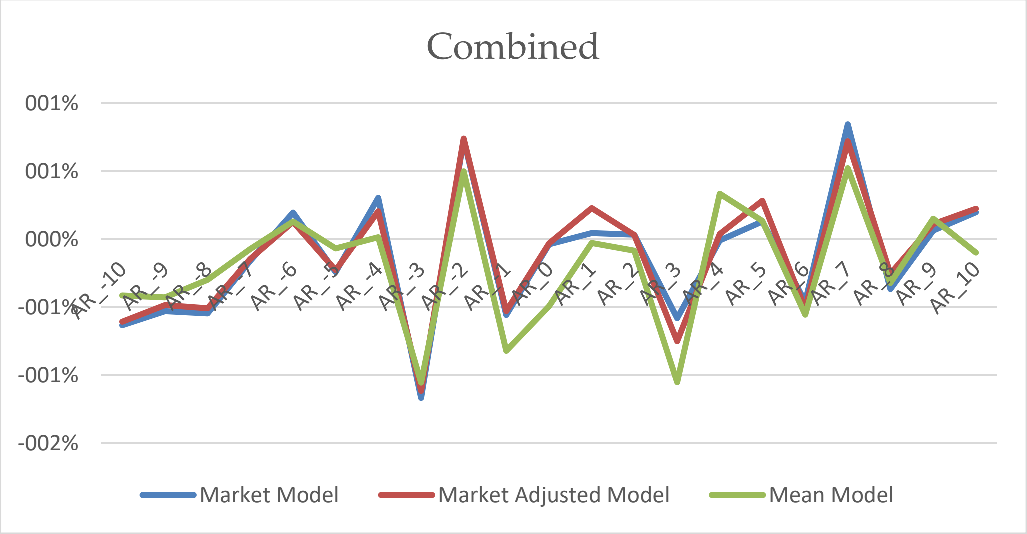


Figure 95: Comparison of the abnormal returns according to the 3 models used in the study for "hacked" companies

Figure 95 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other models on day 0. According to the mean adjusted model the values are lower than the results of the market model and the market adjusted model on the event day. This situation is also valid on day 3.

Table 45 shows the specific values for the abnormal return on event day. The analyses are made specifically for the “hacked” companies. There are different and comparable results according to the different models used in the dissertation.

Table 45: Abnormal returns on event day for “hacked” companies

ARt=0	**Market Model**	**Market Adjusted Model**	**Mean Model**
Mean Abnormal Return	-0,04%	-0,03%	-0,49%
Median Abnormal Return	0,13%	0,18%	-0,25%
Percentage Below Zero	45,57%	43,04%	56,96%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

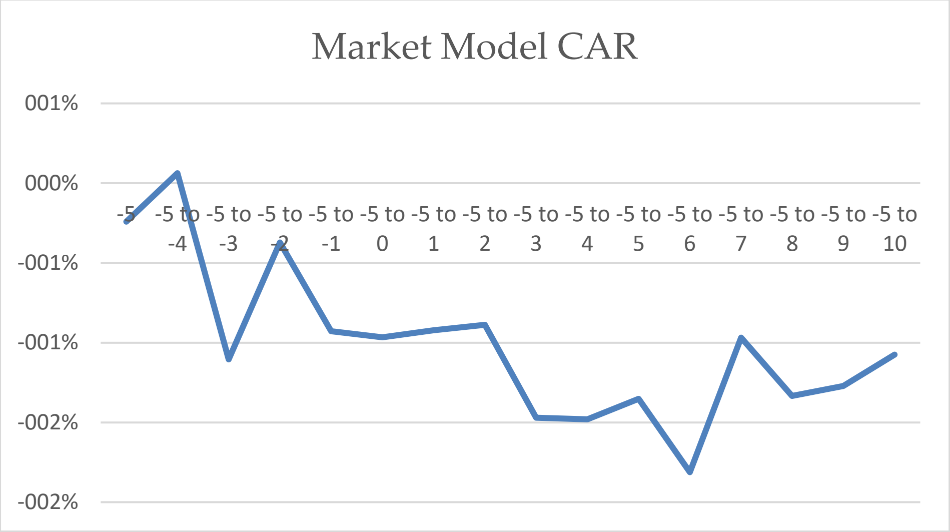


Figure 96: Cumulative abnormal returns by market model for "hacked" companies

Figure 96 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. The values did not show a great movement between the day 0 and day 2. After day 2, the values have started to decrease again.

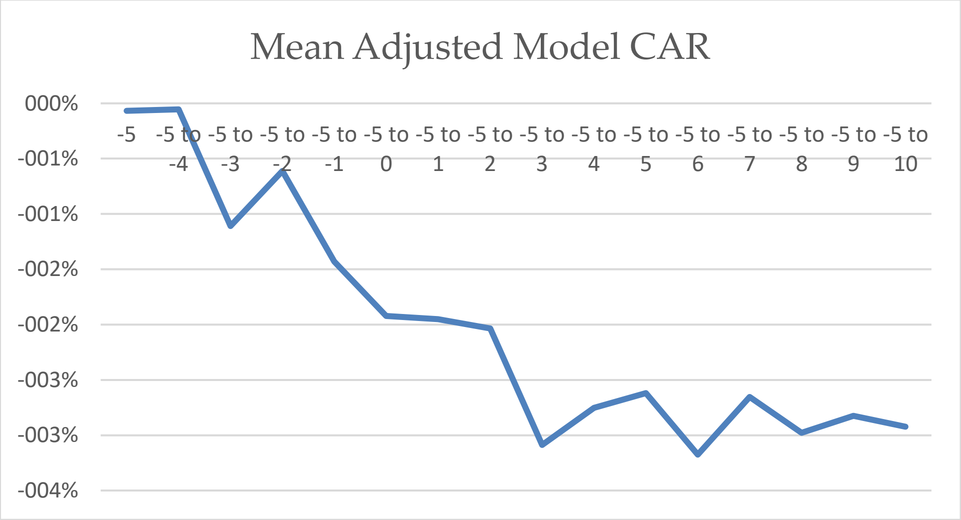


Figure 97: Cumulative abnormal returns by mean adjusted model for "hacked" companies

Figure 97 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to increase on day -2. The decrease in the values continued after the event day.

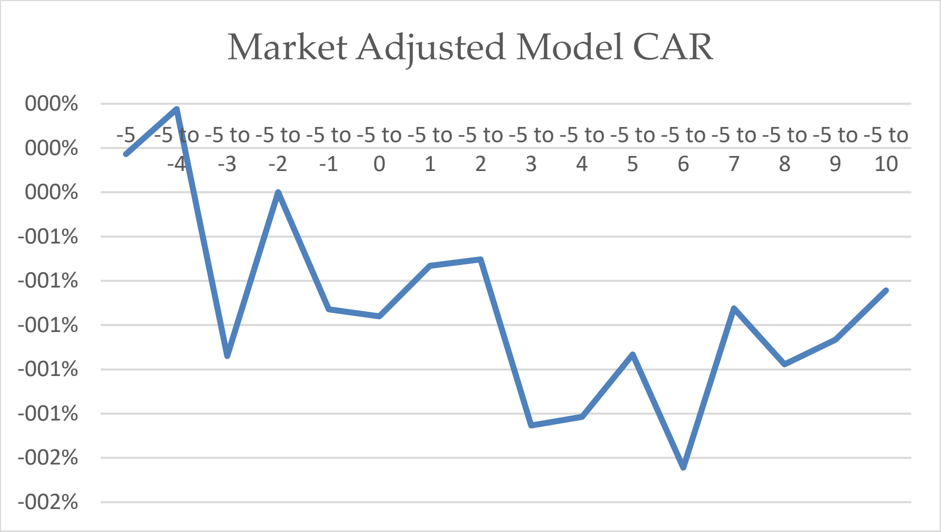


Figure 98: Cumulative abnormal returns by market adjusted model for "hacked" companies

Figure 98 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market adjusted model, starting at day -5. The decrease in the values has started on day -2. After a small increase in the values after the event day the values began to drop on day 2 again.

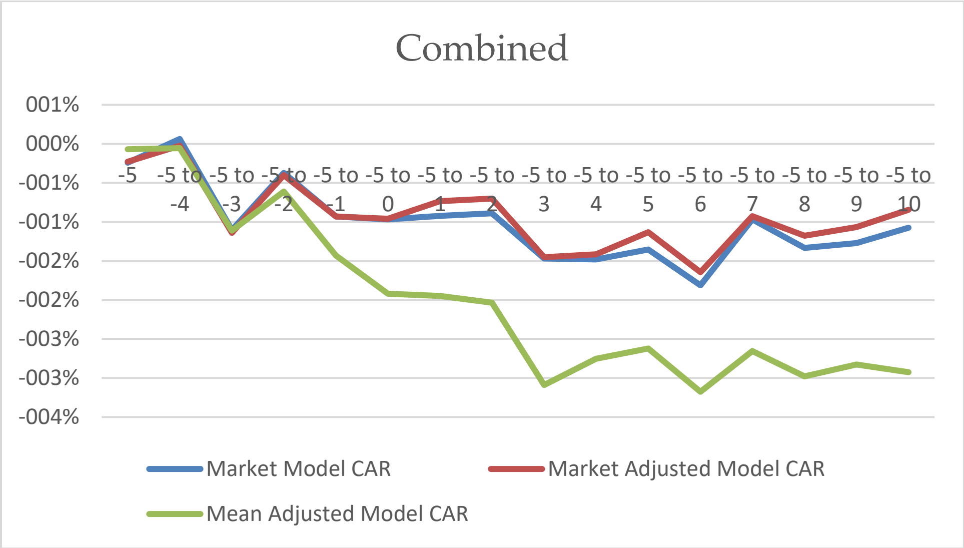


Figure 99: Comparison of the cumulative abnormal returns according to the 3 models used in the study for "hacked" companies

Figure 99 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are matching with each other in general. However, the result of the mean adjusted model is different than the other two models. According to mean adjusted model the decrease in the values are more drastically, which began on day -2.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 46: Cumulative Abnormal Returns for "hacked" companies

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,24%	-0,23%	-0,07%
-5 to -4	0,06%	-0,02%	-0,05%
-5 to -3	-1,10%	-1,14%	-1,11%
-5 to -2	-0,37%	-0,40%	-0,61%
-5 to -1	-0,93%	-0,93%	-1,43%
-5 to 0	-0,97%	-0,96%	-1,92%
-5 to 1	-0,92%	-0,73%	-1,95%
-5 to 2	-0,89%	-0,70%	-2,04%
-5 to 3	-1,47%	-1,45%	-3,09%
-5 to 4	-1,48%	-1,41%	-2,75%
-5 to 5	-1,35%	-1,13%	-2,62%
-5 to 6	-1,81%	-1,64%	-3,18%
-5 to 7	-0,97%	-0,92%	-2,65%
-5 to 8	-1,33%	-1,18%	-2,98%
-5 to 9	-1,27%	-1,07%	-2,83%
-5 to 10	-1,07%	-0,84%	-2,92%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 47: t-statistics for "hacked" companies

Day	Market Model CAR t-stat	Market Adjusted Model CAR t-stat	Mean Adjusted Model CAR t-stat
-5	-0,5	-0,52	-0,06
-5 to -4	0,13	-0,05	-0,05
-5 to -3	-2,27***	-2,6***	-1,04
-5 to -2	-0,76	-0,91	-0,57
-5 to -1	-1,91**	-2,12***	-1,34*
-5 to 0	-1,98***	-2,19***	-1,8**
-5 to 1	-1,89**	-1,67**	-1,83**
-5 to 2	-1,83**	-1,6*	-1,91**
-5 to 3	-3,02***	-3,32***	-2,9***
-5 to 4	-3,04***	-3,23***	-2,59***
-5 to 5	-2,77***	-2,58***	-2,46***
-5 to 6	-3,72***	-3,75***	-2,98***
-5 to 7	-1,99***	-2,11***	-2,49***
-5 to 8	-2,74***	-2,69***	-2,8***
-5 to 9	-2,61***	-2,43***	-2,65***
-5 to 10	-2,21***	-1,93**	-2,75***

The hypothesis for testing the effect of information security breaches caused by hacking:

$H12_0$: Hacking do not have statistically significant impact on the publicly listed firms.

For the event window [-5,10], the null hypothesis is rejected.

5.1.5.2. Results for the companies which are exposed to the "other" kinds of malicious activities

ABNORMAL RETURNS

Results of the abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

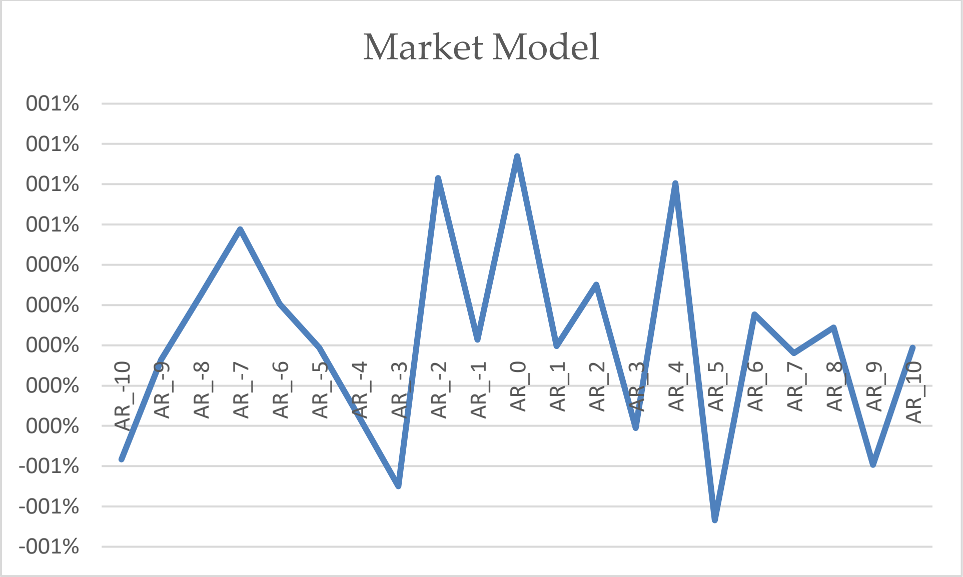


Figure 100: Abnormal returns by market model for the firms exposed to the "other" kinds of malicious activities

Figure 100 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 are the largest in the considered window. After that, the values increased sharply and the abnormal return became positive in day -2. On day -2 the values start to decrease again. There is an increase on the values on day -1 and there is decrease again after day 0.

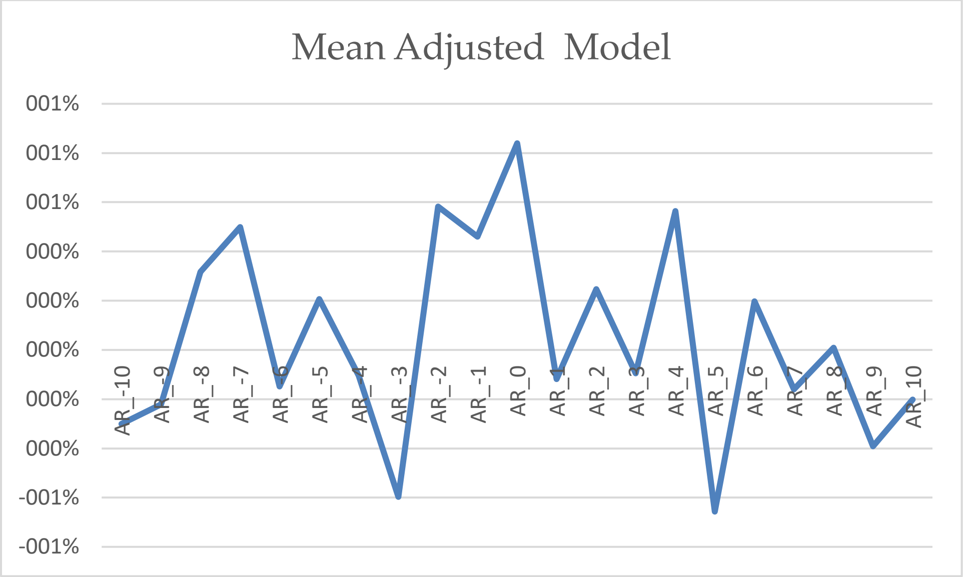


Figure 101: Abnormal returns by mean adjusted model for the firms exposed to the "other" kinds of malicious activities

Figure 101 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). There are large negative values on day -3 and they started to increase sharply after that day. After the announcement date of the event the values have started to decrease and became negative. There is also a sharp decrease in the values on day 5.

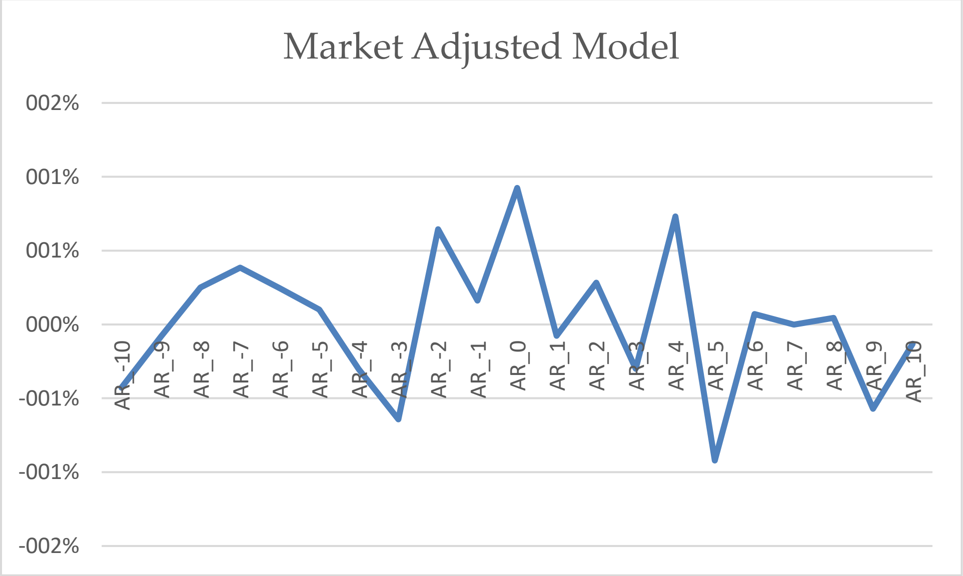


Figure 102: Abnormal returns by market adjusted model for the firms exposed to the "other" kinds of malicious activities

Figure 102 summarizes the abnormal result values over the t-10 to t+10 window (AR_0 represents the event day). The negative values on day -3 started to increase and remained positive until day 0. The values started to decrease after the event day but the largest values can be observed on day 5.

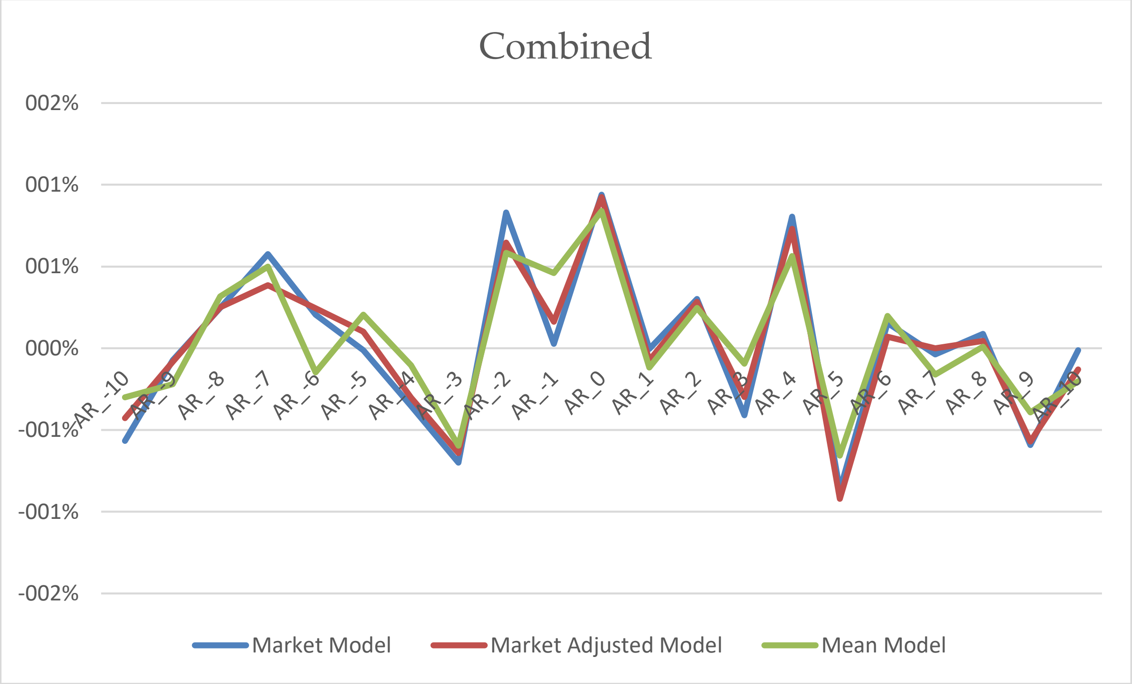


Figure 103: Comparison of the abnormal returns according to the 3 models used in the study for the firms exposed to the "other" kinds of malicious activities

Figure 103 presents the comparison of the results of the three models used in the dissertation. The results are matching with each other in general. However, there can be observed a slight difference between the mean adjusted model and the other models on day -1. According to the mean adjusted model the values are higher than the results of the market model and the market adjusted model on the day before the event day.

Table 48 shows the specific values for the abnormal return on event day. The analyses are made specifically for the firms exposed to the "other" kind of malicious activities. There are different and comparable results according to the different models used in the dissertation.

Table 48: Abnormal returns on event day for the firms exposed to the "other" kind of malicious activities

ARt=0	Market Model	Market Adjusted Model	Mean Model
Mean Abnormal Return	0,94%	0,92%	0,84%
Median Abnormal Return	0,27%	0,20%	0,29%
Percentage Below Zero	42,22%	42,22%	44,44%

CUMULATIVE ABNORMAL RETURNS

Results of the cumulative abnormal returns for the market model, mean adjusted model and the market adjusted model are below. The comparison of the results according to each model can be seen in the last graphic.

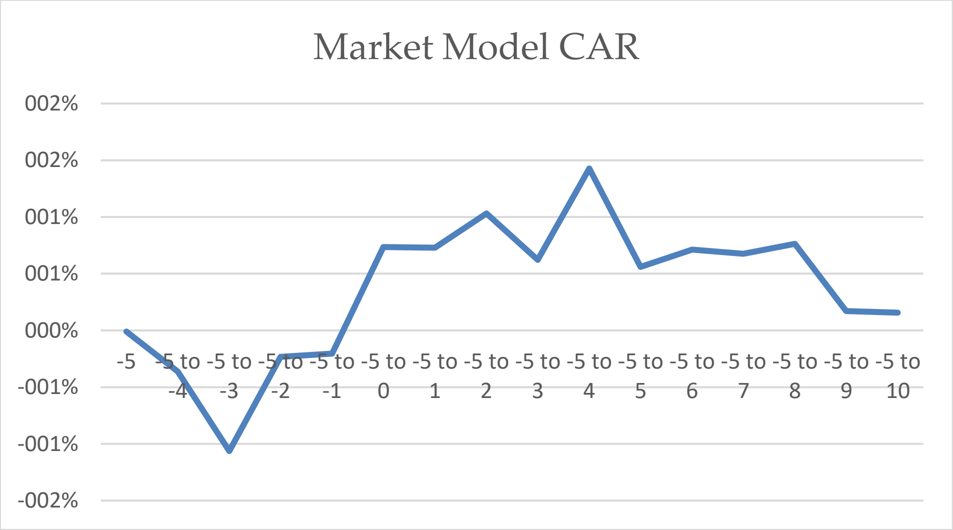


Figure 104: Cumulative abnormal returns by market model for the firms exposed to the "other" kinds of malicious activities

Figure 104 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the market model, starting at day -5. The increase in the values can be observed from the beginning of day -3. Even after the event day, the values have started to increase again.

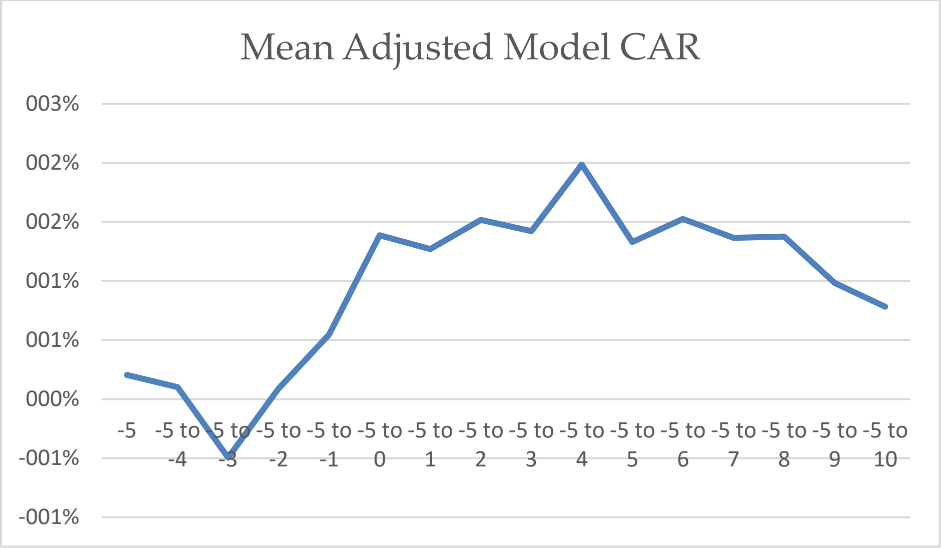


Figure 105: Cumulative abnormal returns by mean adjusted model for the firms exposed to the "other" kinds of malicious activities

Figure 105 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to increase on day -3. After the event day not so much movement is observed on the values for 3 days and after day 3 the values have started to increase again. The decrease states began on day 6.

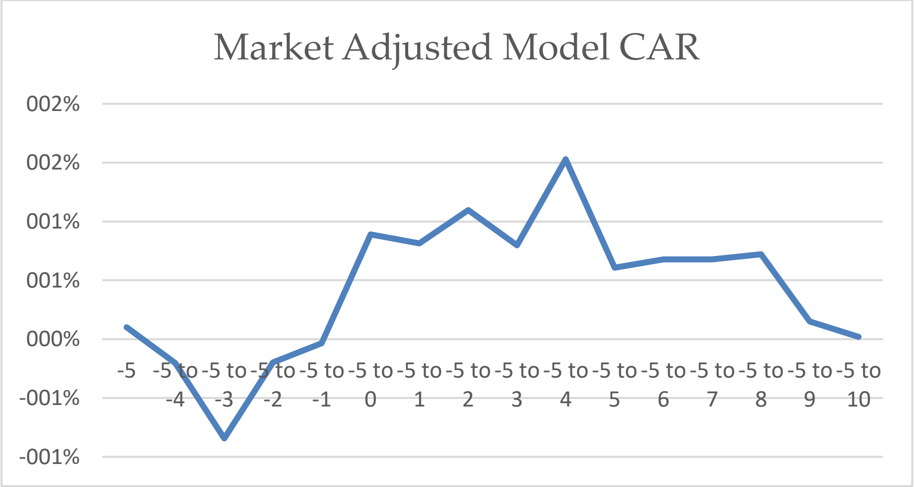


Figure 106: Cumulative abnormal returns by market adjusted model for the firms exposed to the "other" kinds of malicious activities

Figure 106 presents the actual cumulative results (accumulated difference between the returns of the breached companies and the projected market returns) according to the mean adjusted model, starting at day -5. The values have started to increase on day -3. There has been a small drop in the values on day 0, however increase in the values could be observed until day 4. After day 4, the values have decreased again drastically.

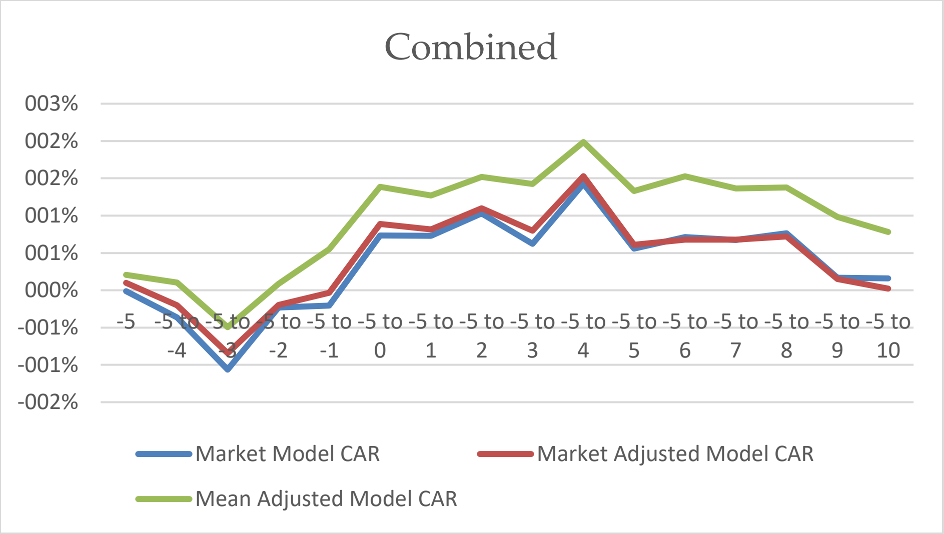


Figure 107: Comparison of the cumulative abnormal returns according to the 3 models used in the study for the firms exposed to the "other" kinds of malicious activities

Figure 107 presents the comparison of the results of the three models used in the dissertation. The results coming from the market model and market adjusted model are matching with each other in general. However, the result of the mean adjusted model is different than the other two models. The values according to mean adjusted model are higher than the market model and the market adjusted model.

The accumulated returns from day -5 to day +10 can be seen as follows:

Table 49: Cumulative Abnormal Returns for to the “other” kinds of malicious activities

Day	**Market Model CAR**	**Market Adjusted Model CAR**	**Mean Adjusted Model CAR**
-5	-0,01%	0,10%	0,21%
-5 to -4	-0,36%	-0,20%	0,10%
-5 to -3	-1,06%	-0,84%	-0,49%
-5 to -2	-0,23%	-0,20%	0,09%
-5 to -1	-0,21%	-0,03%	0,55%
-5 to 0	0,73%	0,89%	1,39%
-5 to 1	0,73%	0,81%	1,27%
-5 to 2	1,03%	1,10%	1,52%
-5 to 3	0,62%	0,80%	1,42%
-5 to 4	1,43%	1,53%	1,99%
-5 to 5	0,56%	0,61%	1,33%
-5 to 6	0,71%	0,68%	1,53%
-5 to 7	0,67%	0,68%	1,37%
-5 to 8	0,76%	0,72%	1,38%
-5 to 9	0,17%	0,15%	0,98%
-5 to 10	0,16%	0,02%	0,78%

t-statistics for the confidence intervals 90% (1,282), 95% (1,645), 99% (1,96) can be seen as follows. (*, ** and *** denotes the significance levels 10%, 5% and 1% respectively.)

Table 50: t-statistics for the “other” kinds of malicious activities

Day	**Market Model CAR t-stat**	**Market Adjusted Model CAR t-stat**	**Mean Adjusted Model CAR t-stat**
-5	-0,02	0,17	0,3

-5 to -4	-0,58	-0,34	0,15
-5 to -3	-1,71**	-1,41*	-0,72
-5 to -2	-0,37	-0,33	0,13
-5 to -1	-0,33	-0,06	0,8
-5 to 0	1,18	1,49*	2,03***
-5 to 1	1,17	1,36*	1,85**
-5 to 2	1,66**	1,83**	2,22***
-5 to 3	1	1,33*	2,08***
-5 to 4	2,3***	2,56***	2,9***
-5 to 5	0,9	1,02	1,94**
-5 to 6	1,15	1,13	2,23***
-5 to 7	1,09	1,13	1,99***
-5 to 8	1,23	1,21	2,01***
-5 to 9	0,27	0,25	1,44*
-5 to 10	0,25	0,04	1,14

The hypothesis for testing the effect of information security breaches caused by other types of breaches:

H13$_0$: Other kinds of IT related risks do not have statistically significant impact on the publicly listed firms.

For the event window [-5,4], the null hypothesis is rejected.

The statistically significant impact could be seen in a shorter period of time than "hacking".

5.2. DISCUSSION OF RESULTS

5.2.1. HAVE THE LISTED FIRMS BEEN AFFECTED FROM IT RELATED FAILURE?

All the three models show a similar pattern by looking at the abnormal returns. The action in values rotates down just 3 days before an event. After that, the values go in the opposite rotation, i.e. they are going up. The change in the values after the event is not striking. The change before the event implies that there is a tip in the market which led the decrease in the values before 3 days of the event. However, when the market does not see a failure right away, the information is taught as a misleading and the values went up again. The information comes before the event, however it is not public information, it is insider information.

The results of the Cumulative Abnormal Returns are similar to the Abnormal Returns results. By looking at Figure 11 it could be suggested that the model that is used is important for a better analysis of the study. The impact of the security breaches is clearer according to the mean adjusted model, so it is vital to use different models while analyzing the impact.

All the results show that the security breaches have impact on the market by causing volatility. By means of prices there are no continuous changes, because the results are rather horizontal after the event.

5.2.2. WHAT ARE THE EFFECTS OF IT RELATED FAILURES ON MANUFACTURING AND SERVICE FIRMS SEPARATELY?

The discussion of the research question involves two separate analyses: one analysis for the sample of manufacturing firms and one analysis for the service providing firms.

Abnormal returns for the manufacturing companies show us there is not an unordinary price change until the day of event. In fact, the values are positive until the day of the event. In spite of the positivity until day 0, the return on the event day is almost 0. This situation could be evaluated as the confusion in the mindset of the investors. This assumption could be supported by the transition from increasing trend to the steady trend after the event day. The results of the cumulative abnormal returns support the abnormal return results. There is no considerable price change before the event day. That brings us to the conclusion that manufacturing firms are more eligible and successful in the reservation of information.

Here, the overall results are contradictory with the results of the overall sample which brings us to the analysis for the service sector.

By looking at the results of the service sector analysis, the prices are falling before 3 days of the event. However, the values are going stronger at day -2 which could be originated from the lack of any official announcement regarding to any failures. The stable fall begins from the day 0. After the investors received the official announcement the there is a negative influence on the stock prices. The beginning of the decrease before official announcement implies that the investors had the opportunity to receive the information before the event and act according to that.

The separation of the results between the service sector and the manufacturing sector shows the vitality of clustering the overall sample. Overall sample may bring accurate results however, when the sample is divided into subsamples the results are more insightful and open to discussion.

5.2.3. WHICH SECTOR IS AFFECTED THE MOST FROM THE IT RELATED FAILURES?

For a more concentrated analysis, this study handled the main 4 sectors that are contained by the overall sample.

5.2.3.1. Consumer Goods

There could be seen a confusion at the event day which leads to mispricing, the values are increade from day -1 to the announcement day. The downward action in the values after the event announcement day shows that the markets are reflecting the impacts of the announcement for consumer goods sector.

5.2.3.2. Financials

By looking at the results of the financial sector analysis, the prices are falling before 3 days of the event. However, the values are going stronger at day -2 which could be originated from the lack of any official announcement regarding to any failures. The stable fall begins from the day 1. After the investors received the official announcement and a short confusion at the event day, the negative influence on the stock prices begins.

It is expected to the results of the financials sector results are similar to the service sector results because financials sector constitutes a big portion of the service firms sample.

It seems as the investors have the opportunity to receive the information before the event and act according to that. However, once again it could be seen that that insider information creates a confusion and mispricing in the prices. The actual fall begins after the announcement day.

5.2.3.3. Technology

The fall in the prices is more vivid in the technology sector. The IT failure is clearer due to the sector, there is no misleading in prices and the results are not exaggerated. The fall in the prices is coherent with the ongoing trend. The downward action began before to days of the event and the prices falls again after the announcement. After 5 days of the event prices began to show an upward action which could be originated from the precautions of the firms (i.e. calling back the faulty devices).

5.2.3.4. Communications

The communications sector results are more surprising and the action is going unlike the expectation. The expectation is a fall in the prices, however, the communication sector is not affected from the IT related failure.

The situation implies that there is an ongoing trust to communications sector. The IT failures are in the second place in the investors' minds.

5.2.4. DOES THE LOST RECORD SIZE HAVE EFFECT ON THE FAILURE IMPACT?

Major data breaches create major effects on the firms' market value. As it is stated before, the sample has been divided into 4 groups according to the lost record size.

Group 1 has encountered with no effect (the group lost the least record size).

Group 2 and has encountered with a short term effect especially between the days -1 and -3.

Group 3 and has also encountered with a short term effect especially between the days 0 and -3.

Group 4 has encountered with the greatest impact of the security incidents which starts nearly 5 days before the announcement date; the values decreased sharply, and proceeded negatively until day +10 where our event window ends.

Due to the reason that Group 2, 3 and 4 has seen the effects of the cyber breaches before the announcement, it is safe to state that market value is affected according to the lost record size. The presence of the insider information could be predicted for group 4, because the values started to decrease before the actul event announcement, i.e. the values have started to decrease nearly on day -5.

5.2.5. AMONG ALL THE OTHER IT RISKS, IS "HACKING" THE GREATEST RISK FOR BUSINESSES?

It is safe to assume the presence of insider information in the "hacking" type of security breaches. The information comes 3 days prior the event, and this situation could also be observed in the second research question's "service" sector part.

After the announcement of the event, the prices continue to fall. However, mostly because of the insider information, the prices originally started to fall before the event.

In contrast, with the other kinds of IT related risks, no fall in values before the event day could be observed. In fact, there is not a fall even after the event day. This brings us into conclusion that the risks as "accidental publish of data", "lost/ stolen computer", "lost/ stolen media", and "poor security" don't affect the investors' decisions and the prices are not affected.

So, as an answer, yes, the greatest IT related risk for the companies is "hacking."

CHAPTER 6: IMPLICATIONS

In this dissertation, it is focused on the impact of the security related risk events on firms' market value.

Due to the findings there is an interesting question that arises: *"What should do firms about the negative movements in their stock prices?"* Although stock prices of the publicly listed firms increase or decrease over the time, the event study methodology discovers a specific impact created by the occurrence of an event. How to handle this effect carefully is an interesting question for the managers of those firms. As Warren Buffett once said "Predicting storms doesn't count; building arks does." It is in the hands of the managers of a firm to build preventive measures to a cyber breach. To protect market value of a firm, maintain stability and eliminating the changes of value decrease in stocks, managers should handle the security risks proactively.

The results of this dissertation also provide evidence to managers to justify their investments on security, i.e. establishing new department, hiring workforce, reaching an agreement with the security service providers.

According to the results, there are interesting implications as follows:

6.1. SECTOR AND EVENT SPECIFIC IMPLICATIONS

First and foremost, the results gave strong evidence to show the importance of sub sampling in an event study. After the sub-sampling according to firms' sector, security breach type and lost data size, the results are becoming more complicated. It is found that all types of information security breach events don't create same economic impact on every firm.

That is why here it can be found some specific implications.

There is no reason to believe that information security breach events create a similar effect on all of the publicly listed firms. There has been evidence of sometimes the announcements about the information security breaches causes negative market reaction and sometimes there is not.

Manufacturing vs. Service Firms

According to the results, manufacturing firms are not affected from the IT related failures although service firms are affected from those kinds of failures remarkably. This effect is not seen properly when the analysis is made upon the whole sample. This implicates also the importance of subsampling while studying Event Study Methodology.

Manufacturing sector is more concentric with technology and service sector is more involved with people. This situation may imply to the capabilities of manufacturing sector of managing the IT related failures more properly. Due to the human influence in the service companies, they are defenseless to the human perception more. The manufacturing firms may have the more "trustable" perception of the stakeholders and service firms, in contrary, may have the perception of "inexpertness" by the stakeholders and this will create an effect on the market value negatively for the service sector.

In conclusion, service firms should be prepared to the IT related failures as well-supported and announce their capabilities in technology to their stakeholders via media outlets, web-sites or their social media accounts in a way that creates the most positive perception on stakeholders.

Sector based implications

As we mentioned before, subsampling is very crucial while studying event study methodology. Although it seems like manufacturing firms do not get affected from the IT related failures on the contrary of service firms, it is thought that it will be better to analyze the situation with further subsampling.

The events were also analyzed by the sector, so there are implications that could be made at the sectoral basis. The findings signify that market reactions differ on the sectoral type and some sectors are affected more than the others. It was found that the most impacted industries are technology and financials. Thus, it seems that the participants of the stock market are making discriminations while assessing the information security breach impacts.

The biggest 4 sectors are analyzed for examining the effect of cyber security related failures on a firm basis. The subsamples are selected as consumer goods (manufacturing), technology (manufacturing), financials (service), and communications (service) sectors because they are the most effected sectors in the sample. The results are consistent with the real world perceptions and logic.

Communication

It is an interesting result that there is no negative effect of cyber security breaches on communication sector. The most reasonable explanation is that the communication sector has managed the announcement and post-announcement days very successfully due to the nature of the sector. The communication sector knows how to communicate with its stakeholders properly and this capability serves well in this kind of situation.

However, this is not a guarantee for future events, so all the recommendations about the security are also valid for the communication sector. If those companies would not protect themselves, they may face to a situation where they should spend much more money than the preventive costs just like the other firms in different sectors.

Consumer goods

Consumer goods sector has been affected from the cyber breaches in a minimal way. It has been observed a slight downward action in stock prices, shortly after the announcement the prices went to their levels before the cyber breach announcement.

It is obvious that stakeholders are not punishing the consumer goods sector firms as severely as the technology and financial firms. One reason for that could be after the consumers have bought their goods they do not follow the news about that firm necessarily. However, it is not the case for financials and technology firms. Those two types of firms should gain their stakeholders' trust consistently and the expectations from them are much higher.

Although consumer goods sector is not affected from the breaches severely, surely, they have to take all the security measures. If the managers of those firms get the idea that "We would not get affected from those cyber security breaches in a financial way" that would be a mistake. The upper management should not think the costs of the IT failures as an operational cost. IT security should be maintained all the time because it can never be known what a new security breach will done to your firm and your stock prices.

Technology

Especially, technology related firms should carry out the security related activities more carefully because shareholders' expectations from them are higher than non-technology firms. The technology firms should protect their information and digital resources better according to the general perception.

The high impact on the technology sector might be due to the high expectations of people in general that companies from IT sector should have better expertise on technology and they should be capable of preventing any kind of digital attacks. Therefore, if they are targeted by any kind of security threats, the investors' perception about their capability and the trust to their reputation will decrease. That is why investors seem to penalize the technology companies more severely.

Financials

In addition to the technology sector, the financials sector also affected from IT related failure severely. Investors are more sensitive to impact of data security breaches in the financial services sector, where the most sensitive data of customers are stored. Due to its nature, the financial services sector would face with the higher risk exposure and consequently high probable losses. That is why financials sector should be taken the necessary preventive measures security breaches, be prepared to any kind of exposure and stay vigilant all the time.

It is also pointed in the results that the reaction of the stock market changes according to the economic sector of the listed firms. This situation states that some firms should be equipped and prepared with the security control systems more than the others. These control systems will monitor the exposure to cyber risk and that will lead to a decrease in the financial and reputational losses.

Hacking vs. Others

It is also found that (as an answer to the 5th research question) "hacking" is the greatest risk among all the other vulnerabilities that a firm can face to. Consequently, understanding the actual impact of hacking on the stock market returns is critical to decide the investments that are going to take place in information security activities.

The most important threat to firms is "hacking". Confidentiality related vulnerabilities (as hacking) cause more negative effect. So, if the company has faced to less sophisticated problems as "stolen laptop" case didn't have any effect on the firm value, so it is safe to assume that being vulnerable to malicious activities are more important to solve rather than fraudulent activities. One possible reason such vulnerability has the larger potential is they may cause more customer losses for a firm.

Some types of failures as "accidentally published data, lost/stolen computer, lost/stolen media, poor security, inside job" seem as they have no material impact on the firm's economic performance.

Breached data size effect

Breached data size effect does not have major effects on the firms' market value unless the lost record size is massive. If the lost record size is immense, firms get affected from the situation in enormous amounts. Despite of the results, it is recommended that security measures should be taken against for all attacks even the potential breach is small or big. One small attack can create vulnerability in the system and cause bigger consequences, so, the preventive measures should be important despite of the magnitude of the potential attacks.

6.2. CULTURE OF GOVERNANCE

The management should be aware of the risks from top down and company should act against these security risks as a unified whole. Opportunities and situations should not be seen as value creation chances and associated risk costs separately. Leadership should always be ready to the chance of occurrence these risks by creating awareness throughout the firm.

If the managers show efforts to reduce or eliminate the security related breaches, consumer confidence to those firms will increase. The most important thing that organizations should show their commitment to digital security of the business systems and this can lead to an enhancement in their business activities and stock performances. Today, there is an increased awareness for the information technology issues among public and they can interpret the endeavors of those organizations and this situation can create an increase on the market value for the firms, whether their systems are breached or not.

There is another implication for managers. Adopting new IT systems will create vulnerability to exposers and new types of errors. So, new system or equipment should be evaluated carefully before integrating them into the operations of a firm.

In addition, employees and their supervisors should be trained in a way that they can handle those probable errors by following clear and effective procedures. Furthermore, employees can resist to change and they can be tense about using the new system or equipment. They should be assured that they would not be blamed for any new errors, instead it is the new system or the equipment the firm will focus on.

6.3. SYSTEMATIC RISK MITIGATION EFFORTS

All efforts for eliminating the risks should be systematic and should be carried out under the appropriate corporate governance framework. If a firm makes some efforts in pieces or just after a security attack, these attempts will be received untrustworthy by the stakeholders.

The usefulness of event studies originated from the fact that the scale of the abnormal returns created by an event provides a measure for the impact of firms' shareholders. This kind of assessment provides an understanding to corporate policy decisions. That kind of information could be a roadmap for the affected firms and a way for managers to act effectively.

CEO (Chief Executive Officer), CIO (Chief Information Officer), CISO (Chief Information Security Officer), and CRO (Chief Risk Officer) from the top management team should be the responsible for carrying out the cyber security activities. Security breach events should be reviewed in the annual meetings along with the other key important issues. The necessary measures and paths should be decided and updated regularly. These measures and paths should include both preventive and corrective actions if necessary.

A different department or at least a security manager can be assigned to perform the digital security activities. If security managers would implement the security policies effectively and control the security of the organizations, vulnerabilities could be minimized. In addition to manager assignment, specific employees should also be assigned to tasks and firms should have clear definitions about the responsibilities on the protection of security.

6.4. NOT SEEING INFORMATION SECURITY AS AN UNNECESSARY COST

Cost of assuring the information security can create an ironic situation. If a company makes a thorough investment in cyber-security, this may result no security breaches over the time and this will lead to a false perception that company is over investing over the security initiatives. Due to the valuable side of information security is hard to proof while there are no security breach events that a firm encounters, top management of the firm should not forget the unseen benefits of security investments.

There is likely a good chance of security challenges will continue to threaten the firms. For the prevention from the negative impacts of the ICT risks, firms need to declare an open privacy and security policy and inform both their employees and shareholders about the rules related to the sensitive security threats. Providing the necessary level of security could be costly, however, security assurance is important for the market value, thus survival, of the firms.

There exists a link between the cyber risks and the firm value. Whether or not the effect of the security breaches is long term, the study provides an insight that shareholders pay attention to the news and announcements about the firm they have invested. This statement brings us to the conclusion that security of a firm definitely is worth investing and customers pay attention to the security of the firm along with the product features.

The results of this dissertation should be encouraging for the firms to invest in information technology security and a reassurance which have doubts about the value of adopting security practices. Spending resources on information security is an investment rather than expenditure like it is seen by most of the firms. Firms need to invest to IT security strategically to satisfy the expectations of their stakeholders. Firms need to allocate their resources to maximize organizational performance and following the results of this dissertation can help them throughout this effort. Security breach events have the potential to cause economic losses to firms and decrease the firm value through the loss of reputation.

6.5. TAKING PRECAUTIONS

So, it is safe to assume that having a vulnerable product can lead to a negative impact for a firm. Due to the bad press associated with this kind of vulnerability/ security breach effect, managers need to pay attention to the press and not giving them a chance by strengthening the firm's digital security. A secure product/service can generate a positive value for the firm. For giving the customers a qualified product/service the security measures should be fully taken.

Firms even may benefit by taking necessary security related precautions. By being upfront to stakeholders' about the new security strategies of the firm, shareholders' trust to the firm will increase and this create a positive reputation. Even the firm has been through a huge breach in the past, hearing the new security measures can decrease the negative sentiments directed to that firm.

For being aware of the vulnerabilities, first the firms should identify them. Employees should also be encouraged for reporting any kind of error that can create a security threat.

6.6. CONCLUSION

A comprehensive analysis of the economic impact of a company's cyber security incidents on its market value is presented in this dissertation. Cyber security incident events are accumulated through a variety of resources for the 2000-2015 period. The event study shows the impact varies on the firms according to their sectoral levels, lost records sizes, or breach types. It is also important whether a company is operating under manufacturing or service settings. The results are also supported by the t-statistics.

The results of this dissertation could be used by both academicians and practitioners. Managers could use the implications as a road map to run their companies more efficiently in case of cyber security treaths. Academicians could also conduct further research and examine the economic impacts on firms on different levels as it is conducted in this research by subsampling. In addition, other type of impacts could also be investigated as the reputation of a company.

Due to the data set in this dissertation does not include non-profit organizations and the analysis is applicable only to publicly listed companies, future studies could be employed on the impacts of security breaches on those kind of organizations.

In conclusion, there is always value in avoiding security breaches in a company.

APPENDIX I

ORGANIZATION	YEAR	Organization Type	METHOD OF LEAK	NO OF RECORDS STOLEN
Australian Immigration Department	2015	Government	Accidentally Published	500000
British Airways	2015	Retail	Hacked	500000
Slack	2015	Tech	Poor Security	500000
Premera	2015	Healthcare	Hacked	11000000
Uber	2015	Tech	Poor Security	50000
Mozilla	2014	Tech	Poor Security	760000
New York Taxis	2014	Transportation	Poor Security	52000
MacRumours.com	2014	Tech	Hacked	860000
LexisNexis	2014	Tech	Hacked	1000000
Korea Credit Bureau	2014	Financial	Inside Job	20000000
Neiman Marcus	2014	Retail	Hacked	1100100
European Central Bank	2014	Financial	Hacked	4000000
NASDAQ	2014	Financial	Hacked	500000
Advocate Medical Group	2013	Healthcare	Lost / Stolen Media	4.000.000
SnapChat	2013	Tech	Hacked	4700000
South Africa police	2013	Government	Hacked	16000
Florida Department of Juvenile Justice	2013	Government	Lost / Stolen Computer	100000
Central Hudson Gas & Electric	2013	Energy	Hacked	110000
Kirkwood Community College	2013	Academic	Hacked	125000
Washington State court system	2013	Government	Hacked	160000
TerraCom & YourTel	2013	Telecommunications	Accidentally Published	170000
Scribd	2013	Tech	Hacked	500000
Drupal	2013	Tech	Hacked	1000000
Kroll Background America	2013	Tech	Hacked	1000000
Kissinger Cables	2013	Government	Inside Job	1700000
Ubuntu	2013	Tech	Hacked	2000000
Evernote	2013	Tech	Hacked	50000000
Living Social	2013	Tech	Hacked	50000000
OVH	2013	Tech	Hacked	500000
Militarysingles.com	2012	Tech	Accidentally Published	163792
Emory Healthcare	2012	Healthcare	Poor Security	315000
Formspring	2012	Tech	Accidentally Published	420000
Medicaid	2012	Government	Hacked	780000
California Department of Child Support Services	2012	Government	Lost / Stolen Media	800000
New York State Electric & Gas	2012	Energy	Inside Job	1800000
Three Iranian banks	2012	Financial	Hacked	3000000
South Carolina Government	2012	Healthcare	Inside Job	228.435
Office of the Texas Attorney General	2012	Government	Accidentally Published	6500000
Gamigo	2012	Tech	Hacked	8000000
Greek government	2012	Government	Hacked	9000000
Dropbox	2012	Tech	Hacked	30.000
US Army	2011	Military	Accidentally Published	50000
Writerspace.com	2011	Tech	Hacked	62000
University of Wisconsin - Milwaukee	2011	Academic	Hacked	73.000

Memorial Healthcare System	2011	Healthcare	Lost / Stolen Media	102153
US Law Enforcement	2011	Government	Accidentally Published	123461
Accendo Insurance Co.	2011	Healthcare	Poor Security	175350
San Francisco Public Utilities Commission	2011	Government	Hacked	180000
Bethesda Game Studios	2011	Tech	Hacked	200000
Restaurant Depot	2011	Retail	Hacked	200000
Massachusetts Executive Office of Labor and Workforce	2011	Government	Poor Security	210000
Southern California Medical-Legal Consultants	2011	Healthcare	Hacked	300000
Spartanburg Regional Healthcare System	2011	Healthcare	Lost / Stolen Computer	400000
Eisenhower Medical Center	2011	Healthcare	Lost / Stolen Computer	514330
Stratfor	2011	Military	Accidentally Published	935000
Oregon Department of Motor Vehicles	2011	Government	Poor Security	1000000
Nemours Foundation	2011	Healthcare	Lost / Stolen Media	1055489
State of Texas	2011	Government	Accidentally Published	3500000
Sutter Medical Foundation	2011	Healthcare	Lost / Stolen Computer	4243434
Tricare	2011	Healthcare	Lost / Stolen Computer	4901432
China Software Developer Network	2011	Tech	Hacked	6000000
NHS	2011	Healthcare	Lost / Stolen Media	8300000
178.com	2011	Tech	Hacked	10000000
Tianya	2011	Tech	Hacked	28000000
Steam	2011	Tech	Hacked	35000000
Yale University	2010	Academic	Accidentally Published	43000
Colorado government (Department of Health Care Policy & Financing)	2010	Healthcare	Lost / Stolen Computer	105470
Lincoln Medical & Mental Health Center	2010	Healthcare	Lost / Stolen Media	130495
Ankle & foot Center of Tampa Bay, Inc.	2010	Healthcare	Hacked	156000
Emergency Healthcare Physicians, Ltd.	2010	Healthcare	Lost / Stolen Media	180111
Seacoast Radiology, PA	2010	Healthcare	Hacked	231400
Embassy Cables	2010	Government	Inside Job	251000
US Military	2010	Military	Inside Job	260000
Classified Iraq War documents	2010	Government	Inside Job	392000
US Federal Reserve Bank of Cleveland	2010	Financial	Hacked	400000
Puerto Rico Department of Health	2010	Healthcare	Hacked	515000
Ohio State University	2010	Academic	Hacked	760000
South Shore Hospital, Massachusetts	2010	Healthcare	Lost / Stolen Media	800000
Gawker.com	2010	Tech	Hacked	1500000
New York City Health & Hospitals Corp.	2010	Healthcare	Lost / Stolen Media	1700000
Educational Credit Management Corp	2010	Financial	Lost / Stolen Media	3300000
US Dept of Defense	2009	Military	Lost / Stolen Media	72000
US National Guard	2009	Military	Lost / Stolen Computer	131000

University of California Berkeley	2009	Academic	Hacked	160000
Affinity Health Plan, Inc.	2009	Healthcare	Lost / Stolen Media	344579
Virginia Prescription Monitoring Program	2009	Healthcare	Hacked	531400
Network Solutions	2009	Tech	Hacked	573000
Blue Cross Blue Shield of Tennessee	2009	Healthcare	Lost / Stolen Media	1023209
AvMed, Inc.	2009	Healthcare	Lost / Stolen Computer	1220000
Virginia Dept. Of Health	2009	Government	Hacked	8257378
RockYou!	2009	Tech	Hacked	32000000
US Military	2009	Military	Lost / Stolen Media	76000000
Service Personnel and Veterans Agency (UK)	2008	Government	Lost / Stolen Media	50000
Stanford University	2008	Academic	Lost / Stolen Computer	72000
UK Home Office	2008	Government	Lost / Stolen Media	84000
Jefferson County	2008	Government	Accidentally Published	1600000
UK Ministry of Defence	2008	Government	Lost / Stolen Media	1700000
University of Miami	2008	Academic	Lost / Stolen Computer	2100000
University of Utah Hospitals & Clinics	2008	Academic	Lost / Stolen Media	2200000
Norwegian Tax Authorities	2008	Government	Accidentally Published	3950000
Data Processors International	2008	Financial	Hacked	5000000
Chile Ministry Of Education	2008	Government	Accidentally Published	6000000
Auction.co.kr	2008	Tech	Hacked	18000000
Texas Lottery	2007	Government	Inside Job	89000
City and Hackney Teaching Primary Care Trust	2007	Government	Lost / Stolen Media	160.000
Compass Bank	2007	Financial	Inside Job	1000000
Driving Standards Agency	2007	Government	Lost / Stolen Media	3.000.000
Hannaford Brothers Supermarket Chain	2007	Retail	Hacked	4200000
UK Revenue & Customs	2007	Government	Lost / Stolen Media	25000000
TK / TJ Maxx	2007	Retail	Hacked	94000000
Cardsystems Solutions Inc.	2005	Financial	Hacked	40000000

APPENDIX II

	Name of the Organization	**Ticker (Bloomberg)**	**Ticker (Reuters)**	**Industry**	**Sector**	**Manufacturing/ Service**
1	**Twitch**	AMZN:US	AMZN.O	Retail - Discretionary	Consumer Goods	S
2	**Anthem Inc**	ANTM:US	ANTM.K	Health Care Facilities & Svcs	Healthcare	S
3	**Sony Corp**	6758:JP	6758.T	Hardware	Technology	M
4	**JPMorgan Chase & Co**	JPM:US	JPM	Banking	Financials	S
5	**Google**	GOOGL:US/ GOOG:US	GOOGL.O	Media	Communications	S
6	**Home Depot Inc**	HD:US	HD	Retail - Discretionary	Consumer Goods	S
7	**Community Health Systems Inc**	CYH:US	CYH	Health Care Facilities & Svcs	Healthcare	S
8	**Domino's Pizza Group PLC**	DOM:LN	DOM:L	Gaming, Lodging & Restaurants	Consumer Goods	M
9	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
10	**eBay Inc**	EBAY:US	EBAY.O	Retail - Discretionary	Consumer Goods	S
11	**United Parcel Service Inc**	UPS:US	UPS	Transportation & Logistics	Industrials	S

12	**Walgreens Boots Alliance Inc**	WBA:US	WBA.O	Retail - Consumer Staples	Consumer Goods	S
13	**Citigroup Inc**	C:US	C	Banking	Financials	S
14	**Nintendo Co Ltd**	7974:JP	7974.T	Hardware	Technology	M
15	**Twitter Inc**	TWTR:US	TWTR.K	Media	Communications	S
16	**Apple Inc**	AAPL:US	AAPL.O	Hardware	Technology	M
17	**Dun & Bradstreet Corp.**	DNB:US	DNB	Technology Services	Technology	S
18	**Vodafone Group PLC**	VOD:LN	VOD.L	Telecom	Communications	S
19	**Facebook Inc.**	FB:US	FB.O	Media	Communications	S
20	**Target Corp.**	TGT:US	TGT	Retail - Consumer Staples	Consumer Goods	S

21	**Yahoo Japan Corp.**	4689:JP	4689.T	Media	Communications	S
22	**Ubisoft Entertainment SA**	UBI:FP	UBIP.PA	Software	Technology	S
23	**Adobe Systems Inc.**	ADBE:US	ADBE.O	Software	Technology	S
24	**Massive American business hack**					
	7-Eleven, JC Penney, Hannaford, Heartland, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard					
25	**7-Eleven Malaysia Holdings Bhd**	SEM:MK	SEM	Retail - Consumer Staples	Consumer Goods	S
26	**JC Penney Co Inc**	JCP:US	JCP	Retail - Discretionary	Consumer Goods	S
27	**Heartland Financial USA Inc**	HPY:US	HPY.V	Banking	Financials	S
28	**JetBlue Airways Corp**	JBLU:US	JBLU.O	Passenger Transportation	Consumer Goods	S
29	**Euronet Worldwide Inc**	EEFT:US	EEFT.O	Specialty Finance	Financials	S
30	**Global Payments Inc**	GPN:US	GPN	Specialty Finance	Financials	S

31	**Yahoo! Inc**	YHOO:US	YHOO.O	Media	Communications	S
32	**Global Payments Inc**	GPN:US	GPN	Specialty Finance	Financials	S
	LinkedIn, eHarmony, Last.fm					
33	**LinkedIn Corp**	LNKD:US	LNKD.K	Media	Communications	S
34	**KT Corp.**	030200:KS	030200.KS	Telecom	Communications	S
35	**Zappos**	AMZN:US	AMZN.O	Retail - Discretionary	Consumer Goods	S
36	**Apple Inc**	AAPL:US	AAPL.O	Hardware	Technology	M
37	**Activision Blizzard Inc**	ATVI:US	ATVI.O	Software	Technology	S
38	**Morgan Stanley**	MS:US	MS	Institutional Financial Svcs	Financials	S

39	**Morgan Stanley**	MS:US	MS	Institutional Financial Svcs	Financials	S
40	**Honda Motor Co Ltd**	7267:JP	7267.T	Automotive	Consumer Goods	M
41	**Citigroup Inc**	C:US	C	Banking	Financials	S
42	**Sony Corp**	6758:JP	6758.T	Hardware	Technology	M
43	**Washington Post**	GHC:US	GHC	Consumer Services	Consumer Goods	S
44	**Nintendo Co Ltd**	7974:JP	7974.T	Hardware	Technology	M
45	**Ubisoft Entertainment SA**	UBI:FP	UBIP.PA	Software	Technology	S
46	**Sega Sammy Holdings Inc**	6460:JP	6460.T	Gaming, Lodging & Restaurants	Consumer Goods	M
47	**Electronic Arts Inc.**	EA:US	EA.O	Software	Technology	S
48	**Countrywide Financial Corp**	BAC:US	BAC	Banking	Financials	S
49	**Nexon Co Ltd**	3659:JP	3659.T	Software	Technology	S
50	**Sony Corp**	6758:JP	6758.T	Hardware	Technology	M

51	**Sony Corp**	6758:JP	6758.T	Hardware	Technology	M
	Health Net - IBM					
52	**International Business Machines Corp (IBM)**	IBM:US	IBM	Technology Services	Technology	M
53	**Health Net**	HNT:US	…	Health Care Facilities & Svcs	Healthcare	S
54	**AT&T Inc**	T:US	T	Telecom	Communications	S
55	**Triple-S Management Corp**	GTS:US	GTS	Health Care Facilities & Svcs	healthcare	S
56	**Betfair**	BET:LN	BET.MI	Gaming, Lodging & Restaurants	Consumer Goods	S
57	**JPMorgan Chase & Co**	JPM:US	HNT^C16	Banking	Financials	S
58	**Health Net**	HNT:US	…	Health Care Facilities & Svcs	Healthcare	S
59	**CheckFree Corporation**	FISV:US	FISV.O	Specialty Finance	Financials	S
60	**Heartland Financial USA Inc**	HPY:US	HPY.V	Banking	Financials	S

61	**Starbucks Corp**	SBUX:US	SBUX.O	Gaming, Lodging & Restaurants	Consumer Goods	M
62	**AT&T Inc**	T:US	T	Telecom	Communications	S
63	**Worldpay Group PLC**	WPG:LN	WPG	Specialty Finance	Financials	S
64	**GS Caltex**	CVX:US	CVX	Oil, Gas & Coal	Energy	S
65	**Bank of New York Mellon Corp**	BK:US	BK	Institutional Financial Svcs	Financials	S
66	**Gap Inc**	GPS:US	GPS	Retail - Discretionary	Consumer Goods	S
67	**Automatic Data Processing Inc**	ADP:US	ADP.O	Technology Services	Technology	S
68	**TJX Cos Inc**	TJX:US	TJX	Retail - Discretionary	Consumer Goods	S
69	**Charles Schwab Corp**	SCHW:US	SCHW.K	Asset Management	Financials	S
70	**Merrill Lynch**	MER.PK:US	BAC	Institutional Financial	Financials	S

	Investment Solutions			Svcs		
71	**eBay Inc**	EBAY:US	EBAY.O	Retail - Discretionary	Consumer Goods	S
72	Monster Worldwide Inc	MWW:US	MWW	Media	Communications	S
73	**Ameritrade Holding Corp**	AMTD:US	AMTD.O	Asset Management	Financials	S
74	**Fidelity National Information Services Inc**	FIS:US	FIS	Specialty Finance	Financials	S
75	**Dai Nippon Printing Co Ltd**	7912:JP	7912.T	Commercial Services	Consumer Goods	S
76	**H&R Block Inc**	HRB:US	HRB	Commercial Services	Consumer Goods	S
77	**FedEx Corp**	FDX:US	FDX	Transportation & Logistics	Industrials	S
78	**OfficeMax Inc.**	OMX:US acquired by ODP:US	ODP.O	Retail - Discretionary	Consumer Goods	S
79	**Honeywell International Inc**	HON:US	HON	Electrical Equipment	Industrials	M
80	**Mastercard Inc**	MA:US	MA	Specialty Finance	Financials	S

81	**Medco Health Solutions Inc.**	MHS:US acquired by ESRX:US	…	Health Care Facilities & Svcs	healthcare	S
82	**Verizon Communications Inc.**	VZ:US	VZ	Telecom	Communications	S
83	**General Motors Co**	GM:US	GM	Automotive	Consumer Goods	M
84	**Boeing Co**	BA:US, BOEI34:BZ, BA*:MM	BA	Aerospace & Defense	Industrials	M
85	**Aetna Inc**	AET:US	AET	Health Care Facilities & Svcs	healthcare	S
86	**Wells Fargo & Co**	WFC:US	WFC	Banking	Financials	S
87	**M&T Bank Corp**	MTB:US	MTB	Banking	Financials	S
88	**Hewlett Packard Enterprise Co**	HPE:US	HPE	Technology Services	Technology	M
89	**Countrywide Financial Corp**	BAC:US	BAC	Banking	Financials	S

90	**KDDI Corp**	9433:JP	9433.T	Telecom	Communications	S
91	**Circuit City Stores Inc.**	CCTYQ:US	…	Retail - Discretionary	Consumer Goods	S
92	**AT&T Inc**	T:US	T	Telecom	Communications	S
93	**E*TRADE Financial Corp**	ETFC:US	ETFC.O	Asset Management	Financials	S
94	**Ameritrade Holding Corp**	AMTD:US	AMTD.O	Asset Management	Financials	S
	T-Mobile, Deutsche Telecom					
95	**T-Mobile US Inc**	TMUS:US	TMUS.O	Telecom	Communications	S
96	**Deutsche Telecom AG**	DTE:GR	DTEGn.DE	Telecom	Communications	S
97	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
98	**Automatic Data Processing Inc**	ADP:US	ADP.O	Technology Services	Technology	S
99	**Ameritrade Holding Corp**	AMTD:US	AMTD.O	Asset Management	Financials	S
100	**Choicepoint Inc**	CPS	CPS	Technology Services	Technology	S
101	**Bank of America Corp**	BAC:US	BAC	Banking	Financials	S

102	**Ralph Lauren Corp**	RL:US	RL	Apparel & Textile Products	Consumer Goods	S
103	**Microsoft Corp**	MSFT:US	MSFT.O	Software	Technology	S
104	**American Express Co**	AXP:US	AXP	Specialty Finance	Financials	S
105	**J.P. Morgan Chase & Co**	JPM:US	JPM	Banking	Financials	S
106	**Washington Mutual Inc.**	WAMUQ:US	…	Banking	Financials	S
107	**MBNA Corp.**	KRB:US	…	Specialty Finance	Financials	S
108	**Verizon Communications Inc.**	VZW:US Cellco Partnership	VZ	Telecom	Communications	S
109	**Walt Disney Co.**	DIS:US	DIS	Media	Communications	S
110	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
111	**DaimlerChrysler AG**	DCX:GR changed into DAI:GR (daimler) - FCAU:US formerly CGC (chrysler)	…	Automotive	Consumer Goods	M
112	**Kraft Foods Group Inc**	KRFT:US	KRFT:BN	Consumer Products	Consumer Goods	M
113	**New York Times Co.**	NYT:US	NYT	Media	Communications	S
114	**United Parcel Service Inc**	UPS:US	UPS	Transportation & Logistics	Industrials	S
115	**Creative Technology Ltd.**	CREAF:SP	CREAF.PK	Hardware	Technology	M
116	**Citigroup Inc**	C:US	C	Banking	Financials	S
117	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
118	**Boeing Co**	BA:US		Aerospace & Defense	Industrials	M
119	**Washington Post**	GHC:US	GHC	Consumer Services	Consumer Goods	S
12	**Microsoft**	MSFT:US	MSFT.O	Software	Technology	S

0	**Corp**					
121	**Delta Air Lines Inc**	DAL:US	DAL	Passenger Transportation	Consumer Goods	S
122	**Goldman Sachs Group Inc.**	GS:US	GS	Institutional Financial Svcs	Financials	S
123	**JPMorgan Chase & Co**	JPM:US	JPM	Banking	Financials	S
124	**Vodafone Group PLC**	VOD:LN	VOD.L	Telecom	Communications	S
125	**Cisco Systems Inc.**	CSCO:US	CSCO.O	Hardware	Technology	M
126	**Akamai Technologies Inc**	AKAM:US	AKAM.O	Software	Technology	S
127	**FedEx Corp**	FDX:US	FDX	Transportation & Logistics	Industrials	S
128	**Xerox Corp.**	XRX:US	XRX	Technology Services	Technology	M
129	**Yahoo! Inc**	YHOO:US	YHOO.O	Media	Communications	S
130	**DoubleClick Inc.**	DCLK:US acquired by GOOGL:US	…	Software	Technology	S
131	**Gateway Inc.**	GTW	…	Technology Hardware, Storage and Peripherals	Technology	M
132	**Nortel Networks Ltd**	NT:CN	…	Telecom	Communications	M
133	**Bank of America Corp**	BAC:US	BAC	Banking	Financials	S
134	**Microsoft Corp**	MSFT:US	MSFT.O	Software	Technology	S
135	**American Express Co**	AXP:US	AXP	Specialty Finance	Financials	S
136	**Continental Airlines Inc**	CAL	CAL	Passenger Transportation	Consumer Goods	S
137	**Citigroup Inc**	C:US	C	Banking	Financials	S
138	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
139	**CBS Corp**	CBS:US	CBS	Media	Communications	
140	**Lockheed Martin Corp**	LMT:US	LMT	Aerospace & Defense	Industrials	M
141	**Microsoft Corp**	MSFT:US	MSFT.O	Software	Technology	S
142	**Starbucks Corp**	SBUX:US	SBUX.O	Gaming, Lodging &	Consumer Goods	M

				Restaurants		
143	**Verizon Communications Inc.**	VZ:US	VZ	Telecom	Communications	S
144	**CSX Corp**	CSX:US	CSX.O	Transportation & Logistics	Industrials	S
145	**Vivendi SA**	VIV:FP	VIVT4.SA	Media	Communications	S
146	**FedEx Corp**	FDX:US	FDX	Transportation & Logistics	Industrials	S
147	**Interland Inc.**	ILND	…	Technology Services	Technology	S
148	**Countrywide Financial Corp**	BAC:US	BAC	Banking	Financials	S
149	**Comcast Corp**	CMCSA:US	CMCSA.O	Media	Communications	S
150	**Gannett Co Inc**	GCI:US	GCI	Media	Communications	S
151	**New York Times Co**	NYT:US	NYT	Media	Communications	S
152	**Verizon Communications Inc.**	VZ:US	VZ	Telecom	Communications	S
153	**Yahoo! Inc**	YHOO:US	YHOO.O	Media	Communications	S
154	**VeriSign Inc**	VRSN:US	VRSN.O	Media	Communications	S
155	**Interland Inc.**	ILND	…	Technology Services	Technology	S
156	**Ford Motor Co**	F	F	Automotive	Consumer Goods	M
157	**American Express Co**	AXP:US	AXP	Specialty Finance	Financials	S
158	**Travelocity**	SABR	SABR.O	Technology Services	Technology	S
159	**OfficeMax Inc.**	OMX:US	…	Retail - Discretionary	Consumer Goods	S
160	**DoubleClick Inc.**	DCLK:US acquired by GOOGL:US	…	Software	Technology	S
161	**Dow Jones & Co**	INDU:IND	…	Institutional Financial Svcs	Financials	S
162	**Bank of New York Mellon Corp**	BK:US	BK	Institutional Financial Svcs	Financials	S
16	**Cox**	COX	…	Media	Communicati	S

3	**Communications Inc**				ons	
164	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
165	Excite@Home	T:US	T	Telecom	Communications	S
166	**FedEx Corp**	FDX:US	FDX	Transportation & Logistics	Industrials	S
167	**AT&T Inc**	T:US	T	Telecom	Communications	S
168	**Microsoft Corp**	MSFT:US	MSFT.O	Software	Technology	S
169	**New York Times Co.**	NYT:US	NYT	Media	Communications	S
170	**SONICblue Inc**	SBLUQ:US	…	Hardware	Technology	M
171	**WorldCom Inc**	WCOME:US	…	Telecom	Communications	S
172	**S1 Corporation**	SON	012750.KS	Software	Technology	S
173	**Intel Corp**	INTC:US	INTC.O	Semiconductors	Technology	M
174	**Hewlett Packard Enterprise Co**	HPE:US	HPE	Technology Services	Technology	M
175	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
176	**Amazon.com Inc**	AMZN:US	AMZN.O	Retail - Discretionary	Consumer Goods	S
177	**Citigroup Inc**	C:US	C	Banking	Financials	S
178	**Northwest Airlines Inc**	NWACQ:US	…	Passenger Transportation	Consumer Goods	S
179	**American Online - AOL**	TWX:US	TWX	Media	Communications	S
180	**Drug Emporium Inc**			Retail - Consumer Staples	Consumer Goods	S
181	**Charles Schwab Corp**	SCHW:US	SCHW.K	Asset Management	Financials	S
182	**Lycos Internet Inc**	LYIL:IN	LYCO.NS	Software	Technology	S
183	**Yahoo! Inc**	YHOO:US	YHOO.O	Media	Communications	S
184	**Amazon.com Inc**	AMZN:US	AMZN.O	Retail - Discretionary	Consumer Goods	S

185	**eBay Inc**	EBAY:US	EBAY.O	Retail - Discretionary	Consumer Goods	S
186	**Ameritrade Holding Corp**	AMTD:US	AMTD.O	Asset Management	Financials	S
187	**E*TRADE Financial Corp**	ETFC:US	ETFC.O	Asset Management	Financials	S
188	**WorldCom Inc**	MCWEQ:US	…	Telecom	Communications	S
189	**Excite@Home**	T:US	T	Telecom	Communications	S
190	**National Discount Brokers Group Inc**	NDB	…	Institutional Financial Svcs	Financials	S
191	**AT&T Inc**	T:US	T	Telecom	Communications	S
192	**Barnes & Noble Inc**	BKS:US	BKS	Retail - Discretionary	Consumer Goods	S
193	**Bear Stearns Cos LLC**	2942331Q:US	…	Institutional Financial Svcs	Financials	S
194	**BTG PLC**	BTG plc (BTG.L)	BTG.L	Biotech & Pharma	Healthcare	M
195	**Cognos ULC**	COGN:US	…	Software	Technology	S
196	**Estee Lauder Cos Inc**	EL:US	EL	Consumer Products	Consumer Goods	M
197	**Ford Motor Co**	F:US	F	Automotive	Consumer Goods	M
198	**Merrill Lynch Investment Solutions**	MWTMNGE:LX	…	Institutional Financial Svcs	Financials	S
199	**Net2Phone Inc**	NTOP	…	Telecom	Communications	S
200	**TicketMaster Corporation**	TKTM	…	Media	Communications	S
201	**Trans World Airlines Inc**	TWAIQ:US	…	Passenger Transportation	Consumer Goods	S
202	**Nike Inc**	NKE:US	NKE	Apparel & Textile Products	Consumer Goods	M
203	**Sabre Corp**	TSG	…	Technology Services	Technology	S
204	**Western Union Co**	FDC	FDC	Specialty Finance	Financials	S
205	**Walt Disney Co.**	DIS:US	DIS	Media	Communications	S
206	**Egghead.com Inc**	EGHDQ:US	…	Retail - Discretionary	Consumer Goods	S

APPENDIX III

	ORGANIZATION	EVENT YEAR	ANNOUNCEMENT DATE	METHOD OF LEAK
1	**Twitch**	2015	23.03.2015	unknown
2	**Anthem Inc**	2015	04.02.2015	hacked
3	**Sony Corp**	2014	24.11.2014	hacked
4	**JPMorgan Chase & Co**	2014	02.10.2014	hacked
5	**Google**	2014	10.09.2014	hacked
6	**Home Depot Inc**	2014	08.09.2014	hacked
7	**Community Health Systems Inc**	2014	18.08.2014	hacked
8	**Domino's Pizza Group PLC**	2014	16.06.2014	hacked
9	**American Online - AOL**	2014	28.04.2014	hacked
10	**eBay Inc**	2014	21.05.2014	hacked
11	**United Parcel Service Inc**	2014	26.03.2014	hacked
12	**Walgreens Boots Alliance Inc**	2013	07.06.2013	lost / stolen computer
13	**Citigroup Inc**	2013	17.07.2013	poor security
14	**Nintendo Co Ltd**	2013	05.07.2013	hacked
15	**Twitter Inc**	2013	02.02.2013	hacked
16	**Apple Inc**	2013	18.07.2013	hacked
17	**Dun & Bradstreet Corp.**	2013	25.09.2013	hacked
18	**Vodafone Group PLC**	2013	12.09.2013	inside job
19	**Facebook Inc.**	2013	21.06.2013	accidentally published
20	**Target Corp.**	2013	27.11.2013	hacked
21	**Yahoo Japan Corp.**	2013	16.05.2013	hacked
22	**Ubisoft Entertainment SA**	2013	02.07.2013	hacked
23	**Adobe Systems Inc.**	2013	03.10.2013	hacked
24	**Massive American business hack**	2013	26.07.2013	
	7-Eleven, JC Penney, Hannaford, Heartland, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard			
25	**7-Eleven Malaysia Holdings Bhd**	2013	26.07.2013	hacked
26	**JC Penney Co Inc**	2013	26.07.2013	hacked
27	**Heartland Financial USA Inc**	2013	26.07.2013	hacked
28	**JetBlue Airways Corp**	2013	26.07.2013	hacked
29	**Euronet Worldwide Inc**	2013	26.07.2013	hacked
30	**Global Payments Inc**	2013	26.07.2013	hacked

31	**Yahoo! Inc**	2012	12.07.2012	hacked
32	**Global Payments Inc**	2012	30.03.2012	hacked
	LinkedIn, eHarmony, Last.fm			
33	**LinkedIn Corp**	2012	08.06.2012	accidentally published
34	**KT Corp.**	2012	29.07.2012	hacked
35	**Zappos**	2012	15.01.2012	hacked
36	**Apple Inc**	2012	08.03.2012	accidentally published
37	**Activision Blizzard Inc**	2012	09.08.2012	hacked
38	**Morgan Stanley**	2011	21.07.2011	lost / stolen media
39	**Morgan Stanley**	2011	28.02.2011	hacked
40	**Honda Motor Co Ltd**	2011	26.05.211	poor security
41	**Citigroup Inc**	2011	08.06.2011	hacked
42	**Sony Corp**	2011	03.06.2011	hacked
43	**Washington Post**	2011	27.06.2011	hacked
44	**Nintendo Co Ltd**	2011	05.06.2011	hacked
45	**Ubisoft Entertainment SA**	2011	27.06.2011	hacked
46	**Sega Sammy Holdings Inc**	2011	17.06.2011	hacked
47	**Electronic Arts Inc.**	2011	15.06.2011	hacked
48	**Countrywide Financial Corp**	2011	28.09.2011	inside job
49	**Nexon Co Ltd**	2011	26.11.2011	hacked
50	**Sony Corp**	2011	26.04.2011	hacked
51	**Sony Corp**	2011		hacked
	Health Net - IBM			
52	**International Business Machines Corp (IBM)**	2011	14.03.2011	lost / stolen media
53	**Health Net**	2011	14.03.2011	lost / stolen media
54	**AT&T Inc**	2010	10.06.2010	hacked
55	**Triple-S Management Corp**	2010	23.11.2010	lost / stolen media
56	**Betfair**	2010	30.09.2011	hacked
57	**JPMorgan Chase & Co**	2010		lost / stolen media

58	**Health Net**	2009	18.11.2009	lost / stolen media
59	**CheckFree Corporation**	2008	02.12.2008	hacked
60	**Heartland Financial USA Inc**	2008	20.01.2009	hacked
61	**Starbucks Corp**	2008	29.10.2008	lost / stolen computer
62	**AT&T Inc**	2008	15.05.2008	lost / stolen computer
63	**Worldpay Group PLC**	2008	23.12.2008	hacked
64	**GS Caltex**	2008	06.09.2008	inside job
65	**Bank of New York Mellon Corp**	2008	22.05.2008	lost / stolen media
66	**Gap Inc**	2007	28.09.2007	lost / stolen computer
67	**Automatic Data Processing Inc**	2007	15.09.2007	hacked
68	**TJX Cos Inc**	2007	18.01.2007	hacked
69	**Charles Schwab Corp**	2007	08.03.2007	hacked
70	**Merrill Lynch Investment Solutions**	2007	08.03.2007	hacked
71	**eBay Inc**	2007	18.08.2007	poor security
72	**Monster Worldwide Inc**	2007	21.08.2007	hacked
73	**Ameritrade Holding Corp**	2007	10.08.2007	hacked
74	**Fidelity National Information Services Inc**	2007	03.07.2007	inside job
75	**Dai Nippon Printing Co Ltd**	2007	12.03.2007	inside job
76	**H&R Block Inc**	2006	02.01.2006	lost / stolen computer
77	**FedEx Corp**	2006	04.02.2006	accidentally published
78	**OfficeMax Inc.**	2006	09.02.2006	hacked
79	**Honeywell International Inc**	2006	09.02.2006	poor security
80	**Mastercard Inc**	2006	27.02.2006	hacked
81	**Medco Health Solutions Inc.**	2006	01.03.2006	lost / stolen computer
82	**Verizon Communications Inc.**	2006	08.03.2006	lost / stolen computer
83	**General Motors Co**	2006	14.03.2006	inside job

84	**Boeing Co**	2006	21.03.2006	lost / stolen computer
85	**Aetna Inc**	2006	26.03.2006	lost / stolen computer
86	**Wells Fargo & Co**	2006	05.05.2006	lost / stolen computer
87	**M&T Bank Corp**	2006	19.05.2006	lost / stolen computer
88	**Hewlett Packard Enterprise Co**	2006	22.03.2006	lost / stolen media
89	**Countrywide Financial Corp**	2006	02.08.2008	inside job
90	**KDDI Corp**	2006	13.06.2006	hacked
91	**Circuit City Stores Inc.**	2006	02.06.2006	poor security
92	**AT&T Inc**	2006	30.08.2006	hacked
93	**E*TRADE Financial Corp**	2006	24.10.2006	hacked
94	**Ameritrade Holding Corp**	2006	24.10.2006	hacked
	T-Mobile, Deutsche Telecom			
95	**T-Mobile US Inc**	2006	04.10.2008	lost / stolen media
96	**Deutsche Telecom AG**	2006	04.10.2008	lost / stolen media
97	**American Online - AOL**	2006	06.08.2006	accidentally published
98	**Automatic Data Processing Inc**	2005	06.06.2006	poor security
99	**Ameritrade Holding Corp**	2005	19.04.2005	lost / stolen media
100	**Choicepoint Inc**	2005	17.02.2005	poor security
101	**Bank of America Corp**	2005	26.02.2005	lost / stolen computer
102	**Ralph Lauren Corp**	2005	14.04.2005	hacked
103	**Microsoft Corp**	2005	03.06.2005	hacked
104	**American Express Co**	2005	21.06.2005	hacked
105	**J.P. Morgan Chase & Co**	2005	21.06.2005	hacked
106	**Washington Mutual Inc.**	2005	21.06.2005	hacked
107	**MBNA Corp.**	2005	23.06.2005	inside job
108	**Verizon Communications Inc.**	2005	12.08.2005	poor security
109	**Walt Disney Co.**	2005	17.08.2005	hacked
110	**American Online - AOL**	2005	17.08.2005	hacked
111	**DaimlerChrysler AG**	2005	18.08.2005	hacked
112	**Kraft Foods Group Inc**	2005	19.08.2005	hacked
113	**New York Times Co.**	2005	20.08.2005	hacked
114	**United Parcel Service Inc**	2005	21.08.2005	hacked
115	**Creative Technology Ltd.**	2005	01.09.2005	hacked

116	**Citigroup Inc**	2005	06.06.2005	lost / stolen media
117	**American Online - AOL**	2004	23.06.2004	inside job
118	**Boeing Co**	2004	27.01.2004	hacked
119	**Washington Post**	2004	06.02.2004	inside job
120	**Microsoft Corp**	2004	13.02.2004	lost / stolen media
121	**Delta Air Lines Inc**	2004	05.05.2004	hacked
122	**Goldman Sachs Group Inc.**	2004	05.05.2004	hacked
123	**JPMorgan Chase & Co**	2004	05.05.2004	hacked
124	**Vodafone Group PLC**	2004	05.05.2004	hacked
125	**Cisco Systems Inc.**	2004	18.05.2004	poor security
126	**Akamai Technologies Inc**	2004	16.06.2004	hacked
127	**FedEx Corp**	2004	16.06.2004	hacked
128	**Xerox Corp.**	2004	16.06.2004	hacked
129	**Yahoo! Inc**	2004	16.06.2004	hacked
130	**DoubleClick Inc.**	2004	28.07.2004	hacked
131	**Gateway Inc.**	2004	28.07.2004	hacked
132	**Nortel Networks Ltd**	2004	28.07.2004	hacked
133	**Bank of America Corp**	2003	26.01.2003	hacked
134	**Microsoft Corp**	2003	28.01.2003	hacked
135	**American Express Co**	2003	30.01.2003	hacked
136	**Continental Airlines Inc**	2003	30.01.2003	hacked
137	**Citigroup Inc**	2003	11.03.2003	inside job
138	**American Online - AOL**	2003	21.04.2003	accidentally published
139	**CBS Corp**	2003	14.08.2003	hacked
140	**Lockheed Martin Corp**	2003	14.08.2003	hacked
141	**Microsoft Corp**	2003	16.08.2003	poor security
142	**Starbucks Corp**	2003	20.08.2003	hacked
143	**Verizon Communications Inc.**	2003	20.08.2003	hacked
144	**CSX Corp**	2003	21.08.2003	
145	**Vivendi SA**	2003	08.10.2003	lost / stolen media
146	**FedEx Corp**	2003	23.08.2003	hacked
147	**Interland Inc.**	2003	08.09.2003	hacked
148	**Countrywide Financial Corp**	2003	30.01.2003	hacked
149	**Comcast Corp**	2002	08.02.2002	poor security
150	**Gannett Co Inc**	2002	12.07.2002	hacked
151	**New York Times Co**	2002	27.02.2002	poor security
152	**Verizon Communications Inc.**	2002	21.08.2002	poor security
153	**Yahoo! Inc**	2002	05.03.2002	poor security
154	**VeriSign Inc**	2002	21.03.2002	hacked
155	**Interland Inc.**	2002	21.03.2002	hacked
156	**Ford Motor Co**	2002	17.05.2002	poor security

157	**American Express Co**	2001	24.01.2001	poor security
158	**Travelocity**	2001	25.01.2001	poor security
159	**OfficeMax Inc.**	2001	22.02.2001	poor security
160	**DoubleClick Inc.**	2001	30.03.2001	hacked
161	**Dow Jones & Co**	2001	20.07.2001	hacked
162	**Bank of New York Mellon Corp**	2001	01.08.2001	poor security
163	**Cox Communications Inc**	2001	08.08.2001	hacked
164	**American Online - AOL**	2001	09.08.2001	hacked
165	**Excite@Home**	2001	09.08.2001	hacked
166	**FedEx Corp**	2001	09.08.2001	hacked
167	**AT&T Inc**	2001	10.08.2001	hacked
168	**Microsoft Corp**	2001	09.08.2001	hacked
169	**New York Times Co.**	2001	01.11.2001	hacked
170	**SONICblue Inc**	2001	20.09.2001	hacked
171	**WorldCom Inc**	2001	06.12.2001	poor security
172	**S1 Corporation**	2001	06.07.2001	poor security
173	**Intel Corp**	2001	15.02.2001	hacked
174	**Hewlett Packard Enterprise Co**	2001	15.02.2001	hacked
175	**American Online - AOL**	2001	26.01.2001	poor security
176	**Amazon.com Inc**	2001	05.03.2001	poor security
177	**Citigroup Inc**	2001	06.09.2001	poor security
178	**Northwest Airlines Inc**	2000	08.01.2000	poor security
179	**American Online - AOL**	2000	27.01.2000	poor security
180	**Drug Emporium Inc**	2000	31.01.2000	poor security
181	**Charles Schwab Corp**	2000	08.02.2000	hacked
182	**Lycos Internet Inc**	2000	08.02.2000	hacked
183	**Yahoo! Inc**	2000	08.02.2000	hacked
184	**Amazon.com Inc**	2000	09.02.2000	hacked
185	**eBay Inc**	2000	09.02.2000	hacked
186	**Ameritrade Holding Corp**	2000	10.02.2000	hacked
187	**E*TRADE Financial Corp**	2000	10.02.2000	hacked
188	**WorldCom Inc**	2000	10.02.2000	hacked
189	**Excite@Home**	2000	11.02.2000	hacked
190	**National Discount Brokers Group Inc**	2000	25.02.2000	hacked
191	**AT&T Inc**	2000	05.05.2000	hacked
192	**Barnes & Noble Inc**	2000	05.05.2000	hacked
193	**Bear Stearns Cos LLC**	2000	05.05.2000	hacked
194	**BTG PLC**	2000	05.05.2000	hacked
195	**Cognos ULC**	2000	05.05.2000	hacked
196	**Estee Lauder Cos Inc**	2000	05.05.2000	hacked
197	**Ford Motor Co**	2000	05.05.2000	hacked

198	**Merrill Lynch Investment Solutions**	2000	05.05.2000	hacked
199	**Net2Phone Inc**	2000	05.05.2000	hacked
200	**TicketMaster Corporation**	2000	05.05.2000	hacked
201	**Trans World Airlines Inc**	2000	05.05.2000	hacked
202	**Nike Inc**	2000	22.06.2000	poor security
203	**Sabre Corp**	2000	27.06.2000	poor security
204	**Western Union Co**	2000	11.09.2000	poor security
205	**Walt Disney Co.**	2000	27.09.2000	poor security
206	**Egghead.com Inc**	2000	23.12.2000	poor security

REFERENCES

Abbate, J. 2010. *Privatizing the Internet: Competing Visions and Chaotic Events, 1987–1995.* IEEE Annals of the History of Computing, Vol. 32(1): 10-22

Acquisti, A., Friedman, A., and Telang, R. 2006. *Is there a cost to privacy breaches? An event study.* ICIS 2006. Proceedings of the International Conference on Information Systems, 1563-1580.

Adam, F. and O'Doherty, P. 2000. *Lessons from Enterprise Resource Planning Implementations in Ireland–Towards Smaller and Shorter ERP Projects*. Journal Of Information Technology, Vol. 15(4): 305-316.

Akkermans, H.A., Bogerd, P., Yücesan, E. and Van Wassenhove, L.N. 2003. *The Impact of ERP on Supply Chain Management: Exploratory Findings from a European Delphi Study*. European Journal of Operational Research, Vol. 146(2): 284-301.

Al-Ahmad, W., Al-Fagih, K., Khanfar, K., Alsamara, K., Abuleil, S. and Abu-Salem, H. 2009. *A taxonomy of an IT project failure: root causes. International Management Review*, Vol. 5(1): 93-104.

Alberts, C.J. and Dorofee, A. 2002. M*anaging Information Security Risks: The OCTAVE Approach*. Addison-Wesley Longman Publishing Co., Inc.

Alter, S. and Sherer, S.A. 2004. *A General, But Readily Adaptable Model of Information System Risk.* AIS, Vol. 14(1): 1–28.

Andoh-Baidoo, F.K., and Osei-Bryson, K.M. 2007. *Exploring the characteristics of Internet security breaches that impact the market value of breached firms*. Expert Systems with Applications, Vol. 32(3): 703-725.

Appleton, E.L. 1997. *How to Survive ERP*. Datamation, Vol. 43(3): 50-3.

Arcuri, M.C., Brogi, M. and Gandolfi, G. 2014. *The effect of information security breaches on stock returns: Is the cyber crime a threat to firms?* Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), 175-193.

Avison, D. and Wilson, D. 2002. *IT failure and the collapse of One. Tel.* In Information Systems, 31-46.

Aytes, K., Byers, S., and Santhanakrishnan, M. 2006. *The Economic Impact of Information Security Breaches: Firm Value and Intra-industry Effects.* AMCIS 2006 Proceedings, 3305-3312.

Banker, R.D., Bardhan, I.R., Hsihui, C. And Shu, L. 2006. *Plant information systems, manufacturing capabilities, and plant performance.* MIS Quarterly, Vol. 30(2): 315-337.

Baran, P. 1964. *On distributed communications networks.* IEEE transactions on Communications Systems, Vol. 12(1): 1-9.

Barclay, C. 2008. *Towards an integrated measurement of IS project performance: The project performance scorecard.* Information Systems Frontiers, Vol. 10(3): 331-345.

Barker, T. and Frolick, M.N. 2003. *ERP implementation failure: A case study.* Information Systems Management, Vol. 20(4): 43-49.

Beynon-Davies, P. 1995. *Information systems 'failure': the case of the London Ambulance Service's Computer Aided Despatch project.* European Journal of Information Systems, Vol. 4(3): 171-184.

Bharadwaj, A. and Keil, M. 2001. *The effect of information technology failures on the market value of firms: An empirical examination.* INFORMS Miami, November 2001

Bhattacherjee, A. and Hikmet, N. 2007. *Physicians' resistance toward healthcare information technology: a theoretical model and empirical test.* European Journal of Information Systems, Vol. 16(6): 725-737.

Bignell, V. and Fortune, J. 1984. *Understanding Systems Failure*. Manchester University Press.

Bolster, P., Pantalone, C.H. and Trahan, E.A. 2010. *Security Breaches and Firm Value.* Journal of Business Valuation and Economic Loss Analysis, Vol. 5(1): 1-11.

Borek, A., Parlikad, A.K., Webb, J. and Woodall, P. 2013. *Total Information Risk Management: Maximizing the Value Of Data And Information Assets*. Newnes.

Bose, I. and Leung, A.C.M. 2013. *The Impact of Adoption of Identity Theft Countermeasures on Firm Value.* Decision Support Systems, Vol. 55(3), 753-763.

Borko, H. 1968. *The Conceptual Foundations of Information Systems*. In E. B. Montgomery (Ed.), The foundations of access to knowledge: A symposium. Syracuse: Syracuse University Press.

Bose, I. and Leung, A.C.M. 2014. *Do phishing alerts impact global corporations? A firm value analysis*. Decision Support Systems, Vol. 64: 67-78.

Brakely, H.H. 1999. *What Makes ERP Effective?* Manufacturing Systems, Vol. 17(3): 120.

Bruque, S., Moyano, J. and Eisenberg, J. 2008. *Individual adaptation to IT-induced change: The role of social networks.* Journal of Management Information Systems, Vol. 25(3): 177-206.

Brynjolfsson, E. 1996. *The Contribution Of Information Technology to Consumer Welfare.* Information Systems Research, Vol. 7(3): 281-300.

Brynjolfsson, E. and Hitt, L.M. 2003. *Computing Productivity: Firm-Level Evidence*. Review of Economics and Statistics, Vol. 85(4): 793-808.

Bureau of Economic Analysis. 2007. *Table 5.3.5: Private fixed investments by type.* Available at http://www.bea.gov/bea/dn/nipaweb/ TableView.asp?SelctedTable=128&FirstYear=2006&LastYera=2008&Freq=Qtr.

Bussen, W. and Myers, M.D. 1997. *Executive information system failure: a New Zealand case study.* Journal of Information Technology, Vol. 12(2): 145-153.

Burritt, R. 2000. *Buyer Beware*. Australian CPA, Vol. 70(8): 48-9.

Büyüközkan, G., and Ruan, D. *Choquet Integral Based Aggregation Approach to Software Development Risk Assessment*. Information Sciences, Vol. 180(3): 441-451.

Campbell, John Y., Andrew W. Lo, and MacKinlay A. C. 1997. *The Econometrics of Financial Markets*, Princeton University Press, Princeton, NJ!.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. 2003. *The Economic Cost Of Publicly Announced Information Security Breaches: Empirical Evidence From The Stock Market.* Journal of Computer Security, Vol. 11(3): 431-448.

Cao, Q. and Dowlatshahi, S. 2005. *The impact of alignment between virtual enterprise and information technology on business performance in an agile manufacturing environment.* Journal of Operations Management, Vol. 23(5): 531-550.

Cardenas, J., Coronado, A., Donald, A., Parra, F. and Mahmood, M.A. 2012. *The economic impact of security breaches on publicly traded corporations: An empirical investigation.* AMCIS 2012 Proceedings. 7.

Cavusoglu, H., Mishra, B. and Raghunathan, S. 2004. *The Effect Of Internet Security Breach Announcements On Market Value: Capital Market Reactions For Breached Firms and Internet Security Developers.* International Journal of Electronic Commerce. Vol. 9(1): 70-104.

Cavusoglu, H., Cavusoglu, H., and Zhang, J. 2008. *Security patch management: Share the burden or share the damage?.* Management Science, Vol. 54(4): 657-670.

CBS, 2003. *Locking Windows.* Associated Press, January 16.

CERT, 2004. *CERT/CC Statistics 1988–2003*. Carnegie- Mellon University, Software Engineering Institute, January 22.

Chai, S., Kim, M. and Rao, H.R. 2011. *Firms' information security investment decisions: Stock market evidence of investors' behavior.* Decision Support Systems, Vol. 50(4): 651-661.

Chen, S.J. and Chen, S.M., 2003. *Fuzzy Risk Analysis Based On Similarity Measures Of Generalized Fuzzy Numbers*. IEEE Transactions on fuzzy systems, Vol. 11(1): 45-56.

Clarke, J., Jandik, T. and Mandelker, G., 2001. *The efficient markets hypothesis.* Expert financial planning: Advice from industry leaders, pp. 126-141.

Clemente, R., Bartoli, M., Bossi, M.C., D'orazio, G. and Cosmo, G. 2005. *Risk management in availability SLA*. In: 5th International Workshop on Design of Reliable Communication Networks (DRCN 2005). Proceedings. IEEE; 2005, October. p. 8.

Cooke, D.P. and Peterson, W.J. 1998. *SAP Implementation: Strategies and Results*. The Conference Board. New York, NY.

Coons, S.A. 1963. An Outline of the Requirements For A Computer-Aided Design System. In Proceedings of AFIPS Spring Joint Computer Conference Vol. 23: 299-304.

Cooper, M.J., Dimitrov, O. and Rau, P.R., 2001. *A rose.com by any other name.* The Journal of Finance, Vol. 56(6): 2371-2388.

Copeland, B.J. 2004. *Colossus: Its Origins and Originators*. IEEE Annals of the History of Computing, Vol. 26(4), pp.38-45.

Copeland, B.J. 2005. *Colossus: The First Electronic Computer (Popular Science).* Oxford University Press.

Coursen, S., 1997. *The financial impact of viruses.* Information Systems Security. Vol. 6(1): 64-70.

Davenport, T.H. 1998. *Putting the Enterprise into the Enterprise System.* Harvard business review, Vol. 76(4): 121-31.

Davis, M. 2000. *The Universal Computer: The Road From Leibniz To Turing*. WW Norton & Company.

De Haes, S. and Van Grembergen, W. 2009. *An Exploratory Study into IT Governance Implementations and Its Impact on Business/IT Alignment.* Information Systems Management, Vol. 26(2): 123-137.

Dehning, B., Richardson, V.J. and Zmud, R.W. 2007. *The financial performance effects of IT-based supply chain management systems in manufacturing firms.* Journal of Operations Management, Vol. 25(4): 806-824.

DeLone, W.H. and McLean, E.R. 1992. I*nformation Systems Success: The Quest for the Dependent Variable.* Information Systems Research, Vol. 3(1): 60-95.

Dewan, S. and Min, C.K. 1997. *The Substitution of Information Technology for Other Factors of Production: A Firm Level Analysis*. Management Science, Vol. 43(12): 1660-1675.

Douglas, J.L. 2006. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Auerbach Publications.

Dwivedi, Y.K., Ravichandran, K., Williams, M.D., Miller, S., Lal, B., Antony, G.V. and Kartik, M. 2013. *IS/IT project failures: a review of the extant literature for deriving a taxonomy of failure factors*. In International Working Conference on Transfer and Diffusion of IT: 73-88. Springer Berlin Heidelberg.

Ehie, I.C. and Madsen, M. 2005. *Identifying Critical Issues in Enterprise Resource Planning (ERP) Implementation.* Computers in Industry, Vol. 56(6): 545-557.

Eklund. J. and Ellström P.E. 2000. *Standardisation - A Means for Creating Developing Work.* Linköping University, In Applied Ergonomics, Vol. 31(6): 641-648.

El Kadiri, S., Grabot, B., Thoben, K.D., Hribernik, K., Emmanouilidis, C., Von Cieminski, G. and Kiritsis, D. 2016. *Current Trends On ICT Technologies For Enterprise İnformation Systems.* Computers in Industry, Vol. 79: 14-33.

Engelbart, D.C. and English, W.K. 1968. *A Research Center for Augmenting Human Intellect*. In Proceedings of the December 9-11, 1968, fall joint computer conference, part I: 395-410. ACM.

Ettredge, M. and Richardson, V.J. 2002. *Assessing The Risk In E-Commerce*. In System Sciences, HICSS, Proceedings of the 35th Annual Hawaii International Conference on (pp. 11). Los Alamitos, CA: IEEE Computer Society Press.

Ettredge, M.L. and Richardson, V.J. 2003. *Information transfer among internet firms: the case of hacker attacks.* Journal of Information Systems, Vol. 17(2): 71-82.

Ewusi-Mensah, K. 2003. *Software Development Failures: Anatomy of Abandoned Projects.* The MIT press.

Fan, M., Stallaert, J. and Whinston, A.B. 2000. *The Adoption and Design Methodologies of Component-Based Enterprise Systems.* European Journal of Information Systems, Vol. 9(1): 25-35.

Fama, E.F. 1970. *Efficient capital markets: A review of theory and empirical work.* The journal of Finance, Vol. 25(2): 383-417.

Fama, E.F. 1991. *Efficient capital markets: II.* The journal of finance. Vol. 46(5): 1575-1617.

Fan, C.F. and Yu, Y.C. 2004. *BBN-based software project risk management*. Journal of Systems and Software, Vol. 73(2): 193-203.

Fasth, Å. 2012. *Quantifying Levels of Automation. Department of product and production development*. Chalmers University of Technology, 2012.

Feng, N., Wang, H. J., and Li, M. 2014. *A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis.* Information sciences, Vol. 256: 57-73.

Fitzgerald, G. and Russo, N.L. 2005. *The turnaround of the London ambulance service computer-aided despatch system (LASCAD).* European Journal of Information Systems, Vol. 14(3): 244-257.

Flowers, T.H. 1983. *The Design of Colossus (foreword by Howard Campaigne).* Annals of the History of Computing, Vol. 5(3): 239-252.

Gaftea, V. 2014. *Socio-economic Major Risks Related to the Information Technology.* Procedia Economics and Finance, Vol. 8: 336-345.

Gamarra, C., Guerrero, J.M. and Montero, E. 2016. *A Knowledge Discovery in Databases Approach for Industrial Microgrid Planning.* Renewable and Sustainable Energy Reviews, Vol. 60: 615-630.

Gattiker, T.F. and Goodhue, D.L. 2005. *What Happens After ERP Implementation: Understanding the Impact of Interdependence and Differentiation on Plant-Level Outcomes.* MIS Quarterly, Vol. 29(3): 559-585.

Gatzlaff, K.M. and McCullough, K.A. 2010. *The effect of data breaches on shareholder wealth.* Risk Management and Insurance Review, Vol. 13(1): 61-83. Gibson, C.F. 2003. *IT-enabled business change: an approach to understanding and managing risk.* MIS Quarterly Executive, Vol. 2(2): 104– 115.

Goel, S. and Shawky, H.A. 2009. *Estimating the market impact of security breach announcements on firm values.* Information & Management, Vol. 46(7): 404-410.

Good, J., Michie, D. and Timms, G. 1945. *General Report on Tunny: With Emphasis on Statistical Methods*. Bletchley Park Report HW, 25(4): 35.

Gordon, L.A., Loeb, M.P. and Zhou, L. 2011. *The impact of information security breaches: Has there been a downward shift in costs?* Journal of Computer Security, Vol. 19(1): 33-56.

Gordon, L.A. and Loeb, M.P. 2002. *The Economics of Information Security Investment.* ACM Transactions on Information and System Security (TISSEC), Vol. 5(4): 438-457.

Gordon, L.A., Loeb, M.P. W., Lucyshyn, W. and Richardson, R. 2005. *CSI/FBI Computer Crime and Security Survey,* Computer Security Institute, San Francisco.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2010. *CSI/FBI Computer Crime and Security Survey.* Computer Security Institute, San Francisco.

Greenstein, S. 2001. *Commercialization of The Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked So Well.* Innovation Policy and the Economy, Vol. 1: 151-186.

Grier, D.A. 2000. *Agricultural Computing and the Context for John Atanasoff.* IEEE Annals of the History of Computing, Vol. 22(1): 48-61.

Grier, D.A. 2004. *Letters to the Editor*, IEEE Annals of the History of Computing, Vol. 26(3): 66-68.

Grunske, L. and Joyce, D. 2008. *Quantitative Risk-Based Security Prediction for Component-Based Systems with Explicitly Modeled Attack Profiles*. Journal of Systems and Software, Vol. 81(8): 1327-1345.

Gullander, P., Fast-Berglund, Å., Harlin, U., Mattsson, S., Groth, C., Åkerman, M. and Stahre, J. 2014. *Meetings–The Innovative Glue Between The Organisation System And Information System.* In The sixth Swedish Production Symposium.

Gupta, A. 2000. *Enterprise Resource Planning: The Emerging Organizational Value Systems.* Industrial Management & Data Systems, Vol. 100(3): 114-118.

Gupta, H. 2011. *Management Information System*. Int. Book House, New Dehli, India

Hahn, T.B. 1996. *Pioneers of the Online Age.* Information Processing & Management, Vol. 32(1): 33-48.

Haigh, T. 2008. *Protocols for Profit. Web and E-mail Technologies as Product and Infrastructure*. The internet and American business: 105-158. 1st ed. Cambridge, Mass.: MIT Press

Haigh, T. 2011. *The History Of Information Technology.* Annual Review of Information Science and Technology, Vol. 45(1): 431-487.

Harmon, P. 2010. *The Scope and Evolution of Business Process Management*. In Handbook on Business Process Management 1: 37-81. Springer Berlin Heidelberg.

Harris, S. 2010. *CISSP All-in-One Exam Guide*. McGraw-Hill, Inc..

Hayes, R.M. 1985. *The History of Library and Information Science: A Commentary.* The Journal of Library History, Vol. 20(2): 173-178.

Hayes, D.C., Hunton, J.E. and Reck, J.L. 2001. *Market Reaction to ERP Implementation Announcements.* Journal of Information systems, Vol. 15(1): 2-18. Heeks, R. 2002.

Information Systems and Developing Countries: Failure, Success and Local Improvisations. The Information Society Vol. 18(2): 101-112.

Hendrick, H.W. and Kleiner, B.M. 2001. *Macroergonomics: An introduction to work system design.* Human Factors and Ergonomics Society.

Hendricks, K.B. and Singhal, V.R. 1996. *Quality awards and the market value of the firm: An empirical investigation*. Management science, Vol. 42(3): 415-436.
Hendricks, K.B., Singhal, V.R. and Stratman, J.K. 2007. *The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations*. Journal of Operations Management, Vol. 25 (1): 65–82

Heskett, J.L., Sasser, W.E., Hart, C.W.L. 1990. *Service Breakthroughs: Changing the Rules of the Game.* The Free Press, New York, NY.

Hinz, O., Nofer, M., Schiereck, D. and Trillig, J. 2015. *The influence of data theft on the share prices and systematic risk of consumer electronics companies.* Information & Management, Vol. 52(3): 337-347.

Hirschheim, R. and Newman, M. 1988. *Information systems and user resistance: theory and practice.* The Computer Journal, Vol. 31(5): 398-408.

Hitt, L.M. and Brynjolfsson, E. 1996. *Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value*. MIS Quarterly, Vol. 20(2): 121-142.

Horvath, V., Ghez, J., Khodyakov, D. and Yaqub, O. 2015. *Education, Technology and Connectedness. Global Societal Trends to 2030.*Thematic Report 2. Rand Europe.

Hovav, A. and D'Arcy, J. 2003. *The Impact Of Denial-Of-Service Attack Announcements On The Market Value Of Firms*. Risk Management and Insurance Review, Vol. 6(2): 97-121.

Hovav, A. and D'arcy, J. 2005. *Capital Market Reaction to Defective IT Products: The Case Of Computer Viruses.* Computers & Security, Vol. 24(5): 409-424.

Huang, Z. and Palvia, P. 2001. *ERP Implementation Issues in Advanced and Developing Countries*. Business Process Management Journal, Vol. 7(3): 276-284.

Im, K.S., Dow, K.E. and Grover, V., 2001. *Research Report: A Reexamination of IT Investment and the Market Value of the Firm—an Event Study Methodology*. Information Systems Research, Vol. 12(1), pp.103-117.

Irani, Z. 2002. *Information Systems Evaluation: Navigating Through the Problem Domain.* Information & Management, Vol. 40(1): 11-24.

Ishiguro, M., Tanaka, H., Matsuura, K. and Murase, I. 2006. *The effect of information security incidents on corporate values in the Japanese stock market.* In International Workshop on the Economics of Securing the Information Infrastructure (WESII).

ISO/IEC. 2013. *Information Technology Security Techniques Code Of Practice For Information Security Management.* Geneva: ISO; International Organization for Standardization, 27002.

Jain, A., Jain, P.K., Chan, F.T. and Singh, S. 2013. *A Review on Manufacturing Flexibility.* International Journal of Production Research, Vol. 51(19): 5946-5970.

Jeong, B.K. and Lu, Y. 2008. *The impact of radio frequency identification (RFID) investment announcements on the market value of the firm.* Journal of Theoretical and Applied Electronic Commerce Research, Vol. 3(1): 41-54.

Johnson, T.E. 1963. *Sketchpad III, Three Dimensional Graphical Communication with a Digital Computer.* In Proceedings of AFIPS Spring Joint Computer Conference, Vol. 23: 347–353.

Jouini, M., Rabai, L. B. A., and Aissa, A. B. 2014. *Classification of security threats in information systems*. Procedia Computer Science, Vol. (32): 489-496.

Jourdan Z., Rainer R.K. Jr, Marshall T.E., Nelson Ford, F. 2010. An Investigation Of Organizational Information Security Risk Analysis. Journal of Service Science, Vol. 3(2): 33–42.

Kakabadse, N.K., Kakabadse, A. and Kouzmin, A. 2003. *Reviewing The Knowledge Management Literature: Towards A Taxonomy.* Journal of knowledge management, Vol. 7(4): 75-91.

Kannan, K., Rees, J. and Sridhar, S. 2004. *Reexamining the impact of information security breach announcements on firm performance.* In Proceedings of the Ninth INFORMS Conference on Information Systems and Technology (CIST).

Kannan, K., Rees, J. and Sridhar, S. 2007. *Market Reactions To Information Security Breach Announcements: An Empirical Analysis.* International Journal of Electronic Commerce, Vol. 12(1): 69-91.

Kappelman, L.A., McKeeman, R. and Zhang, L. 2006. *Early warning signs of IT project failure: The dominant dozen.* Information systems management, Vol. 23(4): 31-36.

Karabacak, B. and Sogukpinar, I. 2005. *ISRAM: Information Security Risk Analysis Method.* Computers & Security, Vol. 24(2): 147-159.

Karlsson, M., Mattsson, S., Fast-Berglund, Å. and Stahre, J., 2013. *Could the use of ICT tools be the way to increase competitiveness in Swedish industry*?. IFAC Proceedings Vol.46(15): 179-186.

Karpoff, J.M. and Rankine, G. 1994. *In search of a signaling effect: The wealth effects of corporate name changes.* Journal of Banking & Finance, Vol. 18(6): 1027-1045.

Karygiannis, T. and Owens, L. 2002. *Wireless network security*. NIST special publication, Vol. 800: 48.

Kaspersky Lab, 2012. *Global IT security risks: 2012*

Keil, M., Cule, P.E., Lyytinen, K. and Schmidt, R.C. 1998. *A framework for identifying software project risks.* Communications of the ACM, Vol. 41(11): 76-83.

Kelley, M.R. 1994. *Productivity and information technology: The elusive connection.* Management Science, Vol. 40(11): 1406-1425.

Kelly, L. 2003. *Government reexamines IT failures*. Computing, July. Available at: http://www.accountancyage.com/aa/news/1774407/it-debacles-ensure-future-success-public-sector

Klaus, T. and Blanton, J.E. 2010. *User resistance determinants and the psychological contract in enterprise system implementations*. European Journal of Information Systems, Vol. 19(6): 625-636.

Kivijärvi, H. and Saarinen, T. 1995. *Investment in Information Systems and The Financial Performance Of The Firm.* Information & Management, Vol. 28(2): 143-163.

Koch, C. 2002. *Supply chain: Hershey's bittersweet lesson.* CIO Magazin, November, 15.

Koch, C. 2004. *Nike Rebounds: How (and Why) Nike Recovered from Its Supply Chain Diaster*. CIO Austrialia's Magazine for Executives, June 15.

Koch, C. 2007. *When Bad Things Happen To Good Projects*. *CIO-FRAMINGHAM MA.* Vol. 18: 50-59.

Koh, S.L. and Saad, S.M. 2006. *Managing Uncertainty in ERP-Controlled Manufacturing Environments in SMEs*. International Journal of Production Economics, Vol. 101(1): 109-127.

Konchitchki, Y. and O'Leary, D.E. 2011. *Event study methodologies in information systems research.* International Journal of Accounting Information Systems, Vol. 12(2): 99-115.

Kumar, K. and Hillegersberg, J.V. 2000. *ERP Experience and Evolution.* Communications of the ACM, Vol. 43(4): 23-26.

Landoll, D.J. 2006. *The security risk assessment handbook: A complete guide for performing security risk assessments.* 2nd ed. Boca Raton: Auerbach Publications.

Laumer, S. and Eckhardt, A. 2012. *Why do people reject technologies: a review of user resistance theories.* In Information systems theory: 63-86. Springer New York.

Laumer, S., Maier, C., Weitzel, T. and Eckhardt, A. 2012. *The Implementation of Large-Scale Information Systems in Small and Medium-Sized Enterprises--A Case Study of Work- and Health-Related Consequences.* In System Science (HICSS), 2012 45th Hawaii International Conference: 3159-3168.

Lengnick-Hall, C.A., Lengnick-Hall, M.L. and Abdinnour-Helm, S. 2004. *The role of social and intellectual capital in achieving competitive advantage through enterprise resource planning (ERP) systems*. Journal of Engineering and Technology Management, Vol. 21(4): 307-330.

Leung, A. and Bose, I. 2008. *Indirect Financial Loss of Phishing to Global Market.* ICIS 2008 Proceedings :5.

Liang, H., Saraf, N., Hu, Q. and Xue, Y. 2007. Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. MIS quarterly, Vol. 31(1): 59-87.

Licklider, J.C. and Taylor, R.W. 1968. *The computer as a communication device.* Science and Technology, Vol. 76(2): 21-31.

Loch, K.D., Carr, H.H. and Warkentin, M.E. 1992. *Threats To Information Systems: Today's Reality, Yesterday's Understanding*. MIS Quarterly, Vol. 16(2): 173-186.

Lucas, H.C. 1975. Why information systems fail. New York: Columbia University Press.

Lyytinen, K. and Hirschheim, R. 1988. *Information systems failures: a survey and classification of the empirical literature.* Oxford surveys in information technology, Vol. 4(1): 257-309.

Mabert, V.A., Soni, A. and Venkataramanan, M.A. 2001*. Enterprise Resource Planning: Common Myths Versus Evolving Reality.* Business Horizons, Vol. 44(3): 69-76.

Machlup, F. and Mansfield, U. 1983. *The study of information: Interdisciplinary* messages. New York: Wiley.

MacKinlay, A.C. 1997. *Event studies in economics and finance*. Journal of economic literature, Vol. 35(1): 13-39.
Mahoney, M.S. 2005. *The histories of computing (s).* Interdisciplinary Science Reviews, Vol. 30(2): 119-135.

Maier, C., Laumer, S., Eckhardt, A. and Weitzel, T. 2013. *Analyzing the impact of HRIS implementations on HR personnel's job satisfaction and turnover intention.* The Journal of Strategic Information Systems, Vol. 22(3): 193-207.

Mailloux, L.O., Grimaila, M.R. Colombi, J.M., Hodson, D.D. and Baumgartner, G. 2013. *Emerging Trends In ICT Security*. 1st ed. Morgan Kaufmann.

Markoff, J. 2002. *Stung by security flaws, Microsoft makes software safety a top goal.* January 17, The New York Times.

Mathe, H. and Dagi, T.F. 1996. *Harnessing technology in global service businesses.* Long Range Planning, Vol. 29(4): 449-461.

Mattern, F. and Floerkemeier, C. 2010. *From the Internet of Computers to the Internet of Things.* In From Active Data Management to Event-Based Systems And More 6462: 242-259.

Mattsson, S., Karlsson, M., Fast-Berglund, Å. and Hansson, I., 2014. Managing production complexity by empowering workers: six cases. Procedia CIRP, 17, pp.212-217.

McAfee, J. and Haynes, C. 1989. *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System: What They Are, how They Work, and how to Defend Your PC, Mac, Or Mainframe*. New York, NY: St. Martin's Press.

McCue, A. 2008. Beware the insider security threat. CIO Jury.

McGrath, K. 2002. *The Golden Circle: a way of arguing and acting about technology in the London Ambulance Service*. European Journal of Information Systems, Vol. 11(4): 251-266.

McWilliams, A. and Siegel, D. 1997. *Event studies in management research: Theoretical and empirical issues.* Academy of management journal, Vol. 40(3): 626-657.

Melville, N., Kraemer, K. and Gurbaxani, V. 2004. *Review: Information Technology and Organizational Performance: An Integrative Model Of IT Business Value*. MIS Quarterly, Vol. 28(2): 283-322.

Metcalfe, R.M. and Boggs, D.R. 1976. *Ethernet: Distributed packet switching for local computer networks*. Communications of the ACM, Vol. 19(7): 395-404.

Misra, S.C., Kumar, V. and Kumar, U. 2007. *A strategic modeling technique for information security risk assessment.* Information Management & Computer Security, Vol. 15(1): 64-77.

Modi, S.B., Wiles, M.A. and Mishra, S. 2015. *Shareholder value implications of service failures in triads: The case of customer information security breaches.* Journal of Operations Management, Vol. 35: 21-39.

Morse, E.A., Raval, V. and Wingender Jr, J.R. 2011. *Market price effects of data security breaches.* Information Security Journal: A Global Perspective, Vol. 20(6): 263-273.

Motwani, J., Subramanian, R. and Gopalakrishna, P. 2005. *Critical Factors for Successful ERP Implementation: Exploratory Findings from Four Case Studies.* Computers in Industry, Vol. 56(6): 529-544.

Murray, J.P. 2000. *Reducing IT project complexity. INFORMATION STRATEGY.* The Executive's Journal. Vol. 16(3): 30-38.

Myers, B.A. 1998. *A Brief History of Human-Computer Interaction Technology. Interactions*, Vol. 5(2): 44-54.

Nelson, R. R. 2007. *IT project management: infamous failures, classic mistakes, and best practices.* MIS Quarterly Executive, Vol. 6(2): 67–78.

Nicolaou, A.I. 2004. *Firm Performance Effects In Relation To the Implementation and Use of Enterprise Resource Planning Systems*. Journal of information systems, Vol. 18(2): 79-105.

NIST (National Institute of Standards and Technology). 2013. *Security and Privacy controls for Federal Information Systems and organizations.* NIST Special Publication. p. 800-853.

Palaniswamy, R. and Frank, T. 2000. *Enhancing Manufacturing Performance with ERP Systems*. Information Systems Management, Vol. 17(3): 43-55.

Pan, G., Hackney, R. and Pan, S.L. 2008. *Information Systems implementation failure: Insights from prism*. International Journal of Information Management, Vol. 28(4): 259-269.

Peltier, T.R., 2007. *Information security risk analysis, second ed*., Auerbach Publications, Boca Raton, FL, 2007.

Peslak, A.R. 2005. *The Importance of Information Technology: An Empirical and Longitudinal Study of the Annual Reports of the 50 Largest Companies in the United States*. Journal of Computer Information Systems, Vol. 45(3): 32-42.

Peterson, R. 2004. *Crafting Information Technology Governance*. Information Systems Management, Vol. 21(4): 7-22.

Petter, S., DeLone, W. and McLean, E.R. 2013. *Information Systems Success: The Quest for the Independent Variables.* Journal of Management Information Systems, Vol. 9(4): 7-62.

Pilat, D., 2003. *ICT and Economic Growth: Evidence from OECD Countries.* Industries and Firms, Organisation for Economic Co-operation and Development. Paris: OECD.

Pirounias, S., Mermigas, D. and Patsakis, C. 2014. *The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study.* Journal of Information Security and Applications, Vol. 19(4): 257-271.

Ponemon Institute LLC, 2012. *Cost of data breach study: United Kingdom.* Benchmark Research Conducted Ponemon Institute LLC.

Press, L. 1993. Before The Altair: The History of Personal Computing. Communications of the ACM, Vol. 36(9): 27-33.

Reuters. 1999. *Hershey haunted by computer glitch*, CNET News.com, 29 October.

Roberts, H. 1967. *Statistical versus clinical prediction of the stock market*, Unpublished manuscript.

Roberts, L.G. and Wessler, B.D. 1970. *Computer Network Development To Achieve Resource Sharing.* In Proceedings of the May 5-7, 1970, Spring Joint Computer Conference: 543-549.

Roberts, H.E. and Yates, W. 1975. *Altair 8800 Minicomputer*. Popular Electronics, Vol. 7(1):33-38.

Rojas, R. 1997. *Konrad Zuse's legacy: the architecture of the Z1 and Z3*. IEEE Annals of the History of Computing, Vol. 19(2): 5-16.

Ross, D.T. and Rodriguez, J.E. 1963. *Theoretical foundations for the computer-aided design system.* In Proceedings of AFIPS Spring Joint Computer Conference 23: 305-322.

Rosen, S. 1990. The Origins of Modern Computing. ACM Computing Reviews, Vol. 31(6): 449-481.

Rowley, J. 2007. *The Wisdom Hierarchy: Representations of the DIKW Hierarchy*. Journal of Information Science, Vol. 33(2): 163-180.

Rubenstein, A.H. and Geisler, E. 1990. *The Impact of Information Technologies on Operations of Service Sector Firms.* in Bowen, D.E., Chase, R.B., Cummings, T.G. and Associates (Eds), Service Management Effectiveness, Jossey-Bass, San Francisco, CA

Said, O. and Masud, M. 2013. *Towards Internet of Things: Survey and Future Vision.* International Journal of Computer Networks (IJCN), Vol. 5(1): 1-17.

Salmela, H. 2008. *Analysing business losses caused by information systems risk: a business process analysis approach.* Journal of Information Technology, Vol. 23(3): 185-202.

Sauer, C. 1993. *Why information systems fail: a case study approach*. Alfred Waller Ltd., Publishers.

Schmidt, R., Lyytinen, K. and Mark Keil, P.C. 2001. *Identifying software project risks: An international Delphi study.* Journal of management information systems, Vol. 17(4): 5-36.

Scott, J.E. and Vessey, I. 2000. *Implementing enterprise resource planning systems: the role of learning from failure.* Information systems frontiers, Vol. 2(2): 213-232.

Scott, J.E. and Vessey, I. 2002. *Managing Risks in Enterprise Systems Implementations.* Communications of the ACM, Vol. 45(4): 74-81.

Shah, R. and Shin, H., 2007. *Relationships among Information Technology, Inventory, and Profitability: An Investigation of Level Invariance Using Sector Level Data.* Journal of Operations Management, Vol. 25(4): 768-784.

Short, J.E., Bohn, R.E. and Baru, C. 2011. *How Much Information? 2010 Report On Enterprise Server Information.* UCSD Global Information Industry Center: 1-38.

Smith, H. and Fingar, P. 2003. *IT doesn't matter--business processes do: a critical analysis of Nicholas Carr's IT article in the Harvard business review.* Meghan-Kiffer Press.

Smith, K.T., Smith, M. and Smith, J.L. 2010. *Case Studies of cybercrime and its impact on marketing activity and shareholder value.*

Solic, K., Ocevcic, H. and Golub, M. 2015. *The Information Systems' Security Level Assessment Model Based On an Ontology and Evidential Reasoning Approach.* Computers & Security, Vol. 55: 100-112.

Souppaya M. P, Scarfone K., Hoffman P. 2011. *Guide to security for full virtualization Technologies.* NIST: Special Publication. Vol. 800(125). DIANE Publishing.

Spanos, G. and Angelis, L. 2016. *The impact of information security events to the stock market: A systematic literature review.* Computers & Security, Vol. 58: 216-229.

Stare, M., Jaklič, A. and Kotnik, P. 2006. *Exploiting ICT Potential in Service Firms in Transition Economies.* The Service Industries Journal, Vol. 26(03): 287-302.

Stratopoulos, T. and Dehning, B. 2000. *Does Successful Investment In Information Technology Solve The Productivity Paradox?* Information & Management, Vol. 38(2): 103-117.

Strong, D.M. and Volkoff, O. 2010. *Understanding Organization—Enterprise System Fit: A Path to Theorizing the Information Technology Artifact*. MIS Quarterly, Vol. 34(4): 731-756.

Subramani, M. and Walden, E. 2001. *The impact of e-commerce announcements on the market value of firms.* Information Systems Research, Vol. 12(2): 135-154.

Sun, L., Srivastava, R.P. and Mock, T.J. 2006. *An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions.* Journal of Management Information Systems, Vol. 22(4): 109-142.

Tarafdar, M. and Gordon, S.R. 2007. *Understanding the influence of information systems competencies on process innovation: A resource-based view*. The Journal of Strategic Information Systems, Vol. 16(4): 353-392.

Telang, R. and Wattal, S. 2007. *An empirical analysis of the impact of software vulnerability announcements on firm stock price.* IEEE Transactions on Software Engineering, Vol. 33(8): 544-557.

Tsai, C.W., Lai, C.F., Chiang, M.C. and Yang, L.T. 2014. *Data mining for Internet of Things: A survey*. IEEE Communications Surveys and Tutorials, Vol. 16(1): 77-97.

Tarn, J.M., Yen, D.C. and Beaumont, M. 2002. *Exploring the Rationales for ERP and SCM Integration.* Industrial Management & Data Systems, Vol. 102(1): 26-34.

Wailgum, T. 2005. *University ERP: Big Mess on Campus*. CIO Magazin, May 1.

Wailgum, T. 2009. *10. Famous ERP Disasters, Dustups And Disappointments*. CIO Magazin, March 24.

Wallace, L., Keil, M. and Rai, A. 2004. *Understanding software project risk: a cluster analysis*. Information & Management, Vol. 42(1): 115-125.

Wilcox, S. and Brown, B. 2004. *Risk Assessment, Risk Management, and the HIPAA Security Rule: A Matter Of Life And Death*. Journal of Health Care Compliance, Vol. 6(4): 43-45.

Willis, H. T. and Willis-Brown, A. H. 2002. *Extending the value of ERP*. Industrial Management & Data Systems, Vol. 102(1): 35-38.

Wilkinson, A. 1998. *Empowerment: Theory And Practice*. Personnel Review, Vol. 27(1): 40-56.

Urgo, M.A. 1996. *Computers and Productivity: Analysis Of Current Literature and Some Significant Issues.* Business Information Review, Vol. 13(3): 195-198.

Yayla, A.A. and Hu, Q. 2011. *The impact of information security events on the stock value of firms: The effect of contingency factors.* Journal of Information Technology, Vol. 26(1): 60-77.

Yeo, K.T. 2002. *Critical failure factors in information system projects.* International Journal of Project Management, Vol. 20(3): 241-246.

Yue, W.T., Çakanyıldırım, M., Ryu, Y.U. and Liu, D. 2007. Network Externalities, Layered Protection and IT Security Risk Management. Decision Support Systems, Vol. 44(1): 1-16.

Verizon. 2012. *Data Breach Investigations Report.*

Yen, D.C., Chou, D.C. and Chang, J. 2002. *A Synergic Analysis for Web-Based Enterprise Resources Planning Systems.* Computer Standards & Interfaces, Vol. 24(4): 337-346.

Yu, C., Xu, X. and Lu, Y., 2015. *Computer-İntegrated Manufacturing, Cyber-Physical Systems And Cloud Manufacturing–Concepts And Relationships*. Manufacturing Letters, Vol. 6: 5-9.

Von Krogh, G. 2002. *The communal resource and information systems*. The Journal of Strategic Information Systems, Vol. 11(2): 85-107.

Zeithaml, V.A., Parasuraman, A. and Berry, L.L. 1990. *Delivering Quality Service: Balancing Customer Perceptions and Expectations.* The Free Press, New York, NY.

Zhang, Y., Vin, H., Alvisi, L., Lee, W. and Dao, S.K. 2001. *Heterogeneous networking: a new survivability paradigm.* In Proceedings of the 2001 workshop on New security paradigms (pp. 33-39). ACM.

Zheng, S., Yen, D.C. and Tarn, J.M. 2000. *The new spectrum of the cross-enterprise solution: the integration of supply chain management and enterprise resources planning systems*. Journal of Computer Information Systems, Vol. 41(1): 84-93.