Private data management pitfalls: the implications on the online organisations

Name: Stavros Pontikis

Executive Summary

Data breach incidents are constantly rising and affecting a large number of online organisations. These incidents are having as a result a strong financial and reputational impact upon the implicated companies.

The purpose of this business report is to analyse this financial impact by evaluating the unexpected changes on the exposed company’s stock market price. The methodology used to identify the impact of an event on the market value of the company is the event study methodology. An estimation window of 121 trading days was used in order to calculate the expected return of those companies in the announcement day of the incident.

Using a sample of 31 incidents from 2004 to 2016, this study finds that 71% of the online firms’ market values reacted negatively on the announcement day of a data breach incident. More precisely, the companies in the entertainment industry and the data breaches that included confidential data proved to have the most significant negative reaction.

These incidents also set a major danger for damaging the reputation and the brand image of the companies exposed. Hence, the management, security and privacy of the private data stored online should be a priority for the online organisations as a management pitfall could potentially have catastrophic results.

Keywords: Online organisations, digital transformation, digital impact, data breach, stock market impact, digital news, digital world

Table of Contents

List of Tables iii

List of Figures v

CHAPTER ONE: INTRODUCTION.. 1

1.1 Introduction 1

1.2 Background 2

1.3 Research Objectives 4

1.4 Chapter Summary 5

CHAPTER TWO: LITERATURE REVIEW 6

2.1 Chapter Overview.. 6

2.2 Importance of the data stored online 6

2.3 Online security and privacy 7

2.4 Data breach methods 7

2.5 Data security and protection practices 9

2.6 Data breach consequences... 10

2.6.1 Financial Impact.. 11

2.6.2 Reputational Impact.. 13

2.7 Chapter Summary 14

CHAPTER THREE: RESEARCH METHODOLOGY................................ 15

3.1 Chapter Overview.. 15

3.2 Event Study Methodology 15

3.3 Data collection... 17

3.4 Selection criteria and event windows 17

3.5 Chapter Summary 18

CHAPTER FOUR: ANALYSIS 19

4.1 Chapter Overview 19

4.2 Data Analysis 19

4.3 Event Study Analysis 23

4.4 Chapter Summary 25

CHAPTER FIVE: DISCUSSION OF RESULTS 26

5.1 Chapter Overview 26

5.2 Full sample results 26

5.3 Analysis of the impact by category 29

5.3.1 Stock market impact by type of industry 29

5.3.2 Stock market impact by year of data breach 31

5.3.3 Stock market impact by sensitivity of data 32

5.4 Chapter Summary 33

CHAPTER 6 CONCLUSION 34

6.1 Chapter Overview 34

6.2 Limitations 34

6.3 Further Research 34

6.4 Conclusion 35

References 37

Bibliography 45

Appendices 46

Appendix A: E-Commerce Success Model 46

Appendix B: Ethical Approval 48

Appendix C: Full sample of the companies 49

List of Tables

Table 1: Reputational and financial costs 4

Table 2: Data breach methods and number of organisations affected....... 9

Table 3: Results of previously conducted event studies 13

Table 4: Incidents separated by type of industry they are serving 20

Table 5: Incidents separated by year 21

Table 6: Incidents separated by the type of the data sensitivity 22

Table 7: Comparison with other studies.. 29

Table 8: ARR and CAAR results by industry serving 29

Table 9: AAR and CAAR results by year of data breaches...................... 31

Table 10: Data Breaches full sample 52

List of Figures

Figure 1: Anthem's stock price reaction 3
Figure 2: Timeline of the event study 18
Figure 3: Stock Market Return from Excel 23
Figure 4: Calculation of the Expected Return using the market model 25
Figure 5: Calculation of the Abnormal Return 25
Figure 6: Calculation of the CAR values Excel 25
Figure 7: ARR and CAAR results for event window (-1, 12) 27
Figure 8: ARR and CAAR results for event window (-10, 12) 28
Figure 9: CAAR results by industry for event window (-1, 12).................. 30
Figure 10: Netflix stock market reaction.. 30
Figure 11: CAAR results by sensitivity of data 32
Figure 12: E-commerce success model.. 46
Figure 13: Ethical Approval 48

CHAPTER ONE: INTRODUCTION

1.1 Introduction

It was three years ago when the biggest scandal in the history of the internet was revealed and people got terrified by the dangers the World Wide Web hides. It was revealed that the National Security Agency of the USA (NSA) was using a surveillance software called “PRISM’ to collect private information from the users of nine multinational companies. Microsoft, Apple, AOL, Yahoo, Facebook and Google were some of the implicated companies (The Guardian, 2013). While this incident was about to be forgotten, the well-known website “Myspace” confirmed that 360 million personal records were stolen and published online on May of 2016, setting a new record in the data breach events history (TechCrunch, 2016). It is estimated that the number of similar incidents will steadily increase in the future and in combination with the exponential increase of the data stored online a potential cyber-attack to an organisation will expose massive volumes of private data (Digital Guardian, 2015).

These incidents generated for the information technology (IT) and management, a new concern named as security and privacy, which is considered as one of the main issues of the digital age (Luftman et al., 2013). In regards to that, companies are investing a lot in the IT security, aiming to create strategies in order to protect the privacy of the personal data stored online, also called big data, striving to minimise the risk of information being leaked (Bandyopadhyay et al., 2012).

However, lots of data management pitfalls occurred in the past, causing data leakage online and developing contemporary issues for the implicated organisations that are being heavily discussed in the news, generating trust issues for the consumers and creating the feeling of insecurity and vulnerability (Campbell, Edgar & Stonehouse, 2011).

As a result, these situations have a strong impact on the operation of the organisation, causing possible negative reaction of their stock market price, additional expenses to cover any damages to the users enmeshed and set in danger the reputation of the companies exposed (Campbell et al., 2003).

The aim of this business report is to analyse the impact of private data leakage incidents on the operation of the online organisations and to explore the strategies that are implemented by the companies in order to restore their reputation levels and improve the management of the private data.

1.2 Background

Data breach or data leak is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so (U.S department of health and human services, p.2, 2015). The data breaches expose personal information stored online that may involve health information, personal information (emails, phone numbers, credit card numbers) and even companies strategies (Gordon and Loeb, 2002).

These events, started to exist, after the wide creation of the e-commerce world, that forced the companies to a digital transformation process and websites such as Amazon or eBay were born with the aim of creating a digital online trading system (Laudon and Traver, 2013). There are references of data breaches on high-profile firms such Amazon from 2000 (Cavusogly, Mishra and Raghunathan, 2004), however, the first examined event of this study is dated back in 2004, where the servers of the AOL Inc. hacked, exposing 92 million customer accounts in public, causing a lot of discussion in the media about online privacy and security (CNN Money, 2004). From that time onwards, the data disclosure incidents started to increase and according to the Identity Theft Resource Center report (2015), these incidents increased by 8.1% from 2014.

Based on the e-commerce success model (Appendix A), security and privacy issues are linked with *Trust* which is one of the six dimensions that contribute to the success of a company in the online world. Through this framework, it is demonstrated that the lack of *Trust* due to low-security levels, leads to avoidance of use of the services offered and lack of e-commerce satisfaction (Molla and Licker, 2001).

It is identified that the damage on customers' trust may affect the financial performance of the organisation involved. More precisely, 86.5% of consumers stated that they would not do business with an organisation that had suffered from a data breach incident involving personal information such as credit card numbers (Semafone, 2014). Additionally, the average cost from direct and indirect expenses incurred by the organisation, such as discounts to the users, hotline support or losses coming from customer turnover, is estimated to be $4 million per breach (Ponemon Institute, 2016).

Furthermore, the financial consequences are also anticipated in the sales and the market value of the enmeshed company. For example, the Target Corporation has reported that after the massive security breach of 70 million private information, the sales dropped by 46% from the same quarter the year before (Manworren, Letwat and Daily, 2016). Another noticeable example is the impact on the Anthem's stock price the following day of the announcement of a data breach that caused a negative return of 1.1% (Bloomberg, 2016).

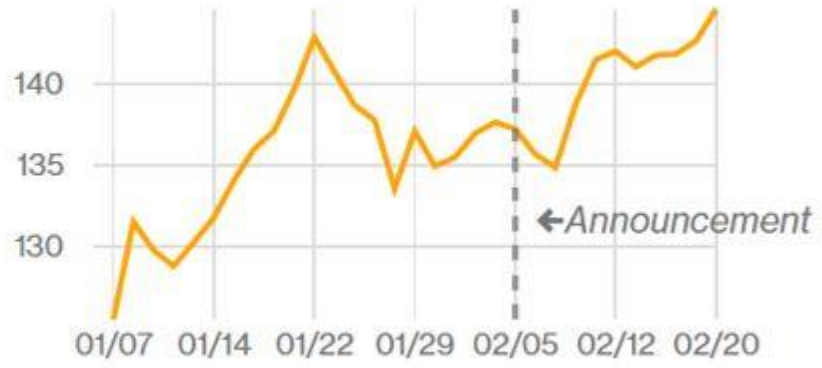


Figure 1: Anthem's stock price reaction (Bloomberg, 2016)

Finally, the most hazardous consequence in the operation of the organisation, causing the strongest financial impact is the reputation and brand damage. It is not only considered that the data breach is the first threat in terms of reputational impact, but also that the reputation and brand damage might cost to the organisation more than $5.4 million for the next two years (Forbes Insights, 2014).

Common threats ranked in terms of reputational impact (on scale of 1-7)		**Financial impact by cost category (in millions of dollars)**	
Data Breach / Data theft	5.5	**Reputation and brand damage**	$5.7
Natural or Manmade disasters	5.2	Lost Productivity	$3.9
IT system failure	4.3	Lost Revenue	$3.2
Data Loss	4.0	Forensics	$2.5
Cyber security breach	3.8	Technical Support	$2.3
Human Error	2.6	Compliance Regulatory	$1.6

Table 1: Reputational and financial costs (Forbes Insights, 2014)

1.3 Research Objectives

Considering the previously mentioned incidents, it is indisputable that the information stored online are valuable and that a data breach incident has crucial consequences on the operation of an organisation. Thus, the primary objectives of this business report are:

- To develop an understanding of the value of the private data stored online and the ways and practices to protect it.
- To explain the financial, the reputational and brand image damage of an organisation after a data breach incident.
- To analyse the financial impact upon an implicated organisation with a data breach event, by examining the stock market prices of the exposed companies using the event study methodology.

- To discuss the potential strategies created from the companies to protect the customers, earn back they trust, increase the security levels and restore the company's reputation.

1.4 Chapter Summary

The purpose of this chapter was to briefly clarify some basic terminology and to introduce the background of this business report. Chapter 2 explains the importance of online security and analyses some issues and practices used to protect the private data. Chapter 3, deepens on the financial and reputational consequences of mismanagement of the private data. Chapter 4, presents the research methodology used and the data collection process. Chapter 5 explains the variables and the analysis process. Chapter 6 presents the results and discussion. Chapter 7 illustrates the limitations of the research.

CHAPTER TWO: LITERATURE REVIEW

2.1 Chapter Overview

The aim of this chapter is to indicate the value of the private data stored online and the various types of data breaches. Moreover, this chapter also presents the strategies used in order to protect the data stored online. Finally, the last sub-chapters of the literature review explain in depth the financial and reputational consequences that derive from the data breach incidents.

2.2 Importance of the data stored online

As previously mentioned, consumers' *Trust* towards an online organisation is linked with the security and privacy of the personal information. The e-organisations, not only track the movements of theirs users, save their personal settings so as to improve their online experience (Gurau, Ranchhod and Gauzente, 2003), but also store a huge amount of personal data such as e-mails or credit cards numbers to facilitate the online processes and increase the e-consumers' satisfaction levels (Wang and Liao, 2008).

The stored data online is analysed by the companies in order to increase their sales revenues from targeted advertising of products and services. Additionally, this analysis of the data stored may have as a result the introduction of new products or services that might increase the market share of a company (BCG, 2012). Hence, the value of the data stored online can be estimated from the number of satisfied consumers from the ease of use of a website, the earnings of the advertising companies and the companies that are being successfully advertised and have the possibility of expansion of the market share (Liem and Petropoulos, 2016).

Therefore, the companies introduced a new term in their business ethics entitled as "big data" ethics. This term is setting responsible the organisations for the management and protection of their consumers' private information, as a data management pitfall could cause a possible disaster on the operation of the company as it would create to the users Trust issues and avoidance of use of the implicated organisation. (Zimmer, 2010).

2.3 Online security and privacy

The security and privacy of the online data are nowadays one of the main issues for the e-organisations. Firms are constantly investing on increasing the security levels and even creating departments for Cyber Security Management (CSM). Cybersecurity management is defined as the use of strategies, techniques and tools to protect the cyber infrastructure from a possible attack that will cause a leak of the online stored data (Kumar, Srivastava and Lazarevic, 2005). The term is also integrated with the information security, which is responsible for ensuring security and minimizing the impact from security pitfalls (Anderson, 2003).

The companies should continuously improve those two concepts, as a security incident may lead to the disclosure of confidential data or disaster of data stored online (Solms and van Niekerk, 2013). Additionally, these incidents can destroy the already mentioned value of the data from the consumers’ perspective. A potential data breach would be considered as unprofessional for the organisations exposed, while the disaster of data can create usability issues to the users.

It is estimated that the total number of records breached in 2015, is over 169.07 million, which means that every day 0.46 million personal records could be breached. (Statista, 2015). Thus, firms should use practices to protect from these events. The best way to avoid a cyber security attack is to identify the breach methods that are being implemented and be prepared to defend them (Gemalto, 2015).

2.4 Data breach methods

A recently conducted survey on information security breaches, states that the types of data breaches varies from each case, but 90% of large organisations reported that they suffered any form of security breach.

The main methods of data breaches and the total number of organisations suffered from those based on 939 responses from large and small organisations in the UK can be seen in the table below (HM Government, 2015):

Methods of data breach	Description	Incidents
Infection by viruses or malicious software (HACK)	This is the most common data breach method. It involves pieces of software that are specially made to take control from the user and access to system resources (Pektaş and Acarman, 2013).	Large organisations: 84 Small organisations: 63
Theft or fraud involving computers (PHYS or PORT or STAT)	This category is separated in three sub-categories. All categories involve lost or stolen device that contained the data leaked. The acronyms stand for: PHYS: documents, physical content PORT: portable devices such as laptops, USBs STAT: stationery devices (Ayyagari, 2012).	Large organisations: 55 Small organisations: 6
Other incidents caused by staff (DISC)	This category includes the following mistakes that are caused by staff: • Unauthorized access to a database or a network	Large organisations: 81 Small organisations: 27

	• Share of private passwords with other employees • Mistakes in the transfer of data between servers (Cisco, 2016).	
Attacks by an unauthorized outsider (excluding hacking attempts) (CARD)	These methods are correlated with fraud to mainly obtain credit card information. The frauds are mainly by: • Fraud organisations that imitate the original with the aim to steal the personal information of certain targeted people • Customers impersonated other people using a fake identity. (HM Government, 2015)	Large organisations: 70 Small organisations: 35

Table 2: Data breach methods and number of organisations affected (HM Government, 2015)

It is estimated that nowadays only a single attack upon one company can evoke a loss of hundreds of thousands records which is considered as a catastrophic event for the targeted company. For this reason, the companies should create the right strategies to protect the personal data (Digital Guardian, 2015).

2.5 Data security and protection practices

There is not a clear framework that would guarantee the safety of the information stored online (Mearian, 2016). In the past, companies believed that the information are only protected when stored offline. However, this method hides one major threat, the threat of losing the data due to a natural disaster or a hardware failure (LaChapelle, 2012). Data loss ranked in the fourth position of the reputational damage factors (Table 1.1). Thus, to increase not only the protection of data, but also the security for unauthorized staff that might have access to the offline database, firms adopted the use of cloud computing. Cloud computing, facilitated the transfer, edit and share of data with the use of online servers but it also created security issues for the companies. (Chen and Zhao, 2016).

The first suggested practice to secure the data in the cloud is to classify it and secure it in three different sections: Public, Private and Limited access (Sood, 2012). Furthermore, firms should anonymise and encrypt the confidential data stored in the Private and Limited Access sections. Using this method, the data would be possible to be read only by authorized staff that can decrypt the stored information (Lafuente, 2015). In addition, any company that stores personal data should ensure that all portable devices are encrypted and store those devices when they are idle (Walker-Osborn, Fitzsimons and Ruane, 2013).

Finally, companies have to ensure that they use Cyber Essentials Schemes such as firewalls or anti-viruses and that the staff is well trained are aware of the Data Protection Act 1998. More precisely, staff members that have access to an electronic device, should be trained to keep their passwords secure, to encrypt their and their customers' information and continuously update their knowledge on cyber security (ICO, 2016).

2.6 Data breach consequences

The total consequences of a data breach incident to an organisation are not clear. Some studies focus on the legal issues for the companies, such as fines or penalties (Itgovernance, n.d.), other studies focused on the direct costs such as expenses to upgrade the security or offers of discounts to the victims (Fortune, 2016), whereas other studies focus on the financial costs examining the market value, and others to the reputational damage caused by these incidents (Ponemon

Institute, 2016). The main focus of this business report would be in analysing in depth the impact on the stock market using the event study methodology and create an understanding of the size of the impact of the reputational damage.

2.6.1 Financial Impact

It is identified from previous studies that the announcement of a data breach incident provokes strong financial impact on the exposed company (Campbell et al., 2003), however, the true cost of these incidents is still manifold (Cavusoglu, Mishra and Raghunathan, 2004). Ponemon institute, estimates the average cost of a data breach to be around $4 million (Ponemon Institute, 2016), whereas other studies have found that the cost varies from 3 thousand to 3 million, depending the size of the company (HM Government, 2015), however, there are some cases that the cost overcome these results. For example, the cost of the hacking attempt to Sony's PlayStation network is estimated to $170 million (Washington Post, 2014) whereas the same cost for the Target company is estimated to $39 million, without the losses of revenues from the drop of sales (Garcia, 2015).

Furthermore, a big percentage of researchers focused their interest on investigating the stock market reactions after the publicity of the breach event in the news (Campbell et al., 2003; Schatz and Bashroush, 2016; Andoh-Baidoo, Amoako-Gyampah and Osei-Bryson, 2010). These studies have been conducted, using the event study methodology, as it can measure the impact on the market value of a company that experienced a specific event. More precisely, this methodology indicates that a certain event will impact immediately the security prices of the firm involved, in comparison with the rest marketplace (MacKinlay, 1997).

Although there is a big variety in the results of those studies, most of them have found that there is a negative reaction upon the market price after the announcement of the event. This variety emerges from the different sample sizes and event windows used. Some studies have found that the average impact on the market value of the company was 2.1% which is estimated as a $1.65 billion loss

(Cavusoglu, Mishra and Raghunathan, 2004). Other studies proved that the impact is insignificant and the stock recovers to the previous levels immediately. For example, the stock market of the Home Depot business experienced a small impact after the announcement of the event but a few week later showed 21% increase (Harvard Business Review, 2015). A summary of the results from similar studies can be seen below:

Authors	**Sample Size / Event Window**	**Results**
(Schatz and Bashroush, 2016)	25 organisation (50 Events) Event window: (-2,2)	This research finds minor significance in the companies involved in one incident, but it becomes significant if the same company is involved twice in a data breach incident
(Das Mukhopadhyay and Anand, 2012)	101 Events Event windows: (-1,1) , (-1, 3)	Findings of negative influence on the stock market of the company, but no impact on the parent company if the implicated company is subsidiary
(Morse, Raval and Wingender, 2011)	306 Events Event window (0,1)	This study states that there is an impact on the market value, however, it is not significant. It is possible if the event window was bigger to be more significant.

(Andoh-Baidoo, Amoako-Gyampah and Osei-Bryson, 2010)	41 Events Event window (-1,1)	This research has as a result that within the event window, the companies influenced negatively on average 3.18% of their market value. Additionally, this research proves that investors lose their trust towards the organisations.
(Gatzlaff and McCullough, 2010)	77 Events Event window (0,1)	Using different additional variables, such as the method of data breach, industry's reactions etc. The research finds that the stock market responds negatively and this impact is stronger to companies with growth opportunities

Table 3: Results of previously conducted event studies

2.6.2 Reputational Impact

As mentioned in Chapter 1, the strongest financial impact is anticipated by the damage of the reputation of the company, as the data breaches considered as the first threat of the damage of the reputation (Table 1). The loss of reputation may lead to a decrease in the future sales or even complete avoidance of the use of the services of the implicated firms (Kannan, Rees and Sridhar, 2007; Campbell et al., 2003).

However, the potential relationship between reputation damage and data breaches has been analysed by a limited number of researchers. The main methodology used to analyse this relationship based on the sentiment analysis from comments found on the social media. The main process is to distinguish the content of the comments as positive or negative and measure the sentiment polarity in the event window of the announcement of the data breach.

$$sentiment\ polarity = \frac{\#possitivewords - \#negativewords}{\#possitivewords + negativewords}$$

(Sinanaj, Muntermann and Cziesla, 2015)

This value can be used in the event study methodology to evaluate the impact on the reputation of the company after a data breach incident (Sinanaj, Muntermann and Cziesla, 2015). This method validates that the reputational damage in true and companies should be prepared to react to such events as soon as possible in order to minimize that cost (Drinkwater, 2016).

Finally, other studies verify that a security breach can have an impact on both the market prices and the reputation of the companies, but there are no clear results of the size of the reputational impact (Arcuri, Brogi and Gandolfi, 2016). However, the analysis of the reputational damage is out of the scope of this business report as the identification of the sentimentality of the comments is analysed with the use of purchased social media analytics tools such as the Hootsuite software (Hootsuite, 2016).

2.7 Chapter Summary

This chapter developed a clear understanding of the value of the private data stored online from the customers’ and the company’s perspective. Furthermore, the chapter demonstrated the data breach methods and data securities practices in order to avoid those incidents. Finally, the literature review of the financial and reputational consequences takes place in order to create an image of how serious the consequences of a data breach incident on a company are.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Chapter Overview

The purpose of this chapter is to create an understanding of the research methodology used to analyse the impact on the market value of a company implicated in a data breach event. Moreover, it is explained the data collection process, as well as the examination of the collected data in order to be eligible to be analysed.

3.2 Event Study Methodology

As mentioned in literature review chapter and based on previously conducted quantitative studies the most accurate methodology to inspect the influence of an event on the company's stock prices is the event study methodology (MacKinlay, 1997). More precisely, this method is investigating the short-term changes of the security prices of the company during the observation window of the announcement of the incident (Kothari and Warner, 2004).

The evaluation of the daily impact of each event is measured using the abnormal return (AR_{it}), which identifies the unexpected changes in the stock prices that are associated with an event. The calculation of the abnormal return on a certain day (t) is calculated as:

$$\boldsymbol{AR_{it} = R_{it} - E(R_{it}|X_t)} \qquad \text{(MacKinlay, 1997)}$$

Where:

- R_{it} = the Actual Return of the stock market during the observation window.
- $E(R_{it}|X_t)$ = the Normal Return or Expected Return of the stock market, based on the previous returns.
- X_t = additional variable for the better estimation. This variable can be constant using the "*constant mean return model"* or it can represent the market return using the "*market model*". The market model

assumes a stable linear relation between the market return and the security return.

The expected return emerges from the use of the market model regression that can calculate the expected stock return on a day (t):

$$\boldsymbol{R_{it} = a_i + \beta_i R_{mt}}$$ **(**MacKinlay, 1997)

Where: R_{mt} is the return of the market portfolio (S&P 500) and a_i, β_i are parameters of the linear market model equation (a_i=intercept, β_i=slope) that are estimated based on over 120 days the previous return prices.

Moreover, in order to support the results and to create a visual image of the total impact on the stock price, the use of the cumulative abnormal returns (CAR) is necessary. The calculation of the CAR is created by adding the abnormal returns for the event window:

$$\boldsymbol{CAR_s = \sum_{i=-1}^{10} \overline{ARi}}$$ (Arcuri, Brogi and Gandolfi, 2014)

However, before calculated the abnormal return and the cumulative abnormal return the following steps should be applied:

i. Selection of the events of interest and identification of the security prices (stock prices) for the examined companies over the event period.
ii. Definition of the event window to identify unexpected changes
iii. Determination of whether the company fulfils the selection criteria
iv. Collection of the market portfolio prices for each event individually
v. Calculation of the market model parameters based to identify the expected return
vi. Calculation of the abnormal returns (AR_{it})
vii. Calculation of the cumulative abnormal returns (CAR_s)
viii. Evaluation and presentation of the results.

3.3 Data collection

This study is focused on the data breach events that happened in the online organisations from 2004 to 2016. The data collection process started after the submission and approval of the Ethics Form (Appendix B). As mentioned in this form, the data used for the analysis is secondary data found online. More precisely, the data collection process was based on the data sets found on the Privacy Rights Clearinghouse and the Identity Theft Resource Center websites. The original databases included all the data leak events with more than 30,000 records stolen, so the original data set created had 224 data breach events. Additional events were found in the Bloomberg database and in other online sources. Afterwards, the events of this database were clarified in order to include only the events that concern the online organisations, diminishing the database to 55 events. Finally, the dates of the announcement for each of those events were retrieved by searching each event individually and this date was set as day “0” in the event window.

3.4 Selection criteria and event windows

The selection criteria for these 55 events were to trade on the NASDAQ or the NYSE markets in order to calculate the R_{mt} value and not to be private. After a detailed research for each event individually to see whether they fulfill this requirement, the final sample of this study includes 31 events (Appendix C).

Furthermore, to calculate the abnormal returns using the market model, a time-series with the daily stock price and the daily price of the portfolio should be created. Based on MacKinlay, the timeline for a successful event study should have an estimation window, and event window and a post-event window.

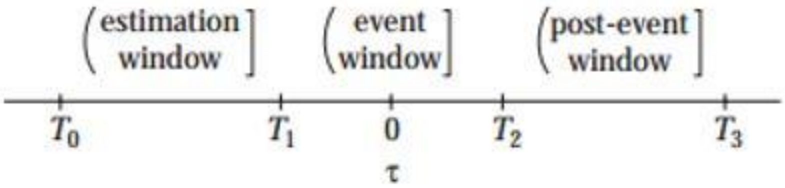


Figure 2: Timeline of the event study

There is not a certain instruction for the length of each window, however, the estimation window should be over 120 days prior to the event window for the accurate calculation of the parameters a_i, β_i of the market model. The event window differs between the previous studies as mentioned in chapter 2, but although the shorter windows are easier in the calculation process, they also do not take into consideration the impact from later announced news (Konchitchki and O'Leary, 2011). Finally, the post-event window gives information on how fast the company would recover from this event, which is linked with the market efficiency (Kothari and Warner, 2006). For the purpose of this business report, the event window used is (-1, 12) in order to examine the impact 12 days after the announcement of the data breach incident.

3.5 Chapter Summary

This chapter explains the event study methodology, which is a reliable process to analyse the impact of a security breach event on the stock market of a company. Additionally, this chapter demonstrated the data collection method after the ethical approval from the University of Kent, and the selection criteria of the secondary data collected. The total sample for this study is 31 incidents, using an estimation window of 121 trading days (more than 140 solar days) and an event window of (-1,10) and (-1,12).

CHAPTER FOUR: ANALYSIS

4.1 Chapter Overview

This chapter will create an understanding of how the analysis has been conducted to identify a potential impact on the stock market of the 31 selected events. The following process has been done to all the incidents individually using the following two event windows: (-1, 12) and (-10, 12). The business report is accompanied by a DVD-ROM with the Excel file that was used for the total analysis.

4.2 Data Analysis

The event study analysis was conducted using the Microsoft Excel software. As mentioned in the previous chapter, the total database consisted by 224 events (Excel Spreadsheet: Original Database). Consequently, a new spreadsheet named as Event List was created, including the events that meet the selection criteria. This Spreadsheet includes the names of the organisations, the industry serving, the day of the announcement of the event, the method of beached used, the number of records leaked and the sensitivity of the data stolen.

In the beginning, the events were analysed individually (Excel Spreadsheet: "Event Study (-1, 12)" and "Event Study (-10, 12)" and then for a better understanding of the results, the events were separated and analysed in the following categories (Excel Spreadsheet: "Categories (-1, 12)", "Categories (-10, 12):

- By type of Industry
- By year of breach
- By sensitivity data

More precisely the events included in those categories are the following:

Industry	Companies (Number of times)	Number of Incidents
Communications	T-Mobile (2) Gmail Talk Talk Web.com	5
Entertainment	Netflix Sony PlayStation Network Sony Pictures	3
Media	AOL (4)	4
Retail	Zappos Target eBay VTech Amazon	5
Other	Monster.com (2) TripAdvisor	3
Social Network	LinkedIn (2) Tumblr Facebook (2) Myspace	6
Web Search	Yahoo voices Google Yahoo (2) Chrome	5

Table 4: Incidents separated by type of industry they are serving

Year	Companies (Number of times)	Number of Incidents
2004	AOL	1
2006	AOL	1
2007	Monster.com	1
2009	Monster.com	1
2010	Netflix	1
2011	Sony PlayStation Network Sony Pictures	2
2012	LinkedIn Yahoo voices Zappos	3
2013	Tumblr Facebook (2) Google LinkedIn Yahoo (2) AOL Chrome T-Mobile	10
2014	Target eBay AOL Gmail TripAdvisor	5
2015	T-Mobile VTech Talk Talk Web.com Amazon	5
2016	Myspace	1

Table 5: Incidents separated by year

Data Sensitivity	Companies (Number of times)	Number of Incidents
User’s Emails / Personal Information	AOL (2) Facebook T-Mobile Yahoo	5
User IDs, Passwords, E-mail address, Names Phone numbers and Demographic Data	Monster (2) Sony Pictures VTech Myspace	5
Personal Information, Passwords, Credit Cards	Sony PlayStation Network Netflix Zappos Chrome Target TripAdvisor Talk Talk Web.com	8
User IDs and Passwords	LinkedIn Yahoo Voice Tumblr eBay AOL Gmail T-Mobile Amazon	8
Chats / Emails	Facebook Google LinkedIn Yahoo AOL	5

Table 6: Incidents separated by the type of the data sensitivity

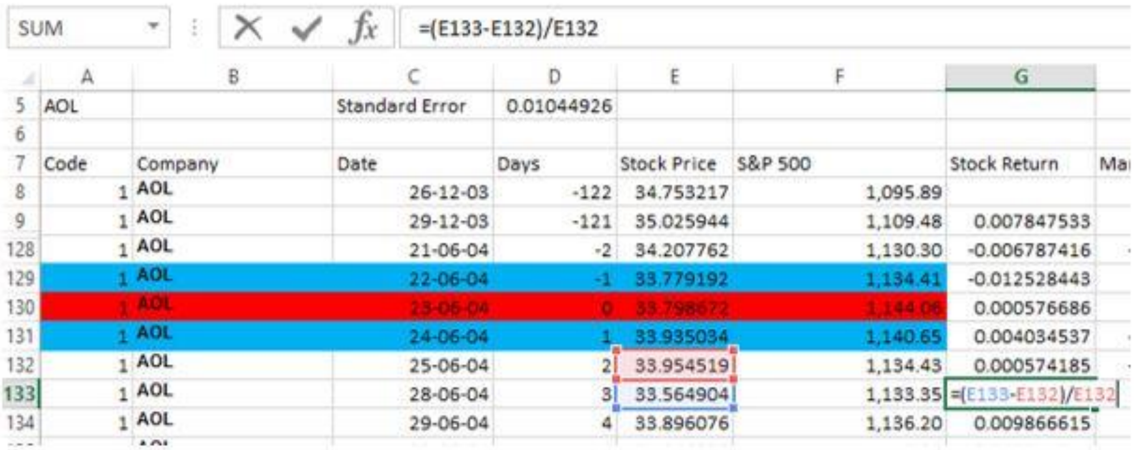
4.3 Event Study Analysis

The event windows used for the analysis were (-1, +12), (-10, 12) and the estimation window in order to calculate the expected return was 121 days prior to the event window. The first step was to collect for each event the stock prices and the market prices (S&P 500), using the Yahoo Finance, the Google Finance and the Bloomberg software.

The second step was to calculate the daily return of the stock and the return of the market for the total 133 days for each event by using the following function:

$$return = \frac{P_x - P_{x-1}}{P_{x-1}} \qquad \text{(Brooks, 2014)}$$

For example, in figure 3 it the calculation of the stock return for the day three is equal to the stock price at the day 3 minus the stock price of the previous day, divided by the previous day. The same process was used for the calculation of the market return.



=(E133-E132)/E132

	A	B	C	D	E	F	G	
5	AOL		Standard Error	0.01044926				
6								
7	Code	Company	Date	Days	Stock Price	S&P 500	Stock Return	Ma
8	1	AOL	26-12-03	-122	34.753217	1,095.89		
9	1	AOL	29-12-03	-121	35.025944	1,109.48	0.007847533	
128	1	AOL	21-06-04	-2	34.207762	1,130.30	-0.006787416	
129	1	AOL	22-06-04	-1	33.779192	1,134.41	-0.012528443	
130	1	AOL	23-06-04	0	33.798672	1,144.06	0.000576686	
131	1	AOL	24-06-04	1	33.935034	1,140.65	0.004034537	
132	1	AOL	25-06-04	2	33.954519	1,134.43	0.000574185	
133	1	AOL	28-06-04	3	33.564904	1,133.35	=(E133-E132)/E132	
134	1	AOL	29-06-04	4	33.896076	1,136.20	0.009866615	

*Figure 3: Stock Market Return from Excel (Spreadsheet (-1, 12))**

*In figure 3 the data from the day -120 to day -3 is hidden for better visibility of the process. The full analysis can be seen in the attached Excel file.

Consequently, using the market model "$R_{it} = a_i + \beta_i R_{mt}$" that assumes a stable linear relation between the market return and the security return, the Normal Return ($E(R_{it}|X_t)$ or Expected Return) was calculated for the event window. More precisely, to calculate the parameters a_i and β_i the process of linear regression has to be followed:

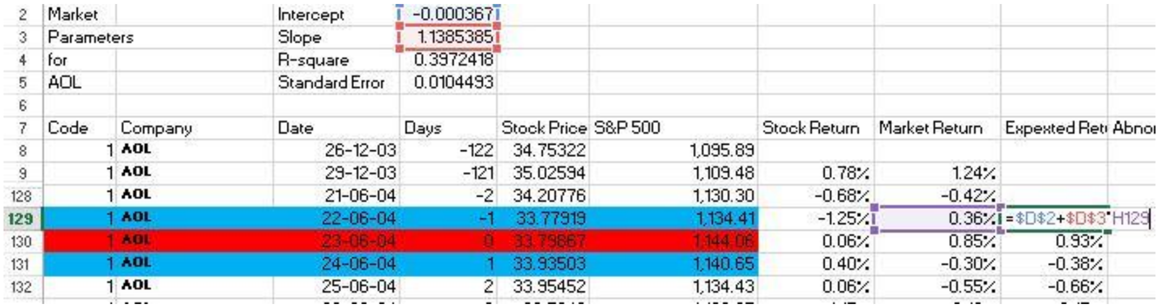
- Calculation of a_i: Use of the "intercept" function in Excel and assigning the returns of the stock market as the Dependent values (Y) and the returns of the market as the Independent values (X) of the linear regression model Y= a +bX.
- Calculation of β_i: Use of the "slope" function in Excel and assigning the returns of the stock market as the Dependent values (Y) and the returns of the market as the Independent values (X) of the linear regression model Y= a +bX.
- Additionally, using the same method and the functions "RSQ" and "STEYX", the calculation of the R-Square and the Standard Error (Pandis, 2016).

The next step of the event study method is the calculation of the abnormal return. As mentioned in the previous chapter, the function used for the calculation is:

$$AR_{it} = R_{it} - E(R_{it}|X_t)$$ (Kannan, Rees and Sridhar, 2007)

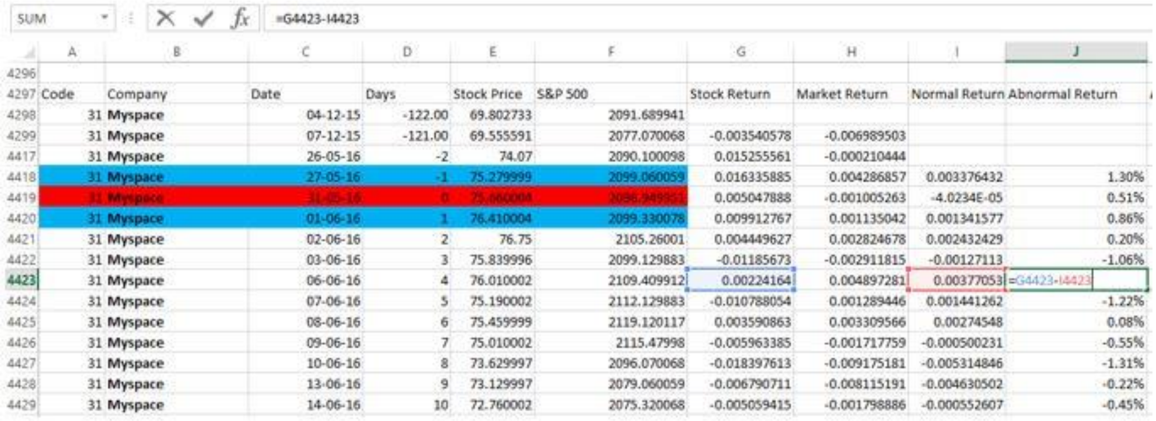
The subtraction of the Stock Return (R_{it}) minus the Expected Return ($E(R_{it}|X_t)$) in the event window and the post-event window is used to define the impact of the event in the stock market prices. If the result is negative then there is certainly an impact as the expected return would greater than the real stock return. Finally, the calculation of the CAR value takes place with the aim of creating a visual image of the total impact.

The three following Figures are presenting the calculation process as done in the Excel Spreadsheets:



2	Market		Intercept	-0.000367							
3	Parameters		Slope	1.1385385							
4	for		R-square	0.3972418							
5	AOL		Standard Error	0.0104493							
6											
7	Code	Company	Date	Days	Stock Price	S&P 500		Stock Return	Market Return	Expected Ret	Abnor
8	1	AOL	26-12-03	-122	34.75322		1,095.89				
9	1	AOL	29-12-03	-121	35.02594		1,109.48	0.78%	1.24%		
128	1	AOL	21-06-04	-2	34.20776		1,130.30	-0.68%	-0.42%		
129	1	AOL	22-06-04	-1	33.77919		1,134.41	-1.25%	0.36%	=$D$2+$D$3*H129	
130	1	AOL	23-06-04	0	33.79867		1,144.06	0.06%	0.85%	0.93%	
131	1	AOL	24-06-04	1	33.93503		1,140.65	0.40%	-0.30%	-0.38%	
132	1	AOL	25-06-04	2	33.95452		1,134.43	0.06%	-0.55%	-0.66%	

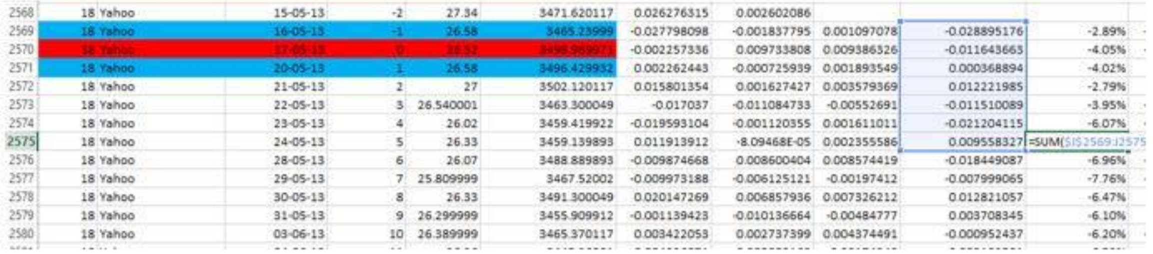
Figure 4: Calculation of the Expected Return using the market model Excel (Spreadsheet (-1, 12)



SUM | fx | =G4423-I4423

	A	B	C	D	E	F	G	H	I	J
4296										
4297	Code	Company	Date	Days	Stock Price	S&P 500	Stock Return	Market Return	Normal Return	Abnormal Return
4298	31	Myspace	04-12-15	-122.00	69.802733	2091.689941				
4299	31	Myspace	07-12-15	-121.00	69.555591	2077.070068	-0.003540578	-0.006989503		
4417	31	Myspace	26-05-16	-2	74.07	2090.100098	0.015255561	-0.000210444		
4418	31	Myspace	27-05-16	-1	75.279999	2099.060059	0.016335885	0.004286857	0.003376432	1.30%
4419	31	Myspace	31-05-16	0	75.660004	2096.949951	0.005047888	-0.001005263	-4.0234E-05	0.51%
4420	31	Myspace	01-06-16	1	76.410004	2099.330078	0.009912767	0.001135042	0.001341577	0.86%
4421	31	Myspace	02-06-16	2	76.75	2105.26001	0.004449627	0.002824678	0.002432429	0.20%
4422	31	Myspace	03-06-16	3	75.839996	2099.129883	-0.01185673	-0.002911815	-0.00127113	-1.06%
4423	31	Myspace	06-06-16	4	76.010002	2109.409912	0.00224164	0.004897281	0.00377053	=G4423-I4423
4424	31	Myspace	07-06-16	5	75.190002	2112.129883	-0.010788054	0.001289446	0.001441262	-1.22%
4425	31	Myspace	08-06-16	6	75.459999	2119.120117	0.003590863	0.003309566	0.00274548	0.08%
4426	31	Myspace	09-06-16	7	75.010002	2115.47998	-0.005963385	-0.001717759	-0.000500231	-0.55%
4427	31	Myspace	10-06-16	8	73.629997	2096.070068	-0.018397613	-0.009175181	-0.005314846	-1.31%
4428	31	Myspace	13-06-16	9	73.129997	2079.060059	-0.006790711	-0.008115191	-0.004630502	-0.22%
4429	31	Myspace	14-06-16	10	72.760002	2075.320068	-0.005059415	-0.001798886	-0.000552607	-0.45%

Figure 5: Calculation of the Abnormal Return Excel (Spreadsheet (-1, 12)



2568	18	Yahoo	15-05-13	-2	27.34	3471.620117	0.026276315	0.002602086			
2569	18	Yahoo	16-05-13	-1	26.58	3465.23999	-0.027798098	-0.001837795	0.001097078	-0.028895176	-2.89%
2570	18	Yahoo	17-05-13	0	26.52	3498.969971	-0.002257336	0.009733808	0.009386326	-0.011643663	-4.05%
2571	18	Yahoo	20-05-13	1	26.58	3496.429932	0.002262443	-0.000725939	0.001893549	0.000368894	-4.02%
2572	18	Yahoo	21-05-13	2	27	3502.120117	0.015801354	0.001627427	0.003579369	0.012221985	-2.79%
2573	18	Yahoo	22-05-13	3	26.540001	3463.300049	-0.017037	-0.011084733	-0.00552691	-0.011510089	-3.95%
2574	18	Yahoo	23-05-13	4	26.02	3459.419922	-0.019593104	-0.001120355	0.001611011	-0.021204115	-6.07%
2575	18	Yahoo	24-05-13	5	26.33	3459.139893	0.011913912	-8.09468E-05	0.002355586	0.009558327	=SUM($I$2569:I2575
2576	18	Yahoo	28-05-13	6	26.07	3488.889893	-0.009874668	0.008600404	0.008574419	-0.018449087	-6.96%
2577	18	Yahoo	29-05-13	7	25.809999	3467.52002	-0.009973188	-0.006125121	-0.00197412	-0.007999065	-7.76%
2578	18	Yahoo	30-05-13	8	26.33	3491.300049	0.020147269	0.006857936	0.007326212	0.012821057	-6.47%
2579	18	Yahoo	31-05-13	9	26.299999	3455.909912	-0.001139423	-0.010136664	-0.00484777	0.003708345	-6.10%
2580	18	Yahoo	03-06-13	10	26.389999	3465.370117	0.003422053	0.002737399	0.004374491	-0.000952437	-6.20%

Figure 6: Calculation of the CAR values Excel (Spreadsheet (-1, 12)

4.4 Chapter Summary

The purpose of this additional chapter was to explain in depth the event study analysis process, with the aim of creating a better understanding of the results. The software used for this process was completed with the use of Microsoft Excel Spreadsheets. For a better understanding of the results a CD-ROM with the Excel file is attached to this business report.

CHAPTER FIVE: DISCUSSION OF RESULTS

5.1 Chapter Overview

This chapter will present the results from the event study by using the following two event windows: (-1, 12), (-10, 12). The first part is the present the results of the average impact using the full sample and focus on some critical values around the event day 0 and the second part compares the impact in the previously mentioned for categories: by type of industry, by year, type of breach, and by the sensitivity of the data.

5.2 Full sample results

This section presents the results of all the 31 events that have been collected in the database. The results have been generated after conducted the event study methodology for each incident individually and the calculated the average of the abnormal returns and the cumulative abnormal returns in the event windows (Excel Spreadsheets: “Categories (-1, 12)”, “Categories (-10, 12)”).

The first result from the 31 data breach incidents, is that for an event window of (-1, 12) the 71% of the total samples’ abnormal returns are negative on the event day (day 0). The negative abnormal return indicates that the actual return is smaller than the expected return, which can be related to the publicity of the “bad” news of the data breach incident. However, using the event window (-10, 12) the percentage of negative abnormal returns decreases to 64.5%, because of the change of the event window size.

A better picture of the total impact can be created with the use of graphs for the average abnormal return (AAR) and the mean or cumulative average abnormal return (CAAR) in the following figure:

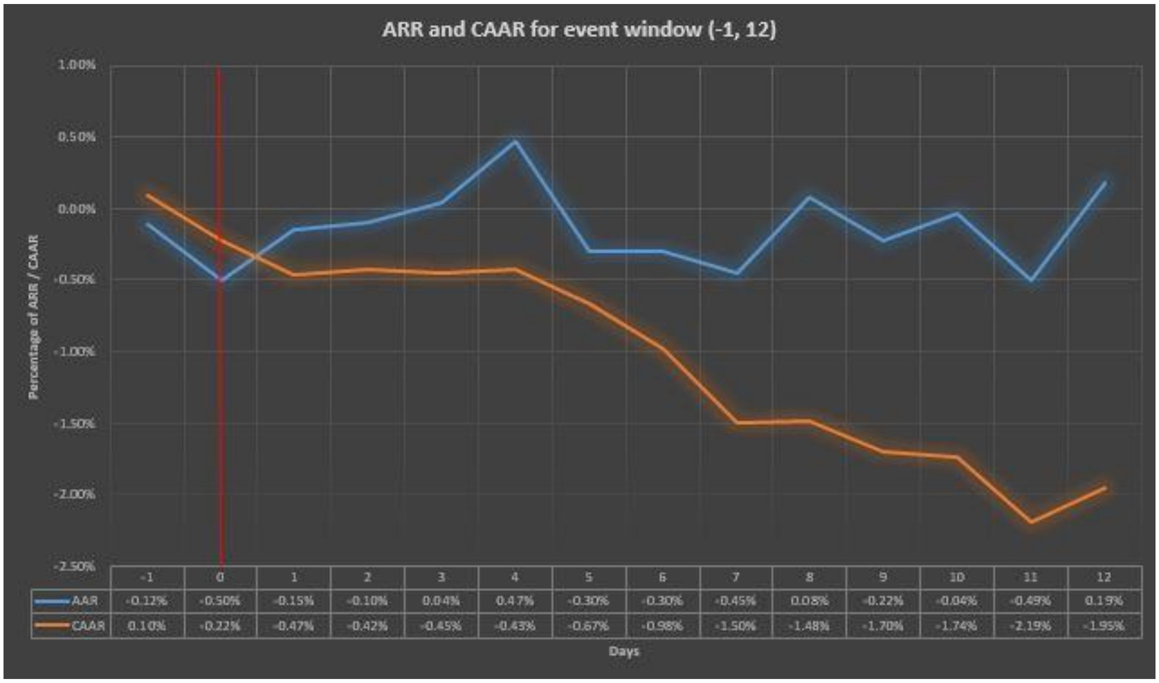


Figure 7: ARR and CAAR results for event window (-1, 12)

As it can be seen from the Figure 7, the AAR is negative for the ten out of thirteen days in the event window. This reaction could be linked with the data breach event as it is obvious that the stock market reacts negatively but the expected returns based on the stock market index were positive. Additionally, it can be seen that twelve days after the event, the stock market has the potential to recover as the abnormal return becomes positive. Finally, using the CAAR function, which is adding the AAR$_{S}$, the total picture of the impact can be created. It is noticeable that the day before the announcement of the incident, the CAAR is positive and that from that day onwards it starts decreasing. At day 6 the CAAR is approximately -1.5%, which can be caused by the repetitive bad publicity from the news.

For a better understanding of the total impact, the selection of a bigger event window is needed. Thus, the event window (-10, 12) is being presented in Figure 8 below. It can be seen that both the AAR and the CAAR are fluctuated around zero until the event day “0”, whereas the CAAR value starts decreasing from this day onwards. In this figure, it is unambiguous that after the day zero there is a significant impact on the market values of the examined firms. However, even in that case, it can be seen that in the last day the stock price starts to recover, which can be related to the end of the discussion of the event in the media.

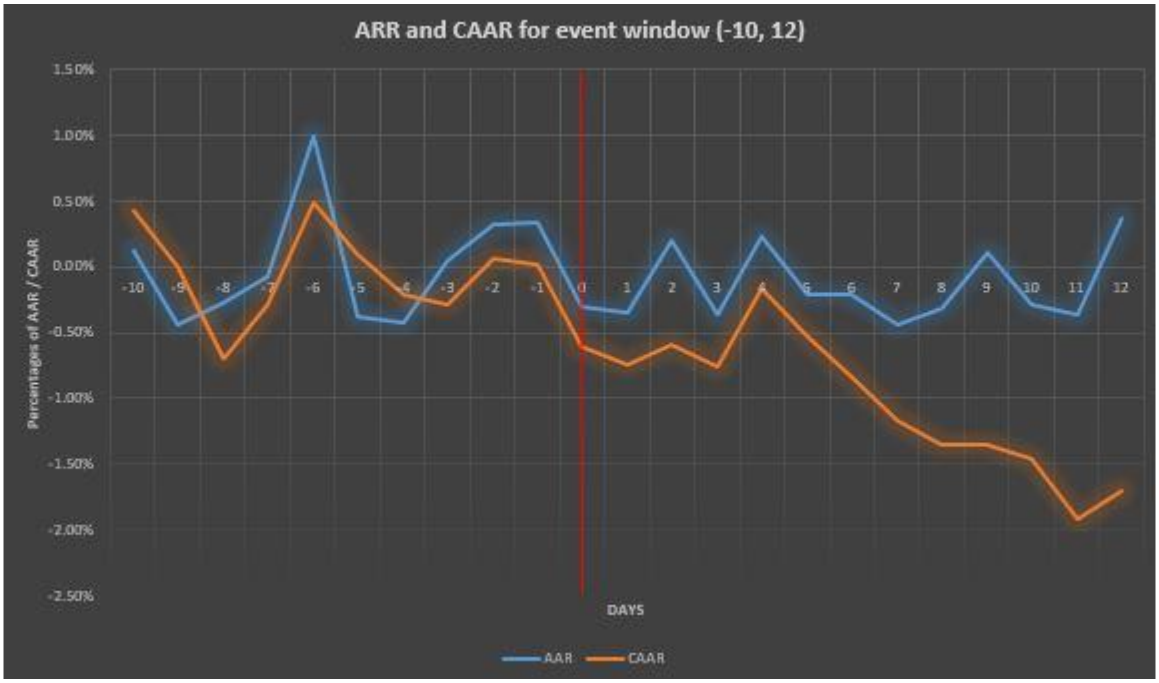


Figure 8: ARR and CAAR results for event window (-10, 12)

The table below presents the results from other studies, as it can be seen there is a small difference in the results, which is caused due to the different event windows used, different:

Researches	Number of Incidents	Estimation window (days)	Event windows	ARR (t=0)	CAAR
Full sample results	31	121 trading days	(-1, 12)	-0.005	-0.01
(Cavusoglu, Mishra and Raghunathan, 2004)	66	160 days	(0,1)	-0.0086	-0.02

(Acquisti, Friedman and Telang, 2006)	79	92 trading days	(-7, 10)	-0.004	-0,0058
(Arcuri, Brogi and Gandolfi, 2014)	128	121 days	(-10, 10)	Not mentioned	-0,021

Table 7: Comparison with other studies

5.3 Analysis of the impact by category

5.3.1 Stock market impact by type of industry

The following table presents the average results of the impact on the stock market by the type of industry based on Table 4. As it can be seen there is equal weight given between the industries and the table was generated in Excel (Spreadsheet Categories (-1, 12)).

Industry	Communications	Entertainment	Media	Other	Retail	Social Network	Web Search
Number of incidents	5	3	4	3	5	6	5
Average Abnormal Return (ARR)	-0.29	-0.42	-0.15	-0.33	-0.19	0.3	-0.14
Cumulative Average Abnormal Return	-2.34	-4.2	-1.18	-1.91	-1.09	2.64	-1.37

Table 8: ARR and CAAR results by industry serving

Using the average of the cumulative abnormal returns, the following graph has been created, representing the total impact of a data breach incident to the different industries:

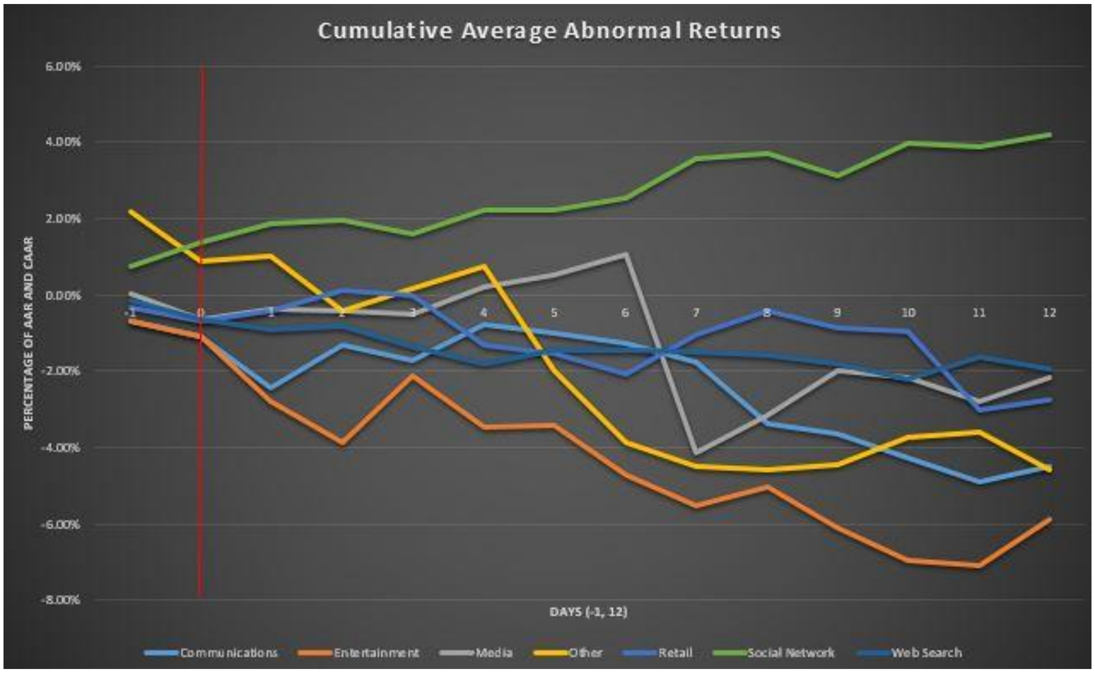
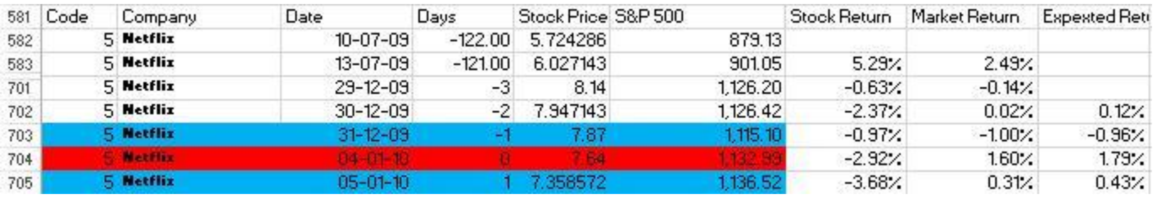


Figure 9: CAAR results by industry for event window (-1, 12)

It is apparent that the entertainment industry suffers more than any other industry after a data breach incident. For example, looking at the individual calculations (Excel Spreadsheet: Event study (-1, 12)), Netflix's stock market price had a negative reaction of 2.92% on the announcement day of a data breach incident, whereas the market index was +1.6%, this is translated as an average loss of 8 million dollars in the market capitalization (Ycharts, 2016). Additionally, based on the calculations the expected return of the stock on that day should be +1.79%, which proves that the data breach incident had a strong impact on the company.



581	Code	Company	Date	Days	Stock Price	S&P 500	Stock Return	Market Return	Expexted Ret
582	5	Netflix	10-07-09	-122.00	5.724286	879.13			
583	5	Netflix	13-07-09	-121.00	6.027143	901.05	5.29%	2.49%	
701	5	Netflix	29-12-09	-3	8.14	1,126.20	-0.63%	-0.14%	
702	5	Netflix	30-12-09	-2	7.947143	1,126.42	-2.37%	0.02%	0.12%
703	5	Netflix	31-12-09	-1	7.87	1,115.10	-0.97%	-1.00%	-0.96%
704	5	Netflix	04-01-10	0	7.64	1,132.99	-2.92%	1.60%	1.79%
705	5	Netflix	05-01-10	1	7.358572	1,136.52	-3.68%	0.31%	0.43%

Figure 10: Netflix stock market reaction (Excel Spreadsheet: "Event study (-1, 12)"

However, an interesting observation of Table 8 is that the social media industry is the only industry that seems not to be affected at all by those security incidents. For example, the massive data breach of 6,500,000 User IDs and passwords of LinkedIn, had as a result, the rise of the stock market by 0.09% on the announcement day and +1.13% the next day. This result could be linked with the different generations that use the social media. More precisely, the main users of the social media belong to the age group of 16 to 24 (Statista, 2014). This age group is named as the Generation Y (people born from the mid 1980s to 2000s) and the people of this generation consider that their privacy is long gone and they don't care about data breach incidents (Infosecurity Magazine, 2014).

5.3.2 Stock market impact by year of data breach

The table below presents the results of the AAR and the CAAR calculations that have been conducted in Excel Spreadsheet: "Categories (-1, 1)".

Years	Average Abnormal Return	Cumulative Average Abnormal Return
2004	0.08	-0.46
2006	0.02	-1.83
2007	-0.22	-4.10
2009	-0.97	-5.27
2010	-0.91	-9.37
2011	-0.18	-1.61
2012	0.27	2.77
2013	0.05	0.74
2014	-0.31	-1.59
2015	-0.31	-3.23
2016	-0.09	0.36

Table 9: AAR and CAAR results by year of data breaches

Once again, the CAAR is the best indicator to understand the total impact on the companies, using the event window (-1, 12). The interesting result is that from 2004 to 2010 there is a rising impact on the stock market prices of the breached companies. However, from 2011 onwards, the internet swarmed by the people of Generation Y and these people changed entirely the consequences of those incidents.

However, in 2014 to 2015 the impact becomes again significant. This can be linked to the NSA spying scandal in 2013 that changed entirely the behavior of the e-users, making them more concerned about their privacy and making them to increase their personal protection by hiding their movements or using different search engines (Annalect, 2013). The assumptions for the year 2016 are not clear as the consequences of the breached companies are still not visible.

5.3.3 Stock market impact by sensitivity of data

Figure 11 presents the total impact of a data breach incident based on the sensitivity of data stolen. It is apparent that the disclosure of personal information such as usernames, passwords, credit cards and demographic data experience strong impact after the announcement of the incidents. On the contrary, the announcement of leaked chats or email conversations, have a minor impact on the stock market price.

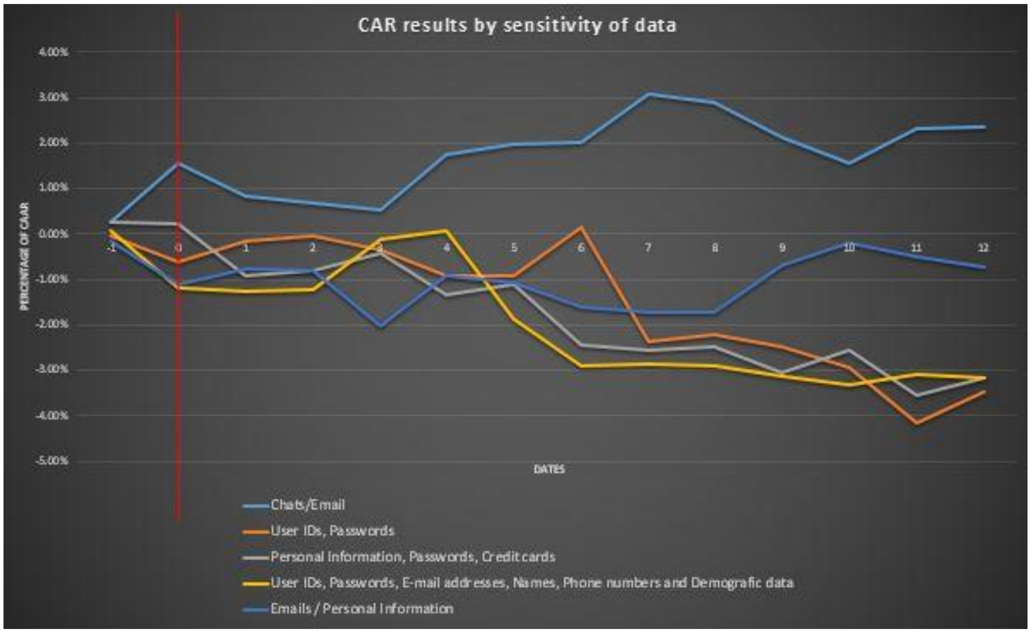


Figure 11: CAAR results by sensitivity of data

As it has been demonstrated by similar researches, the economic impact varies by the sensitivity of data leaked. The market reaction seems to be not significant in the disclosure of not confidential data such as online chats, whereas the disclosure of confidential data (credit card, personal information) provokes strong market reactions (Campbell et al., 2003).

5.4 Chapter Summary

The purpose of this chapter was to analyse the impact of the data breach incidents on the market value of the implicated companies. Using the event study methodology for the 31 incidents, the main findings are that the data breaches can be related with negative stock market return in the following days of the announcement. Additionally, the impact is more significant for the companies that disclosed sensitive and confidential data such as passwords or credit cards, while the most impacted industry has been found to be the entertainment industry.

CHAPTER 6 CONCLUSION

6.1 Chapter Overview

This chapter presents the limitations of this study and based on those limitations, the plans for a future research have been created. Additionally, the chapter summarises all the information to ensure that all the objectives have been answered.

6.2 Limitations

The fist limitation of the event study methodology is on the set of the event day of each case individually. The events are being heavily discussed in the media, as a result, the finding of the original source of the announcement date in some cases to be impossible, so the error of the exact event day is ±1 days in some cases. Additionally, another limitation of the event day is that some of the events occur in non-trading days (ex. weekends or bank holidays) and as a result, the impact on the stock market prices can be almost invisible in the next trading day.

Furthermore, the market model that was used in order to calculate the expected returns assumes a linear relationship between the market and the security return. However, this relationship is also dependent on other variables such as the size of the analysed company (Banz, 1981)

Finally, although the event study methodology analyses unexpected changes upon the stock price of a company after the announcement of an event, it doesn’t take into consideration other incidents that may influence the market value in the examination period, such as the announcement of dividends or introduction of a new product (Londonstockexchange, 2013).

6.3 Further Research

Based on the limitation a further research should be conducted using a bigger sample of online companies and ensuring on adding more variables for the better calculation of the expected return. Additionally, future researches should also examine the impact on the stock market based on the type of data breach (Table 2), the size of the company and the impact on the organisations exposed in a data breach incident more than one times. Finally, an interesting research can be conducted on the question of how many days needed for the stock market to fully recover.

6.4 Conclusion

To sum up, the main focus of this business report is to identify the implication for the online organisations after a data management pitfall. One of the most common IT and management issue for the online companies is the security and privacy of the information stored online.

As the data breach incidents are constantly rising, the companies should continuously train the staff working with sensitive private data and increase the security levels by creating and implementing cyber security strategies based on the online data breach methods used. These improvements are necessary as the information store online are extremely valuable for both the companies and the consumers.

Additionally, as indicated in this business report, a data management pitfall, could have a strong impact on the operation of the online organisation. More precisely, from the examination of 31 data breach incidents and by using the event study methodology, this report finds a significant negative reaction of the stock market price on the announcement day. More precisely, the 71% of the total sample experienced negative abnormal returns on the announcement day, while the companies in the entertainment industry seem to suffer more than other industries. Moreover, the social media websites are proven not to be affected by the announcement of security breaches as the main users of those websites are young people that consider that their privacy is long gone.

However, companies should be alerted all times as in some cases this impact could be very serious and it can lead to strong financial losses for the exposed company. For example, the market price of the web.com website one day after the announcement of a data breach incident had a negative impact of -9.47%, where the expected return on that date bases on the calculations should be -0.70% (Excel Spreadsheet: “Event Study -1, 12). The estimated loss of that negative reaction is 100 million dollars in terms of market capitalisation.

Finally, another severe impact of the mismanagement of the private data is the damage to the reputation and brand image of the company. The data breach events are considered to have the strongest impact on these two categories, while these two categories are considered to have the stronger financial impact on the organisation (Table 1). For this reasons the management, security and privacy of the private data should be a priority for the online organisations as a management pitfall could have potentially catastrophic results.

References

Acquisti, A., Friedman, A. and Telang, R. (2006). IS THERE A COST TO PRIVACY BREACHES? AN EVENT STUDY. *Twenty Seventh International Conference on Information Systems*. [Online] Available at: https://pdfs.semanticscholar.org/386c/5c5b6b8358c8e542f14e52db09158a7845f4.pdf [Accessed 8 Sep. 2016].

Anderson, J. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), pp.308-313.

Andoh-Baidoo, F., Amoako-Gyampah, K. and Osei-Bryson, K. (2010). How Internet Security Breaches Harm Market Value. *IEEE Security & Privacy Magazine*, 8(1), pp.36-42.

Annalect, (2013). *Annalect Q2 2013 Online Consumer Privacy Study*. Americans' Concerns About the Privacy of Online Information Jump in the Wake of NSA Disclosures. [Online] Available at: https://www.annalect.com/wp-content/uploads/AnnalectConsumerOnlineStudy_Q2_2013.pdf [Accessed 7 Sep. 2016].

Arcuri, M., Brogi, M. and Gandolfi, G. (2014). The effect of information security breaches on stock returns: Is the cyber crime a threat to firms?. *European Financial Management Association*. [Online] Available at: http://www.efmaefm.org/0EFMAMEETINGS/EFMA%20ANNUAL%20MEETINGS/2014-Rome/papers/EFMA2014_0408_fullpaper.pdf [Accessed 8 Sep. 2016].

Ayyagari, R. (2012). An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights. *Journal of Information Privacy and Security*, [online] 8(2), pp.33-56. Available at: http://www.tandfonline.com/doi/pdf/10.1080/15536548.2012.10845654?needAccess=true&instName=University+of+Kent.

Banz, R. (1981). The relationship between return and market value of common stocks. *Journal of Financial Economics*, 9(1), pp.3-18.

BCG, (2012). *The value of our digital identity*. [Online] The Boston Consulting Group: Libert Global, p.57. Available at: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf [Accessed 6 Sep. 2016].

Bloomberg. (2016). [Online] Available at: http://www.bloomberg.com/graphics/2014-data-breaches/ [Accessed 12 Aug. 2016].

Brooks, C. (2014). *Introductory econometrics for finance*. 3rd ed. Cambridge: Cambridge University Press, p.637.

Campbell, D., Edgar, D. and Stonehouse, G. (2011). *Business strategy*. Basingstoke: Palgrave Macmillan.

Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market*. *Journal of Computer Security*, [online] 11(3), pp.431-448. Available at: http://iris.nyit.edu/~kkhoo/Spring2008/Topics/Topic10/EconCostPubliclyAnnouncedSecurityBreaches-EmpStockMrkt2003.pdf.

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*, [Online] 9(1), pp.69-104. Available at: https://www.utdallas.edu/~huseyin/paper/market.pdf [Accessed 15 Aug. 2016].

Chen, D. and Zhao, H. (2016). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering*. [Online] Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6187862 [Accessed 28 Aug. 2016].

Cisco. (2016). *Chapter: Passwords and Privileges Commands*. [Online] Available at: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfpass.html [Accessed 8 Sep. 2016].

CNN Money. (2004). *AOL employee arrested and charged with stealing list - Jun. 23, 2004*. [Online] Available at: http://money.cnn.com/2004/06/23/technology/aol_spam/ [Accessed 8 Sep. 2016].

Das, S., Mukhopadhyay, A. and Anand, M. (2012). Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics. *Journal of Information Privacy and Security*, 8(4), pp.27-55.

Digital Guardian. (2015). *The History of Data Breaches*. [Online] Available at: https://digitalguardian.com/blog/history-data-breaches [Accessed 11 Aug. 2016].

Drinkwater, D. (2016). *Does a data breach really affect your firm's reputation?*. [Online] CSO Online. Available at: http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html [Accessed 29 Aug. 2016].

Forbes Insights, (2014). *Fallout: The Reputational Impact of IT risk*. [Online] Available at: http://www.forbes.com/forbesinsights/ibm_reputational_IT_risk/index.html [Accessed 13 Aug. 2016].

Fortune. (2016). *IBM: Data Breaches Now Cost $4 Million on Average*. [Online] Available at: http://fortune.com/2016/06/15/data-breach-cost-study-ibm/ [Accessed 8 Sep. 2016].

Garcia, A. (2015). *Target settles for $39 million over data breach*. [Online] CNNMoney. Available at: http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/ [Accessed 16 Aug. 2016].

Gatzlaff, K. and McCullough, K. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, 13(1), pp.61-83.

Gemalto, (2015). *2015: The Year Data Breaches Got Personal*. [Online]. Available at: http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf [Accessed 14 Aug. 2016].

Gordon, L. and Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, [online] 5(4). Available at: http://sec2013.crysys.hu/~mfelegyhazi/courses/EconSec/readings/04_GordonL02economics_security_investment.pdf [Accessed 12 Aug. 2016].

Gurau, C., Ranchhod, A. and Gauzente, C. (2003). “To legislate or not to legislate”: a comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites. *Journal of Consumer Marketing*, 20(7), pp.652-664.

Harvard Business Review. (2015). *Why Data Breaches Don’t Hurt Stock Prices*. [Online] Available at: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices [Accessed 16 Aug. 2016].

HM GOVERNMENT, (2015). 2015 INFORMATION SECURITY BREACHES SURVEY. [Online]. Available at: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf [Accessed 14 Aug. 2016].

ICO, (2016). *A practical guide to IT security*. Data protection. [Online] Information Commisioner's Office. Available at: https://ico.org.uk/media/1575/it_security_practical_guide.pdf [Accessed 28 Aug. 2016].

Infosecurity Magazine. (2014). *The Generation X, Y, Z of Information Security*. [Online] Available at: https://www.infosecurity-magazine.com/magazine-features/the-generation-x-y-z-of/ [Accessed 26 Aug. 2016].

Itgovernance. (n.d.). *Data Protection Act (DPA) Penalties*. [Online] Available at: http://www.itgovernance.co.uk/dpa-penalties.aspx [Accessed 16 Aug. 2016].

Kannan, K., Rees, J. and Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, 12(1), pp.69-91.

Konchitchki, Y. and O'Leary, D. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems*, 12(2), pp.99-115.

Kothari, S. and Warner, J. (2004). The Econometrics of Event Studies. *SSRN Electronic Journal*. [Online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=608601 [Accessed 6 Aug. 2016].

Kothari, S. and Warner, J. (2006). The Econometrics of Event Studies. *Handbook of Corporate Finance: Empirical Corporate Finance*. [Online] Available at: http://www.bu.edu/econ/files/2011/01/KothariWarner2.pdf [Accessed 6 Aug. 2016].

Kumar, V., Srivastava, J. and Lazarevic, A. (2005). *Managing cyber threats*. New York: Springer.

LaChapelle, C. (2012). *DEFINING THE RIGH DATA PROTECTION STRATEGY*. The Nuances of Backup and Recovery Solutions. [Online] Information Services Group. Available at: http://www.isg-one.com/knowledgecenter/whitepapers/private/papers/White_Paper_-_Data_Backup_Recovery.pdf [Accessed 15 Aug. 2016].

Lafuente, G. (2015). The big data security challenge. *Network Security*, 2015(1), pp.12-14.

Laudon, K. and Traver, C. (2013). *E-commerce*. Boston, Mass.: Pearson.

Liem, C. and Petropoulos, G. (2016). *The economic value of personal data for online platforms, firms and consumers | Bruegel*. [Online] Bruegel. Available at: http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/ [Accessed 6 Sep. 2016].

Londonstockexchange. (2013). *What influences a share price - London Stock Exchange*. [Online] Available at: http://www.londonstockexchange.com/traders-and-brokers/private-investors/private-investors/about-share/what-influence-share-price/what-influence-share-price.htm [Accessed 8 Sep. 2016].

Luftman, J., Zadeh, H., Derksen, B., Santana, M., Rigoni, E. and Huang, Z. (2013). Key information technology and management issues 2011–2012: an international study. *Journal of Information Technology*, [online] 28(4), pp.198-212. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361404 [Accessed 7 Aug. 2016].

MACKINLAY, C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, [online] 35, pp.13-39. Available at: http://www1.american.edu/academic.depts/ksb/finance_realestate/rhauswald/fin673/673mat/MacKinlay%20(1997),%20Event%20Studies%20in%20Economics%20and%20Finance.pdf [Accessed 16 Aug. 2016].

Manworren, N., Letwat, J. and Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3), pp.257-266.

Mearian, L. (2016). *No, your data isn't secure in the cloud*. [Online] Computerworld. Available at: http://www.computerworld.com/article/2483552/cloud-security/no--your-data-isn-t-secure-in-the-cloud.html [Accessed 28 Aug. 2016].

Molla, A. and Licker, P. (2001). E-Commerce Systems Success: An Attempt to Extend and Respecify the Delone and MaClean Model of IS Success. *Journal of Electronic Commerce Research*, [online] 2(4). Available at: https://www.researchgate.net/publication/220437633_E-Commerce_Systems_Success_An_Attempt_to_Extend_and_Respecify_the_Delone_and_MaClean_Model_of_IS_Success [Accessed 12 Aug. 2016].

Morse, E., Raval, V. and Wingender, J. (2011). Market Price Effects of Data Security Breaches. *Information Security Journal: A Global Perspective*, [online] 20(6), pp.263-273. Available at: http://www.tandfonline.com/doi/pdf/10.1080/19393555.2011.611860?needAccess=true [Accessed 3 Aug. 2016].

Pandis, N. (2016). Linear regression. *American Journal of Orthodontics and Dentofacial Orthopedics*, [online] 149(3). Available at: http://ac.els-cdn.com/S0889540615013797/1-s2.0-S0889540615013797-main.pdf?_tid=75bb5baa-6891-11e6-8b3c-00000aacb35f&acdnat=1471888643_b995c74baf042e3140e1b89344e6a92f [Accessed 22 Aug. 2016].

Pektaş, A. and Acarman, T. (2013). A dynamic malware analyzer against virtual machine aware malicious software. *Security and Communication Networks*, [online] 7(12), pp.2245-2257. Available at: http://onlinelibrary.wiley.com/wol1/doi/10.1002/sec.931/full [Accessed 9 Aug. 2016].

Ponemon Institute LLC, (2016). *2016 Cost of Data Breach Study: Global Analysis*. [Online] Benchmark research sponsored by IBM: Ponemon Institute© Research Report. Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN [Accessed 6 Sep. 2016].

Schatz, D. and Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security*, 24(1), pp.73-92.

Semafone. (2014). *86% of customers would shun brands following a data breach - Semafone*. [Online] Available at: https://www.semafone.com/86-customers-shun-brands-following-data-breach/ [Accessed 8 Sep. 2016].

Sinanaj, G., Muntermann, J. and Cziesla, T. (2015). How Data Breaches Ruin Firm Reputation on Social Media! – Insights from a Sentiment-based Event Study. *Wirtschaftsinformatik Proceedings*. [Online] Available at: http://www.wi2015.uni-osnabrueck.de/Files/WI2015-D-14-00293.pdf [Accessed 8 Sep. 2016].

Solms, R. and Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, [online] 38, pp.97-102. Available at: http://ac.els-cdn.com/S0167404813000801/1-s2.0-S0167404813000801-main.pdf?_tid=2145fd5a-7458-11e6-9773-00000aab0f6b&acdnat=1473183434_db48940c835de2687a898c0ce2185516.

Sood, S. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications*, 35(6), pp.1831-1838.

Statista. (2014). *Average age of social media users | Statistic*. [Online] Available at: http://www.statista.com/statistics/274829/age-distribution-of-active-social-media-users-worldwide-by-platform/ [Accessed 26 Aug. 2016].

Statista. (2015). *U.S. data breaches and exposed records 2015 | Statistic*. [Online] Available at: http://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [Accessed 12 Aug. 2016].

TechCrunch. (2016). *Recently confirmed Myspace hack could be the largest yet*. [Online] Available at: https://techcrunch.com/2016/05/31/recently-confirmed-myspace-hack-could-be-the-largest-yet/ [Accessed 11 Aug. 2016].

The Guardian. (2013). *NSA spying scandal: what we have learned.* [Online], Available from: http://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned [Accessed 22 Mar. 2016].

U.S DEPARTMENT OF HEALT AND HUMAN SERVICES (2015). *INFORMAITON SECURITY PROGRAMS AND GUIDELINES FOR RESPONDING TO DATA BREACHES.* Administration for Children and Families, 2.

Walker-Osborn, C., Fitzsimons, L. and Ruane, J. (2013). Data Protection. *ITNOW*, [online] 55(3). Available at: http://itnow.oxfordjournals.org.chain.kent.ac.uk/content/55/3/38.full.pdf+html [Accessed 28 Aug. 2016].

Wang, Y. and Liao, Y. (2008). Assessing eGovernment systems success: A validation of the DeLone and McLean model of information systems success. *Government Information Quarterly*, 25(4), pp.717-733.

Washington Post. (2014). *Why it's so hard to calculate the cost of the Sony Pictures hack*. [Online] Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack/ [Accessed 16 Aug. 2016].

Ycharts. (2016). *Netflix Market Cap (NFLX)*. [Online] Available at: https://ycharts.com/companies/NFLX/market_cap [Accessed 8 Sep. 2016].

Zimmer, M. (2010). ''But the data is already public'': on the ethics of research in Facebook. *Ethics Information Technology*. [Online] Available at: http://www.sfu.ca/~palys/Zimmer-2010-EthicsOfResearchFromFacebook.pdf [Accessed 8 Sep. 2016].

Bibliography

CSO Online. (2016). *Does a data breach really affect your firm's reputation?*. [Online] Available at: http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html [Accessed 16 Aug. 2016].

Gellman, B. (2013). *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. [Online] Washington Post. Available at: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [Accessed 26 Aug. 2016].

Goel, S. and Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), pp.404-410.

Hu, D., Zhao, J. and Cheng, J. (2012). Reputation Management in an Open Source Developer Social Network: An Empirical Study on Determinants of Positive Evaluations. *SSRN Electronic Journal*.

Klíma, T. (2012). Anatomy of data breaches and their impact on market value. *Electronic International Interdisciplinary Conference*.

Tian, Z., Zhang, Z. and Guan, X. (2013). A new evolution model for B2C e-commerce market. *Information Technology and Management*, 14(3), pp.205-215.

Appendices

Appendix A: E-Commerce Success Model

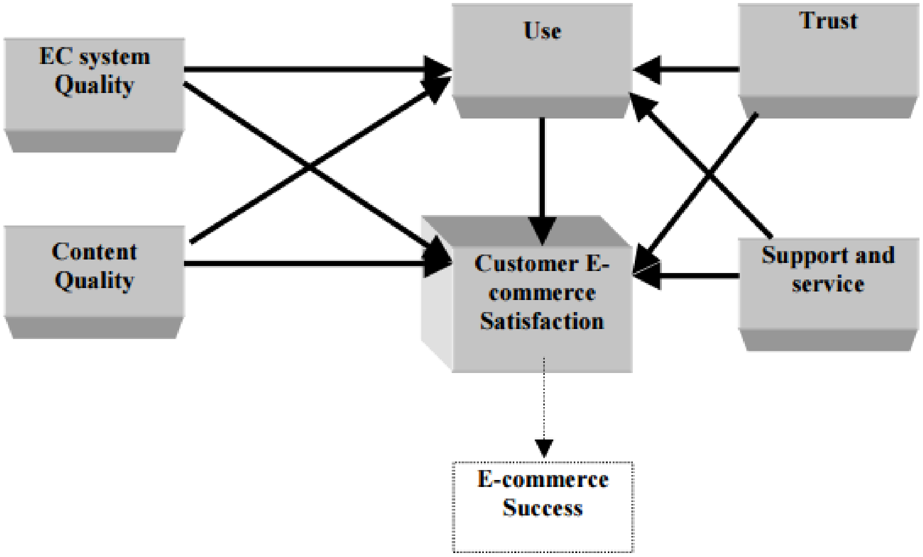


Figure 12: E-commerce success model (Molla and Licker, 2001)

The model presented in Figure 12, was built on the Delone and Maclean model of Information System success. The model indicates some crucial dimensions that if properly followed might lead an e-company (EC) to success. The brief meaning of the 6 dimension is the following (Molla and Licker, 2001):

i. EC System Quality: The quality of the system is defined by the reliability, flexibility and usability of the website.

ii. Content Quality: The content should be easily and securely accessible, and the information offered should be accurate and easy to understand.

iii. Support and service: The e-company should be able to reply to customers 24/7 and the transactions in exchange for a service should be safe, in order to increase customer's loyalty.

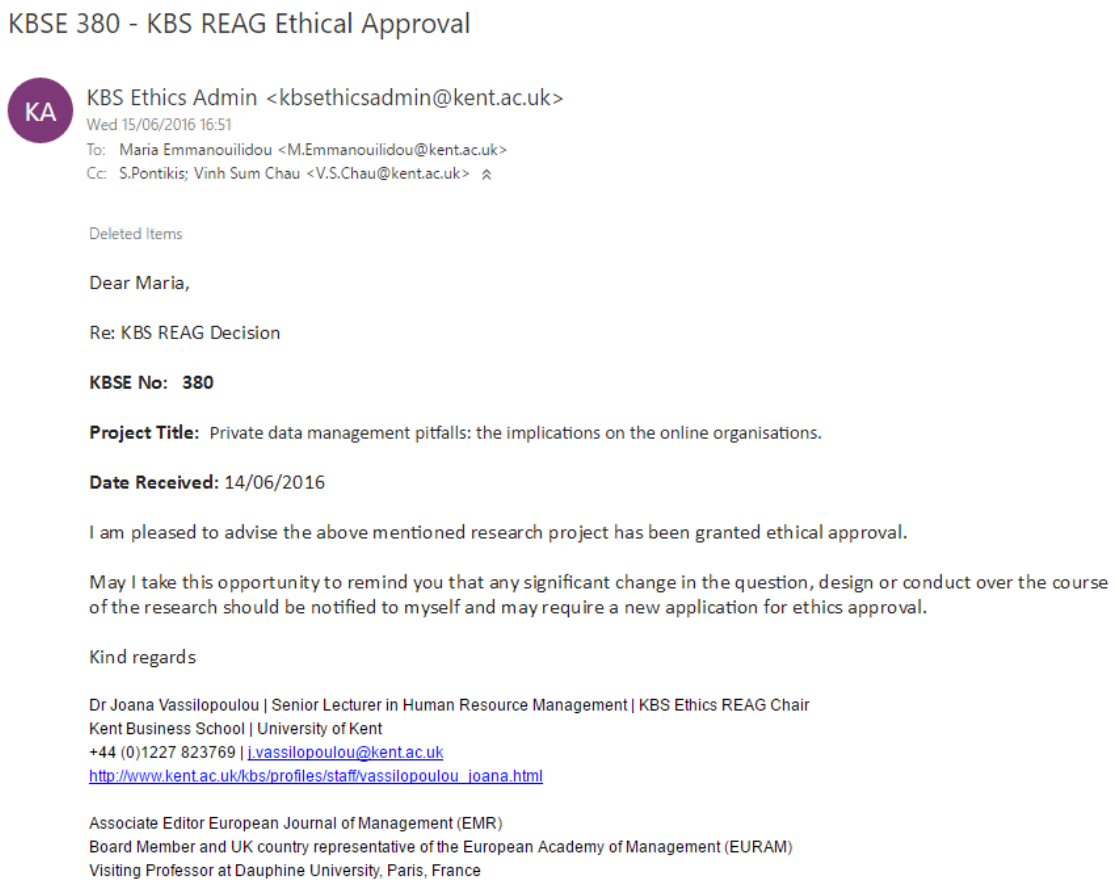
iv. Trust: The term is linked with the security and privacy offered by the website. The higher the security and privacy, the higher the Trust from the e-consumers

v. Use: This is one of the main dimensions of the model as it is linked with the four already mentioned dimensions and it feeds the last one, the satisfaction. The use of a website is increasing if the other dimensions are giving value to the customer and this leads to e-commerce satisfaction.

vi. Customer E-commerce Satisfaction: The general satisfaction of the user of a website. The high levels of satisfactions create intensive use of the website, thus higher revenues for the e-commerce company.

The lack of adoption of these main success dimensions could cause distant users, that are not satisfied and this might cause a financial disaster to the online organisation (Molla and Licker, 2001).

Appendix B: Ethical Approval



KBSE 380 - KBS REAG Ethical Approval

KBS Ethics Admin <kbsethicsadmin@kent.ac.uk>
Wed 15/06/2016 16:51
To: Maria Emmanouilidou <M.Emmanouilidou@kent.ac.uk>
Cc: S.Pontikis; Vinh Sum Chau <V.S.Chau@kent.ac.uk>

Deleted Items

Dear Maria,

Re: KBS REAG Decision

KBSE No: 380

Project Title: Private data management pitfalls: the implications on the online organisations.

Date Received: 14/06/2016

I am pleased to advise the above mentioned research project has been granted ethical approval.

May I take this opportunity to remind you that any significant change in the question, design or conduct over the course of the research should be notified to myself and may require a new application for ethics approval.

Kind regards

Dr Joana Vassilopoulou | Senior Lecturer in Human Resource Management | KBS Ethics REAG Chair
Kent Business School | University of Kent
+44 (0)1227 823769 | j.vassilopoulou@kent.ac.uk
http://www.kent.ac.uk/kbs/profiles/staff/vassilopoulou_joana.html

Associate Editor European Journal of Management (EMR)
Board Member and UK country representative of the European Academy of Management (EURAM)
Visiting Professor at Dauphine University, Paris, France

Figure 13: Ethical Approval

Appendix C: Full sample of the companies

Companies	Date of event	Industry	Number of Records Leaked	Data Sensitivity
AOL	23/6/04	Media	92,000,000	Emails of users / Personal Information
AOL	04/8/06	Media	20,000,000	Emails of users / Personal Information
Monster.com	21/8/07	Other	1,600,000	User IDs, Passwords, E-mail addresses, Names, Phone numbers, and Demographic data
Monster.com	23/1/09	Other	4,500,000	User IDs, Passwords, E-mail addresses, Names, Phone numbers, and Demographic data
Netflix	1/1/10	Entertainment	100,000,000	Personal Information, Passwords Credit cards

Sony PlayStation Network	18/4/11	Entertainment	77,000,000	Personal Information, Passwords Credit cards
Sony Pictures	6/6/11	Entertainment	1,000,000	User IDs, Passwords, E-mail addresses, Names, Phone numbers, and Demographic data
LinkedIn	6/6/12	Social Network	6,500,000	User IDs, Passwords
Yahoo Voices	12/7/12	Web Search	500,000	User IDs, Passwords
Zappos	16/1/12	Retail	24,000,000	Personal Information, Passwords Credit cards
Tumblr	15/1/13	Social Network	65,000,000	User IDs, Passwords
Facebook	24/6/13	Social Network	6,000,000	Emails of users / Personal Information

Facebook	10/6/13	Social Network	Unknown / Not published	Chats/Emails
Google	10/6/13	Web Search	Unknown / Not published	Chats/Emails
LinkedIn	10/6/13	Social Network	Unknown / Not published	Chats/Emails
Yahoo	10/6/13	Web Search	Unknown / Not published	Chats/Emails
AOL	10/6/13	Media	22,000,000	Emails of users / Personal Information
Chrome	17/5/13	Web Search	Unknown / Not published	Personal Information, Passwords Credit cards
Target	10/1/14	Retail	Unknown / Not published	Personal Information, Passwords Credit cards
T-Mobile	30/12/13	Communication	Unknown / Not published	Personal Information, Passwords Credit cards
eBay	21/5/14	Retail	145,000,000	User IDs, Passwords
AOL	28/4/14	Media	2,400,000	User IDs, Passwords
Gmail	11/9/14	Communication	4,930,000	User IDs, Passwords
TripAdvisor	25/8/14	Other	1,400,000	Personal Information, Passwords Credit cards

T-Mobile	15/10/15	Communication	15,000,000	User IDs, Passwords
VTech	30/11/15	Retail	11,500,000	User IDs, Passwords
Talk Talk	5/11/15	Communication	157,000	Personal Information, Passwords Credit cards
Web.com	18/8/15	Communication	93,000	Personal Information, Passwords Credit cards
Amazon	25/11/15	Retail	80,000	User IDs, Passwords
Myspace	31/5/16	Social Network	360,000,000	User IDs, Passwords, E-mail addresses, Names, Phone numbers, and Demographic data

Table 10: Data Breaches full sample