2012-01-01

Market Reactions To Publicly Announced Privacy And Security Breaches Suffered By Companies Listed On The United States Stock Exchanges: A Comparative Empirical Investigation

Adolfo S. Coronado
University of Texas at El Paso, coronado.adolfo@gmail.com

MARKET REACTIONS TO PUBLICLY ANNOUNCED PRIVACY AND SECURITY BREACHES SUFFERED BY COMPANIES LISTED ON THE UNITED STATES STOCK EXCHANGES: A COMPARATIVE EMPIRICAL INVESTIGATION

ADOLFO SERGIO CORONADO

Department of Information and Decision Sciences

APPROVED:

M. Adam Mahmood, Ph.D., Chair

Leopoldo Gemoets, Ph.D.

William Elliott, Ph.D.

Benjamin C. Flores, Ph.D.
Dean of the Graduate School

MARKET REACTIONS TO PUBLICLY ANNOUNCED PRIVACY AND SECURITY BREACHES SUFFERED BY COMPANIES LISTED ON THE UNITED STATES STOCK EXCHANGES: A COMPARATIVE EMPIRICAL INVESTIGATION

by

Adolfo S. Coronado, BBA, MIT

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

Department of Information and Decision Sciences

THE UNIVERSITY OF TEXAS AT EL PASO

December 2012

Abstract

Using a sample of security and privacy breaches the present research examines the comparative announcement impact between the two types of events. The first part of the dissertation analyzes the impact of publicly announced security and privacy breaches on abnormal stock returns, the change in firm risk, and abnormal trading volume are measured. The second part of the dissertation analyzes differential impact between security and privacy breaches on abnormal stock returns, the change in firm risk, and abnormal trading volume are measured.

Using a sample of 114 security (65) and privacy (49) breaches on average, security breaches resulted in more negative abnormal stock returns than do privacy breaches. While firm risk for privacy events does not change appreciably, firms experiencing security events show a significant increase in risk. The risk shifts between the security and privacy breaches is significantly different. Firms that announced a security or privacy breaches experienced abnormal trading volume.

Table of Contents

List of Tables

Chapter 1: Introduction

1.1. Problem Statement

Information security is an important concern of corporations, and as such, it is an important component of strategic management (von Solms, 2001). Market reactions to publicly announced security and privacy breach incidents suffered by companies listed on US stock exchanges offers a mechanism to capture both, tangible, and intangible financial losses. The most damaging types of attacks are, according to the 2009 Computer Security Institute (CSI) survey on Computer Crime and Security, wireless exploits, theft of personal identification and personal health information, and financial fraud (Richardson, 2009). The losses from these attacks had an average cost per incident of $770,000, $710,000, and $450,000, respectively (Richardson, 2009). Over sixty percent of the companies surveyed by Verizon's Data Breach Investigations Report (2010) accounted for a privacy or a security breach. According to a Congressional Research Service report (Cashell, Jackson, Jickling, & Webel, 2004) in 2003 losses due to worms and viruses are estimated at $13 billion, and for all other forms of attacks at $225 billion. The market recognizes the prominence of security and privacy threats faced by organizations which is reflected in a positive market reaction toward information security investments (Chai, Kim, & Rao, 2011).

There have been few attempts to empirically assess the impact of information security and privacy breaches. Many previous studies have, however, failed to adequately separate security and privacy breaches. The results, as such, were confounding and mixed, at best. This study, therefore, clearly distinguishes between privacy and security breach incidents. In the next Section, privacy and security breaches are defined in more detail. Section 1.3 discusses the purposes of the present dissertation. The Chapter concludes by providing an overview of the remaining Chapters.

1.2. Information Security and Privacy Breaches

This dissertation research distinguishes, as stated earlier, between privacy and security breaches. This Section explains in detail the criteria used to classify breaches in these two categories. As also

mentioned earlier, previous studies do not explicitly classify these breaches in well-defined categories. Therefore, an important contribution of the present research is to clearly provide a definition of security and privacy breaches. To draw the distinction between privacy and security breaches, research conducted in the areas of privacy and security is cited. Privacy breaches are defined first, followed by a definition of security incidents.

It should be noted that privacy breaches are defined from the perspective of firms. As such, privacy breaches in the present dissertation are defined following the suggestions made by Straub (1990). Straub (1990) investigated the impact of information systems security investments in providing better control over computer abuse. The definition used in this dissertation for privacy breaches is an incident resulting in unauthorized access and use of computer services, the purposeful interruption of computer services, the theft or modification of computer codes, and the destruction of data (Straub, 1990).

According to the Federal Information Processing Standards (FIPS) publication 199 by the National Institute of Standards and Technology (2004) three levels (i.e. low, moderate, and high) of potential impact on organizations or individuals suffering an information breach. As a result of a privacy breach, a low level of potential impact is expected in the present research. The low level of potential impact involves a degradation of in the firm's ability to perform its primary functions and the "...effectiveness of the functions is noticeably reduced" (NIST, 2004, p. 2). The damage to organizational assets and financial losses are minor.

In accordance with the precedent discussion, the present research classifies the following incidents as privacy breaches:

- Denial of service attacks (DoS)
- Hacker attacks
- Virus attacks, and
- Website defacements.

Security breaches, on the other hand, are defined as any external, web-based act that results in violations of NIST security elements such as identification, authentication, authorization, integrity, non-

repudiation, and confidentiality (Singhal, Winograd, & Scarfone, 2007). This definition of security is also in agreement with the Federal Information Security Management Act (FISMA) of 2002, where information security is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information... " (NIST, 2004, p. 2). More specifically, the present research defines security incidents as those attacks that compromise the confidentiality and integrity of customers' data and information assets.

Based on the FIPS publication 199 (2004), a security breach is classified in the present research as a moderate level of potential impact. The moderate level of potential impact involves a significant degradation of in the firm's ability to perform its primary functions and the "...effectiveness of the functions is significantly reduced" (National Institute of Standards and Technology, 2004, p. 2). The damage to organizational assets and financial losses are significant.

Based on the guidelines provided by Krishnamurthy and Wills (2010) and the FIPS publication 199 incidents involving the following items are classified as security breaches:

- Social security numbers
- Bank account numbers, and credit card numbers
- Driver's license numbers
- Identity theft, and
- The exposure of any other personally identifiable information.

It is possible that a breach initiates in one area (i.e. security or privacy) and then affects the other as well, which creates a challenge in its classification. For example, a virus may infect a system (i.e. privacy breach) and then information regarding credit card information stored in the infected system is compromised (i.e. security breach). In the event an incident transcends from one category to the other, the breach is classified under the category it started in, as suggested by Gordon, Loeb, and Zhou (2011). In the next Section, the purpose of the present dissertation research is discussed.

1.3. Purpose

A recent stream of research has focused on privacy breaches (e.g., Acquisti, Friedman, & Telang, 2006; Campbell, Gordon, Loeb, & Zhou, 2003; Ettredge & Richardson, 2003; Hovav & D'Arcy, 2003;

Ishiguro, Tanaka, Matsuura, & Murase, 2006; Nicholas-Donald, Matus, Ryu, & Mahmood, 2011), while another stream has focused on security breaches (e.g. Andoh-Baidoo, Amoako-Gyampah, & Osei-Bryson, 2010; Andoh-Baidoo & Osei-Bryson, 2007; Cavusoglu, Mishra, & Raghunathan, 2004). None, based on an extensive literature review, has focused on a comparative analysis of the impact of privacy and security breaches. The present dissertation research is divided in three main themes. The first topic is related to the market reaction of publicly announced privacy breaches. The second topic, aims to address the market reaction of publicly announced security breaches. The third topic is a comparative analysis of publicly announced privacy and security breaches. A more detailed discussion on these three is provided next.

The objective of the present dissertation research is to provide a comparative study of market reactions to publicly announced privacy breaches suffered by companies listed on the US Stock exchanges. The comparison takes into consideration abnormal returns, shifts in risk, and abnormal volume experienced by breached firms. These will be further discussed in Chapters 2 and 3.

1.4. Overview of Remaining Chapters

The rest of the dissertation is organized as follows: in Chapter 2, a literature review related to event studies on information security breaches and privacy breaches, event studies on abnormal trading volume changes, studies on risk shifts, and other relevant event studies on the area of information systems are provided. In Chapter 3, the hypotheses development is presented. Chapter 4 introduces the sample selected for the present research and research method. In Chapter 5 the results are put forward. This is followed by Chapter 6, which discusses the results (Section 6.1), provides recommendations for future research (Section 6.2), and concludes (Section 6.3) the present research.

Chapter 2: Literature Review

The findings, as stated earlier, from previous event studies in the area of information systems privacy and security that examined abnormal returns are mixed. Some authors found statistically significant negative abnormal returns due to privacy or security breaches, while others found no such effects. In Section 2.1, the event study methodology is explained. This is followed by a review of the literature in the information systems privacy area in Section 2.2. This is followed by a review of the same in the security area in Section 2.3. Sections 2.4 and 2.5 cover event studies on abnormal trading volume and risk shifts, respectively, conducted mostly in the accounting and finance areas. This is because no research studies in the information systems area have explored these phenomena. An exception is a recent study by Nicholas-Donald, Matus, Ryu, and Mahmood (2011), which offers preliminary results in the area of information privacy breaches. Section 2.6 concludes the Chapter by providing a summary of the literature review of other event studies in the information systems, accounting, and finance areas.

2.1. Event Study Methodology History and Application

Event-studies were developed in finance and accounting areas. An event study is a test of market efficiency and expected rates of return (Kothari, 2001). The first event studies appeared in the 1960s and have been since then an important and well-known methodology (Kothari, 2001). In this Section, a brief history of event studies and its application is presented.

The first event study in financial economics was conducted by Fama et al. (1969). According to Fama, an efficient market is one in which "security prices fully reflect all available information" (Fama, 1970, p. 383). Fama et al.'s work set the tone for researchers by introducing the analysis of the firm's security price performance before, during, and after a specific event. In finance, for example, the seminal articles of Fama et al. (1969) analyzed stock splits effect on stock returns. Ball and Brown (1968) and Beaver (1968), also in the same area, investigated the impact of earnings announcements on stock prices.

The event study methodology, in general, is based on the efficient market hypothesis, which is a theoretically grounded and well-known concept in finance and accounting literatures. The event study methodology relies on the Capital Asset Pricing Model (CAPM) to empirically test the efficient market hypotheses. CAPM let to what today is known as asset pricing theory. This model is based on the work of Sharpe (1964) and Lintner (1965), Sharpe won the Nobel Prize in 1990 in recognition of his work on CAPM. This model is widely used and well-known in business because it is powerful and intuitive, it measures the relationship between expected return and risk (Fama & French, 2004). CAPM also builds on the work of Markowitz (1959), who assumes investors are risk averse and select a portfolio that maximizes the expected return and minimizes the risk. In this context, risk minimization is achieved by selecting a "mean variance-efficient" portfolio, and at the same time by maximizing of the expected return given the variance. In order to test the proposed hypotheses a market model based on CAPM is used. Section 4.2 explains in more detail the test of the market efficiency theory using a market model based on CAPM.

The present research follows the structure suggested by MacKinlay (1997) in designing an event study methodology. According to MacKinlay (1997), an event study should be structured by following these steps:

- Define the event of interest (see Section 1.2),
- Define the event window (see Section 4.2)
- Determine the selection criteria for the inclusion of a firm in the sample (see Section 4.1)
- Calculate abnormal returns and cumulative abnormal returns (see Section 4.4)

In the present research, an event constitutes a privacy or security breach incident suffered by a public company listed on one of the United States stock markets. Second, the event window selected for this research is based on the 3 trading days surrounding the event [-1, 0, +1]. This event window is selected because the event announcement could be leaked a day before it reaches the news channels, or, the announcement could be made public after trading hours (MacKinlay, 1997). The security or privacy breaches identified should be inflicted to a publicly traded firm, and the market information should be available in the Center for Research in Security Prices (CRSP) dataset. Expected returns are calculated

using an OLS regression (see Equation 1 in Section 4.2) using 250 trading days. Abnormal returns are calculated, based on the difference from the expected returns and actual returns (see Equation 2 in Section 4.2). In the present research, abnormal returns are calculated using two models, the one-factor model (see Section 4.2) and the Fama-French's three-factor model (see Section 4.3). The abnormal returns are cumulated during the event window. In other words, for each firm, the abnormal returns for days -1, 0, and 1 are cumulated (see Equation 4 in Section 4.4).

2.2. Event Studies in Information Systems Privacy Breaches

The results from the event studies in the information systems area, as stated earlier, are mixed. Some studies found a statistically significant impact on a firm's value as a result of an information systems privacy breach, while others did not. Three recent event studies on privacy breaches has been reported in the US stock market by Hovav and D'Arcy (2003; 2004) and one in the Japanese stock market by Ishiguro et al. (2006). These studies found no statistically significant impact on stock returns. Five other studies, on the other hand, found a statistically significant negative impact on stock returns (Acquisti et al., 2006; Campbell et al., 2003; Ettredge & Richardson, 2003; Khansa & Liginlal, 2011; Nicholas-Donald et al., 2011). First a discussion of the "non-significant" group is put forward, followed by the "significant" group. This is followed by a discussion of two relevant studies in privacy breaches. The first research used an event study methodology to analyze the contagion effect of privacy breached to non-breached competitors (Zafar, Ko, & Osei-Bryson, 2012), and the second study used a matched sample approach to analyze the economic impact of privacy breaches (Ko & Dorantes, 2006).

Hovav and D'Arcy (2003), in the privacy group, conducted one of the first event studies on stock market reaction to information privacy breaches (e.g., denial of service attacks) published in newspapers. The authors used the market model, which is based on CAPM, to examine the stock market reaction to 23 DoS attack announcements (i.e., events). The authors used 200 days estimation period and five event windows (i.e. [-1, 0], [-1, 1], [-1, 5], [-1, 10], and [-1, 25]). Stock markets do not react, at least according to the authors, negatively to privacy breach announcements.

In another study, Hovav and D'Arcy (2004) examined the impact of virus attack announcements on the market value of breached firms. The authors scrutinized 186 virus attack announcements ranging

from 1998 to 2002. The authors do not provide any details on the model used to estimate returns or the estimation window, other than mentioning the estimation of standardized abnormal returns. The authors found no support for the hypothesis that virus announcements result in negative abnormal returns for all five event periods (i.e. [0, 0], [0, 1], [0, 5], [0, 10], and [0, 25]) used by the authors. These results support the notion that the impact of virus attack announcements does not have a significant negative abnormal return for the breached firms.

Outside the United States, Ishiguro et al. (2006) conducted an event study to assess the impact of information privacy breaches on stocks listed in the Japanese Stock market. Using a one factor market model, a 120 days estimation period, and a seven-day event window, on a sample of 70 privacy breaches, the authors also found no significant impact of privacy violations on the market value of the breached companies listed on the Stock Exchange. The authors noted that the slow reaction to privacy breaches is a common phenomenon in the Japanese market.

The previous three studies found no statistically significant negative market reactions due to privacy breaches. Next, in this Section, the studies that found statistically significant impact of privacy breaches on stock are discussed.

Acquisti et al. (2006) conducted an event study on privacy breaches of 79 companies with an estimation window of 92 days and an event window of 18 days [-7, 10]. Using the market model, the market adjusted model, and the mean adjusted model the authors found a negative and statistically significant impact of breach attacks published in newspapers on stock market returns of breached companies. On the event day and the day after the event day, the cumulative abnormal returns reached 6% and these returns are, according to the authors, robust under different model specifications. Overall, the authors found that publicly announced privacy breaches resulted in a significant negative market return for the breach firms.

An early attempt in the area of privacy breaches was put forward by Campbell et al. (2003). The authors found negative and statistically significant cumulative abnormal returns on the stock prices of the breached companies. Using the market model on a sample of 43 privacy breach events published in major national newspapers, an estimation period of 120 days, and an event window of 3-days (-1,0,+1),

the authors assessed the market reaction to the aforementioned privacy breach announcements. The authors contribute to the area of privacy breaches by finding that there is a negative and statistically significant cumulative abnormal return for the breached firms.

Ettredge and Richardson (2003) undertook a different approach and measured the information transfer among Internet firms. The authors analyzed the popular DoS attacks carried in February 2000 and extended the current research area by also exploring the spillover effect of non-breached firms on "similar" firms. The authors employed a single-index market model with a 255-day estimation period and a three-day event window for the total of 275 non-breached firms. The authors found information transfer (in the form of negative mean abnormal returns) among firms within the industries of the breached firms. Firm size was found to be another factor in information transfer, where larger firms are found to be more likely to be the targets of attacks.

Khansa and Liginlal (2011) predicted stock market returns from malicious attacks and how these attacks caused a spillover effect on security services firms. The authors found that security services firms were influenced positively by the announcement of virus attacks. The authors also found that there was a negative impact on stock prices of the breached firms. The sample of events consisted of around 11,000 privacy breaches announced in Symantec's website. The estimation of stock market returns was obtained with a vector autoregressive and time-delayed neural networks.

In a recent study by Nicholas-Donald et al. (2011), the authors found support for the hypothesis that privacy breaches result in a significant and negative abnormal return. The study relied on a sample of 29 privacy breaches from the time period of 2000 to 2010. The authors estimated abnormal returns using a single-index market model with 250 trading days for the estimation window, and a three-day event window [-1, +1]. In addition to finding support of a significant and negative impact of privacy breaches on abnormal returns, the authors also analyzed the impact on trading volume and risk (as measured by beta).

A recent study by Zafar, Ko, and Osei-Bryson (2012) investigated the effect of privacy breaches on breached firms and the contagion effect on their non-breached competitors. The authors defined a breach a result of a website defacement, denial-of-service attack, data theft, and data corruption. Using a

sample of 119 breached firms and 867 non-breached competitors, the authors found evidence of a contagion effect. The authors found statistically significant evidence of an intra-industry information transfer from the breached firms to non-breached firms for website defacement, data theft, and data corruption. This effect was not present for denial-of-service attacks.

Breaking ranks with the previous studies that used an event study, Ko and Dorantes (2006) utilized a matched sample comparative analysis to investigate the impact of privacy breaches (e.g., virus attacks, unauthorized access, theft of proprietary information, denial of service attacks, sabotage, and web site defacement) on the performance of publicly traded companies. In order to determine whether there were any significant differences between the treatment group (that includes firms that have experienced information privacy breaches) and control group (that includes non-breached companies that match the treatment sample by size and industry), the authors took a matched sample approach that used a t-test and a non-parametric test comparing total assets, number of employees, and annual sales. Overall, no significant differences were found between the publicly traded breached firms and the non-breached firms.

In the aforementioned Section, the event studies in information systems privacy breaches were discussed. The following Section in this chapter discusses the event studies on information systems security breaches.

2.3. Event Studies in Information Systems Security Breaches

In the security area, the results from the event studies are also mixed. Some studies found a statistically significant impact on firm value as a result of information systems security breaches, while others did not. More specifically, two event studies found no statistically significant impact of security breaches on stock returns (e.g., Bolster, Pantalone, & Trahan, 2010; Kannan, Rees, & Sridhar, 2007), while a number of studies found a statistically significant impact of security breaches on abnormal returns (e.g. (Bose & Leung, 2008; Cavusoglu et al., 2004; Chen, Bose, Leung, & Guo, 2011; Garg, Curtis, & Halper, 2003a, 2003b; Gatzlaff & McCullough, 2010; Goel & Shawky, 2009; Gordon et al., 2011; Malhotra & Malhotra, 2011; Morse, Raval, & Wingender, 2011)). The following Section discusses

the aforementioned studies. First, a discussion of the "non-significant" group is put forward, followed by the "significant" group.

Bolster et al. (2010), for example, conducted an event study that combines both privacy and security breaches on a sample of 93 firms. The authors used the market model in order to estimate abnormal returns. Using event windows of (-1, 0), (-1, 0, +1), and (1, 30), and an estimation window of -301 to -46, overall the authors found no statistically significant effect of security and privacy breaches on stock market returns of these companies. Interestingly, even the CARs of stolen data and the loss of social security numbers were not statistically significant. Although the negative abnormal returns are not significant, the authors estimated that the average loss due to a publicly announced breach is around $300 million.

Kannan et al. (2007) conducted an event study on the market reaction to overall impact of information security breaches. Using the CARs computed over 3-day, 8-day, and 30-day event windows, the authors found that none of the CARs are significant. The market reaction to security breaches was further investigated by analyzing the firm size, the type of attack, and the characteristic of the period of attack. Interestingly, the market reactions to confidentiality breaching attacks which are characterized as theft of credit card numbers, source codes, and unauthorized access to websites did not bring in negative abnormal returns. The authors conceded the lack of abnormalities could be due to aggregation of the data of all types of attacks.

The previous two research efforts found that security breaches had no negative and significant impact on stock market value. The research articles discussed next found negative and significant impact on stock market value of security breached firms.

Bose and Leung (2008) conducted an event study on the effect of phishing, online identity theft, announcements on the market value of breached firms. The authors used CAPM to calculate abnormal returns, standardized abnormal returns (SAR), and cumulative standardized abnormal returns (CSAR) on a sample of 2994 phishing attacks derived from publicly available news repositories (e.g., Millersmiles, Hong Kong Monetary Authority, and Malaysia Computer Emergency response team). The authors further used an event window of 3 days [-1, 1] and an estimation window of 200 trading days [-

230, -31]. Overall, the authors found significant and negative effects of phishing announcements on stock returns. Further, the authors noticed that among all the companies investigated, holding companies had the highest CSAR value of -7.3 and subsidiaries had the lowest but significant CSAR value of -3.4.

Cavusoglu et al. (2004) assessed the effect of security breach announcements on the market value of 78 firms. The authors also investigated the effect of these breaches on the market value of security apparatus developing firms. In order to calculate the abnormal returns, the authors used the market model with an estimation window of 160 days ([-160, -1]) and an event window of two days ([0, 1]). The authors found that security breach announcements in general are negatively associated with abnormal stock returns of the breached firms. Furthermore, this association is stronger for the net firms than for the conventional firms and, in particular, there is a positive association between these announcements and the abnormal returns of the security developing firms.

Chen, Bose, Leung, and Guo (2011) found a negative and significant impact as a result of phishing attacks (a form of security breach). The authors estimated abnormal returns using a single-factor market model, with an estimation window of 200 trading days and an event window of 3 days surrounding the event. Chen et al. investigated the severity of the security breaches with a numerical experimentation using a 3 x 3 x 2 experimental design. The experimental design consisted of three sets of input data, three classifiers, and two classification tasks. As outputs, the authors used CAR and Risk Level (as per the classification by Millersmiles). The Millersmiles database is a repository of phishing and spam emails. The authors found that there is no clear relationship between a high risk attack and CAR.

Garg et al. (2003a) used an event study to compare the impact of both privacy (e.g., denial of service attacks) and security (e.g., theft of credit card information) breaches on stock market returns of some publicly traded breached companies. Using a sample of 22 events, an estimation window of a year worth of trading days immediately preceding the day of the event, and 3 event windows of [0], [0, +1], and [0, +2], the authors found a negative 9.3% abnormal returns on the day of the attack increasing to a negative 14.9% abnormal returns on the second day after the attack. Interestingly, the authors found no significant abnormal returns for the privacy breach attacks on Microsoft. In a similar study by the same

authors in (2003b), using a homogeneous sample of 22 events, negative and significant abnormal returns due to the privacy breaches was observed.

Gatzlaff and McCullough (2010) performed an event study for analyzing the impact of data breaches on shareholder wealth. The authors calculated expected returns using a one-factor market model with a 245 estimation period and several event periods, ranging from -5 to 180 days relative to the event day. The sample consisted of 77 data breaches suffered by firms from the period of 2004 to 2006. Overall, the authors found evidence of a negative and significant impact on shareholder wealth as a result of a data breach. The authors supported the notion that firms that are less forthcoming about the details of the data breach are penalized the most. Other important findings lie in the role of the firm size and the subsidiary status in mitigating the negative effects, and that the significance of the negative effect on shareholder wealth is more prominent for the most recent events.

Goel and Shawky (2009) also put forward a study combining both, security and privacy breaches (e.g. malicious code, stolen hardware, and insider attack). The authors used a single-index market model and Fama-French's three-factor model with a sample of 168 events over the period of 2004-2008. The estimation windows consisted of 255 days with an event window of [-119, 10]. The authors found that security breach announcements are associated with 1% negative and significant abnormal returns during the days surrounding the event day.

A recent research effort by Gordon et al. (2011) classified security incidents in three categories (i.e. confidentiality, integrity, and availability) and used these as one holistic category that included all three sub-categories. The events collected by the authors are from the time period of 1995 to 2007, excluding incidents from 121 trading days after 9/11. The authors excluded these events due to the high market volatility with the potential to introduce bias in the analysis. The final sample is composed of 121 events. The authors employed the traditional single-index model and Fama-French's three-factor to estimate expected returns. For both models the estimation window consisted of 121 days and 3 days for the event window ([-1, 1]). The authors found that security breaches, as a generic category (e.g. confidentiality, integrity, and availability), had a negative and significant impact on firm's market returns An interesting finding of the study is that, when the breaches were tested as a single category, the

authors found a statistically significant negative impact on abnormal returns, the same result was found for the availability sub-category. Breaches threatening confidentiality or integrity, however, were found to be not statistically significant.

Malhotra and Malhotra (2011) investigated the effect of customer information breaches as service failures using an event study methodology. The authors found evidence of a short and long-term decline in the market value of breached firms. This relationship is positively related with the magnitude of the breach, as measured by the number of customers' data breached. The authors employed a single-factor model and a four-factor model (introduced by (Carhart, 1997), with a sample of 93 events post year 2000. The estimation period for both models was 200 trading days and the authors used multiple event windows to provide detail in both the short and the long-term horizons.

Morse, Raval, and Wingender (2011) found a negative and statistically significant impact on stock returns as a result of security breaches. The financial industry suffered the greater consequences in negative abnormal returns across the different industries studied in the present research. The sample consisted of 306 events ranging from the time period of 2000 to 2010. The sample was furthermore divided into three categories based on the nature of the attack, these categories were stolen laptops (n=88), fraudulent access (n=43), and hacking (n=34). The abnormal returns were calculated using a single-factor model with an estimation window of 255 trading days, and an event window of 2 days.

The mixed findings in the area of information systems security breaches could be as a result of a number of factors. As previously mentioned, one factor is the lack of a clear definition of what constitutes a security or privacy breach. Another factor is that different studies used different estimation windows and event windows. Third, the sample sizes varied significantly in size, which could also affect the validity of the findings.

2.4. Event Studies in Abnormal Trading Volume Changes

In the information systems area, only one event study analyzed the effect on abnormal trading volume due to privacy breaches (Nicholas-Donald et al., 2011). This Section of the literature review, as such, relies mostly on the work done in the finance and accounting areas. A number of studies in these areas investigated whether an event had caused abnormal trading volume. In the area of finance and

accounting, abnormal trading volume was investigated in the context of capital gains tax rate reduction (Bali & Francis, 2010), around earnings announcements (Bamber, Barron, & Stevens, 2010; Frazzini & Lamont, 2007; Hope, Thomas, & Winterbotham, 2009), when stocks are added to a market index (Biktimirov, Cowan, & Jordan, 2004), on-line stock search intensity (Joseph, Babajide Wintoki, & Zhang, 2011), and national elections (Bialkowski, Gottschalk, & Wisniewski, 2008). This Section concludes with a discussion on the research put forward by Karafiath (2009). The author validated the use of ordinary least squares in estimating abnormal trading volume. The aforementioned studies are discussed next.

Nicholas-Donald et al. (2011) analyzed the effect of privacy breaches on abnormal trading volume. The authors used a sample of 29 privacy breaches. The abnormal volume was calculated based on the work of Yadav (1992), where abnormal trading volume is calculated by comparing the volume during the event-window [-1, 1] and post event trading volume (60 trading days). The authors found that trading volume decreased in the post-event period compared to the volume in the event-window. The significance of this change was not provided in the preliminary results.

Bali and Francis (2010) investigated the reaction in ex-day trading volume resulting from capital gains tax rate reduction from 28% to 20%. The final sample consisted of 18,358 numbers of observations. The abnormal trading volume was estimated using the following procedure: first, an average of the trading volume over 80 trading days ([-45, -6], [6, 45]) relative to the ex-day (day [0]) was calculated. The standardized excess volume (SEV) was then computed by scaling the excess volume for each of the 11 days surrounding the event [-5, 5]. Finally, the cumulative standardized excess volume (CSEV) was computed by aggregating all SEVs. The authors divided the events into high-yield and low-yield groups in the pre and post event periods, respectively. The authors found, for both events, the abnormal trading volume in the days around the event. The CSEV felt by about 26% in the days after the event.

On average, stock prices rise around the scheduled earnings announcement dates. Bamber, Baron, and Stevens (2010) show that earning announcements premium is large, robust, and related to volume surges around the announcement dates. They also found that stocks with the high past

announcement period volume earn the high announcement premium. This suggests that there is a common underlying cause for both the volume and the premium surge. The authors found that this premium surge is related to buying by small investors.

As stated earlier, it is well-known that, on average, stock prices rise around the scheduled earnings announcement dates. Frazzini and Lamont (2007) found that the magnitude of premium around earning announcements is between 7% and 18% per year and is not confined to the 3-day window around the announcement day. They show that this predictable rise in stock prices is driven by a predictable rise in abnormal volume around the earning announcement day. They also show that stocks with high past volume earn the high premium and high volume. They further show that this high volume is driven by buying by small investors.

Hope, Thomas, and Winterbotham (2009) examined the impact of geographic earnings disclosures and trading volume. Geographic earning disclosure is defined as a multinational firm disclosing in their annual report the allocation of earnings in terms of geographical dispersion. Using a sample of disclosing and non-disclosing geographic earnings by firms with significant foreign operations, the authors find a relationship between the decrease in trading volume and non-disclosure of geographic earnings.

Biktimirov, Cowan, and Jordan (2004), investigated as to whether the firms added to or deleted from the small cap Russell 2000 index go through similar changes in returns and trading volume. This study is interesting because the Russell 2000 has a number of advantages over the S&P 500 on the effect of index membership. Some of these advantages are that the additions to the Russell 2000 occur on a regular annual basis, the S&P 500 additions occur irregularly. The Russell 2000, also has more additions than the S&P 500, resulting a larger sample size to be used for the analysis. Using an estimation period of 200 days ([-479, -280]) before the reconstitution day and 81 event days centered on the reconstitution day on large samples of pure additions and pure deletions, Biktimirov et al. (2004) found a clear and significant evidence of a high abnormal volume for both sets during the reconstitution day.

Joseph, Wintoki, and Zhang (2011) examined the effect of online search intensity on abnormal stock returns and trading volume. Using a sample of S&P 500 firms for the time period of 2005-2008,

the authors found evidence that the search intensity predicts abnormal returns and trading volumes. An interesting finding is that the sensitivity to search intensity is lowest for easy to arbitrage, low volatility stocks and higher for difficult to arbitrage, high volatility stocks. The authors shed light on our understanding of the impact of real-time information provided by online searches in abnormal returns and trading volume.

In an interesting twist, Bialkowski, Gottschalk, and Wisniewski (2008) investigated whether politics can influence finance by focusing on the impact of national elections on stock market volatility. Using an event study with a one day event window which is either the Election Day or the first trading day after the election, the authors found a strong abnormal rise in volatility on the Election Day. This country-specific return volatility stayed high for a number of days after the election based on the fact that final election results may not be available for those days and could easily double in the week around elections.

In an effort to validate the extent research in the areas of accounting and finance examining the abnormal trading volume due to new information, Karafiath (2009) offered several alternative tests statistics as an alternative to the popular single-index market model. The authors relied in simulations of random sample of securities collected from CRSP. The authors concluded that using generalized least squares with first and second order auto-regressive structures does not have a significant impact on improvement from ordinary least squares regression (OLS). The authors, therefore, validated the calculation of abnormal trading volume using the traditional single-index market model using OLS.

In the aforementioned Section, the studies investigating abnormal trading in the areas of information systems, finance and accounting were discussed. In the following Section, the literature in risk shifts is discussed for the same areas.

2.5. Risk Shifts

With exception of research studies conducted by Nicholas-Donald et al. (2011), no other studies in the information systems area have conducted an analysis of risk shifts as a result of privacy breaches. The authors used a sample of 29 privacy breaches. The risk shifts was calculated based on the work of Yun and Kim (2010), where risk shift is measured by comparing the betas before the event-window and

post event betas (250 trading days on each time period). The authors found an increase in betas, indicative of increased risk, from the pre-event to the post-event periods. The statistical significance of this change was not provided in the preliminary results.

In the finance and accounting literatures risks shifts as a result of an event have been explored extensively. In the finance literature a couple of research studies, for example, examined how the inclusion in the S&P 500 index affected firm risk (e.g. (Barberis, Shleifer, & Wurgler, 2005; Patton & Verardo, 2009)). In a similar vein, Yun and Kim (2010) analyzed the risk shift of firms as a result of being included in the KOSPI 200 index. Kleidt and Schiereck (2009), on the other hand, examined the impact of an issuance of convertible debt on systematic equity risk. These studies are discussed next.

Barberis, Shleifer, and Wurgler (2005) analyzed additions to the S&P 500 in order to compare the two views of return comovement: traditional, which means attributing comovement in news about fundamental value and an alternative view, that means delinking from fundamentals. The data was collected from S&P 500 index inclusions over the period of September 22, 1976 and December 31, 2000. The sample consisted of 455 inclusions in daily and weekly data, and 324 in monthly data. In order to test their predictions, the authors first ran univariate regressions, one prior to the inclusion (or deletion) of a stock into the S&P 500 index and one after. Comovement from these two univariate regressions was analyzed in order to test for friction or sentiment-based views. The authors found that after the inclusion in the S&P 500 index, a stock's beta increases. Using a bi-variate regression which controls for the return of non-S&P 500 stocks, the increase in risk (as measured by beta) is even larger. They used the bi-variate regression test to compare and contrast the traditional view from the alternative view. These results were stronger because the authors used a bi-variate regression methodology.

Patton and Verardo (2009) analyzed the beta on days of firm-specific news announcements. The sample consisted of all stocks included in the S&P 500 index during January 1995 and December 2006, resulting in a sample of 810 companies. The events analyzed by the authors are the earning announcements of these companies during the aforementioned time period. In order to estimate for changes in betas the authors used a panel regression approach across the entire sample of stocks. The

authors found evidence of a statistically significant change in systematic risk due to firm-specific news, this change reverts to a normal levels after two to five days after the announcement.

Yun and Kim (2010) examined the effect of inclusions or deletions of stocks in the KOSPI 200 index. In order to analyze the impact of the changes in the KOSPI 200 index, volatility and beta changes were examined. The KOSPI 200 index changes started in June 1995 and extends to June 2008, during this time period, the authors identified 2777 regular changes of stocks in the index. The sample was divided in two subsets; one corresponds to events from 1995 to 2001 and the second group from 2002 to 2008. The authors calculated abnormal returns using a one-factor market model and a Fama-French's three-factor model. In calculating the volume patterns, the authors used the mean relative dollar volume ratio. This ratio "...measures each day's relative dollar volume ratio to each stock's past dollar volume to market" (Yun & Kim, 2010, p. 261). In order to test for beta changes, the authors adopted the methodology suggested by Barberis et al. (2005) (i.e. a univariate model). The authors found evidence of abnormal trading activity due to changes in the KOSPI 200 index and a statistically significant increase in daily betas.

Kleidt and Schiereck (2009), as stated earlier, examined the impact of issuance of convertible debt on systematic equity risk. A convertible debt is a type of debt that could be converted for another type of security. The authors found evidence that the issue of convertible debt impose a significant increase in systematic risk. The data consisted of convertible debt issues (CD) and seasoned equity offerings (SEO) from the time period of January 1, 2000 to December 31, 2002 from companies traded in the US. In order to estimate systematic equity risk, the authors used a standard one-factor market model with an estimation window of 250 trading days.

In the aforementioned Section, the studies investigating the impact of a number of events on risk shifts were discussed. In the following Section, a discussion of other event studies in the areas of information systems, accounting, and finance are discussed.

2.6. Other Relevant Event Studies in Information Systems, Accounting, and Finance

Within the area of information systems, a number of studies have been identified that are relevant to the present research (e.g. (Bharadwaj, Keil, & Mähring, 2009; Hovav, Andoh-Baidoo, &

Dhillion, 2007; Hovav & D'Arcy, 2005; Telang & Wattal, 2007). In the finance area, Gillet, Hübner, and Plunus (2010) operationalazed the losses from reputational damage as a result of operational losses reported by financial companies. The following studies employed an event study methodology and the events analyzed are similar to security and privacy breaches (e.g. defective IT products, IT failures, and software vulnerabilities). The similarity draws upon the expected negative impact of the event on the firm's returns. These studies are discussed next.

Bharadwaj, Keil, and Mähring (2009) used a combination of an event study methodology and the resource-based view of the firm theory to analyze the impact of IT failures on the firm value. The authors used a sample of 213 IT failures during the time period of 1990 to 2000. The authors utilized the one-factor market model with an estimation period of 120 trading days ([-120, -2]) and 2-day event window ([-1, 0]). They found support for the hypothesis that IT failures lead to abnormal returns (around 2% on average). The authors also found that the severity of the IT failure is positively correlated with negative abnormal returns. Another interesting finding of the study is that those firms with a previously reported IT failure experience a greater impact on negative abnormal returns.

Hovav, Andoh-Baidoo, & Dhillion (2007) analyzed the impact of security breaches on stock returns. The focus of the research was to evaluate whether the attacker type, attacker's objective, the results of the attack, the attack tools, and access types had played a role in determining the magnitude of the impact on stock returns. The authors found evidence that the different attack characteristics have an impact on the magnitude of abnormal returns. The authors also found that breaches resulting in the disclosure of private information had a significantly larger effect on the market reaction.

Hovav and D'Arcy (2005) studied the effect of defective IT products on the market value of the firm. The focus is on whether the market penalizes firms producing substandard IT products. In the study, the authors considered substandard products are those flawed and blamed for the increase of computer viruses. The sample consisted of 92 events over the period of 1988 to 2002. In order to estimate normal returns the authors used a single-index market model with an estimation window of 200 daily returns, and five different event windows ([0], [0,1], [0,5], [0,10] and [0,25]). The authors found

that IT vendors are penalized by the market only for distributing software with embedded viruses, as opposed to those facilitating the spreading of computer viruses using other means.

Telang and Wattal (2007) investigated the impact of software vulnerability announcements on a firm's stock price. The authors compiled a sample of 147 vulnerability announcements between 1999 and 2004. In this study, the authors used three models in order to estimate expected returns: market-adjusted model, mean-adjusted model, and mean model. The estimation period consisted of 160 trading days and the event window consisted of only one day ([0]). The results suggest that software vulnerability disclosures have a negative and significant impact on the stock performance of vendors. The negative impact on the stock performance was found to be positively correlated with the severity of the vulnerability.

Gillet, Hübner, and Plunus (2010) attempted to operationalize the losses from reputational damage as a result of operational losses reported by financial companies. Using a sample of 154 events occurred between 1990 and 2004 on major European and US Stock Exchanges; the authors found significant and negative abnormal returns on the announcement date of the operational loss. The authors used a 250 trading days for the estimation window and a one-factor market model to estimate abnormal returns. The authors found that the financial companies had experienced a 7% decrease in cumulative abnormal returns and 4% decrease in CAR due to Clients Products and Business Practices (CPBP).

In summary the research on the impact of security and privacy breaches, as can be seen from the aforementioned discussion of relevant research studies, are not conclusive and comprehensive. The objective of the present dissertation is three-fold: first, to avoid confounding the impact of privacy and security breaches, the present research divides the security and privacy breaches into two clear cut categories based on the well-established definitions of these breaches and analyze the data accordingly. No research studies, at least in the information systems area, have done so. Second, in addition to using abnormal stock market returns, the present research employs abnormal risk and abnormal trading volume to systematically and conclusively analyze the impact of privacy and security breach announcements into two clearly defined categories. No research studies in the information systems area have conducted a comprehensive privacy or security breach study. Third, the present research is the first

attempt in conducting a comprehensive and comparative study on the security and privacy categories. This is done using abnormal stock market returns, risk, and treading volume.

Chapter 3: Hypotheses Development

All hypotheses included in the present dissertation are grounded in theory and in previous research. The general theme of the hypotheses in the present research is that the impact from security breaches is more serious than privacy breaches in terms of abnormal returns, volume, and risk measures for a number of reasons. First, the consequences of stealing social security numbers, bank account numbers, credit card numbers, and driver's license numbers are expected be more serious than those for denial of service attacks, hacker attacks, virus attacks, and website defacements. This is due in part, to the potential for law suits and decreased credibility from security attacks. Second, security breaches require breaking through firewalls and other intrusion prevention and detection systems, which means that investors are expected to treat these breaches as more serious and they are more likely to punish the companies by perhaps selling their stocks.

The rest of this Chapter is divided into three Sections. First, Section 3.1 constitutes an analysis of publicly announced privacy and security breaches, each analyzed individually. This is followed by Section 3.2 that deals with the comparative analysis of publicly announced privacy and security breaches.

3.1. Analysis of Publicly Announced Privacy and Security Breaches

In this Section, the impact of privacy and security breaches are analyzed independently. The theme of the hypotheses in this Section is tested by security and privacy breaches groups. Upon analyses of these breaches as separate categories, these will be compared and contrasted against each other with a set of hypotheses put forward in Section 3.2 below.

The Efficient Market Hypothesis posits that all publicly available information is absorbed in a stock's price. The public announcement of an information system privacy or information system security breach, in general, is expected to have a negative impact on the stock of the breached firm. In the present dissertation research, the publicly announced information privacy or security breach on a publicly traded company is expected to have a negative impact on three aspects. First, it will result in negative abnormal returns. Second, it is expected to result in abnormal trading volume. Third and lastly, there is an

expectation of increased risk shifts surrounding the breach. In the information systems literature, as previously discussed, the findings suggests that there is no consensus on whether a privacy or security breach leads to negative abnormal returns (see Chapter 2). Some studies have found a negative and significant abnormal returns due to privacy (Acquisti et al., 2006; Campbell et al., 2003; Ettredge & Richardson, 2003; Khansa & Liginlal, 2011; Nicholas-Donald et al., 2011) or security (Bose & Leung, 2008; Cavusoglu et al., 2004; Chen et al., 2011; Garg et al., 2003a, 2003b; Gatzlaff & McCullough, 2010; Goel & Shawky, 2009; Gordon et al., 2011; Malhotra & Malhotra, 2011; Morse et al., 2011) breaches.

Therefore, based in the previous discussion, the following hypotheses are put forward:

H1a: *A clearly defined information privacy breach will have a significant negative impact on the stock market value of the firm when such a breach becomes public.*

H1b*: A clearly defined information security breach will have a significant negative impact on the stock market value of the firm when such a breach becomes public.*

An important factor an investor evaluates while making an investment decision is the level of risk associated in the underlying asset. The beta coefficients in the CAPM provide an estimate that represents the stock's volatility in relation to the overall stock market. This beta is a proxy of risk. In the present research, a firm's risk is expected to increase as a result of a privacy or a security breach. In this capacity, only one forthcoming research has performed a risk shift as a result of a security breach (Cardenas, Coronado, Nicholas-Donald, Parra, & Mahmood, 2012) and one in the privacy area (Nicholas-Donald et al., 2011). Nicholas-Donald et al. (2011) found that the betas for publicly traded firms incurred in an increase of its betas after a publicly announced privacy breach.

Based on the aforementioned discussion, the following hypotheses are put forward:

H2a: *A clearly defined information privacy breach will result in a significant increase in firm's risk as measured by its betas when such a breach becomes public.*

H2b: *A clearly defined information security breach will result in a significant increase in firm's risk as measured by its betas when such a breach becomes public.*

An additional analysis, that in combination with abnormal returns provides a more detailed view of the market behavior, is that of abnormal trading volume. Past research have suggested that abnormal trading volume is present surrounding earnings announcements (Bamber et al., 2010; Frazzini & Lamont, 2007; Garfinkel & Sokobin, 2006), surrounding capital gains tax rate reductions (Bali & Francis, 2010), when stocks are added to a market index (Bialkowski et al., 2008), and as a result of a privacy breach (Nicholas-Donald et al., 2011). As in abnormal returns and risk shifts, no research study in the information systems area measures abnormal trading volume due to publicly announced security breaches. Therefore, an emphasis in the accounting and finance areas in order to put forward hypotheses related to abnormal trading volume were cited. An exception, in the information systems security area, is the study of Nicholas-Donald (2011). In this study, the authors investigated the abnormal trading volume due to a privacy area. In the research by Nicholas-Donald et al. (2011) firms suffering a privacy breach suffer post-event abnormal trading volume. The authors, however, did not conduct a test to assess if this change is statistically significant. In the finance area, for example, Yun and Kim (2010) investigated the effect on trading volume as a result of changes in the KOSPI 200 Index composition. The authors found that when a firm's stock is added to the KOSPI Index, firm's trading volume increases significantly during the event period and stays high even after the event has taken place. Similarly, abnormal trading volume is observed for firms that have been deleted from the Index.

The discussion above lead to the following hypotheses:

H3a*: A clearly defined information privacy breach will result in a firm's significant abnormal trading volume when such a breach becomes public.*

H3b*: A clearly defined information security breach will result in a firm's significant abnormal trading volume when such a breach becomes public.*

This Section put forward a set of hypotheses in order to test the abnormal returns, abnormal trading volume, and risk shifts due to privacy or security breaches. These hypotheses are tested for each of the two types of breaches in separate groups. The following Sections puts forward a group of hypotheses aimed to make a comparative analysis between the privacy and security breaches. This will

shed light on how the two breaches compare and contrast in terms of the abnormal returns, abnormal trading volumes, and abnormal risks.

3.2. Comparative Analysis of Publicly Announced Privacy and Security Breaches

In this Section, the present research now provides rationale and literature support for each of the hypotheses in what follows. It is expected that due to the nature of the breached assets, security incidents will result on higher negative abnormal returns. Farahmand, Navathe, Sharp, and Enslow (2004) found evidence that the degree of confidential data and the impact in the market value of firms are related. Garg et al. (2003a; 2003c) also found evidence that confidentiality breaches, related to credit card information, are the types of breaches with the highest negative impact in the market value of the breached firms. Campbell et al. (2003) found evidence of a negative and significant relationship between confidentiality related breaches and firm market value, and non-significant for non-confidentiality breaches. Bose and Leung (2008) found that phishing attacks, a type of security breach, resulted in a negative and significant impact on abnormal returns. Hovav and Andoh-Baidoo (2007) found that breaches resulting in the disclosure of private information resulted in a greater impact in the market, this analogous to the definition of a security breach in the present research. Similarly, Gatzlaff and McCullough (2010) found that data breaches had a negative and significant impact on shareholder wealth. Bharadwaj et al. (2009) found that more severe IT failures lead to a higher negative abnormal return. These lead to the following hypothesis:

H4: *Security breach incidents will result in significantly higher negative abnormal returns than privacy incidents.*

The second hypothesis follows a similar line of thought. It is expected for a firm to become riskier if it has a security or privacy breach incident. It is also expected for a firm to incur more negative abnormal returns for security breaches than for privacy breaches. As previously mentioned, the NIST classified security breaches in the present research, are considered to have a higher level of potential impact than privacy breaches. Similar changes in risk are found in the finance and accounting areas. Brennan and Copeland (1988), for example, found evidence of risk change around stock split announcements. Ball and Kothari (1991) and Patton and Verardo (2009) performed an analysis on beta

changes as a result of earning announcements, the authors found a statistically significant risk shift as measured by beta. Nicholas-Donald et al. (2011) found evidence of risk shifts as a result of a privacy breach. Based on the aforementioned discussion, the following hypothesis is put forward:

H5: *Security breach incidents will result in a significantly higher risk increase (as determined by beta) than privacy incidents.*

While abnormal announcement returns and risk shifts reflect a change in the average investors' beliefs, abnormal volume reflects the difference in the marginal traders' reactions to a security or privacy breach announcement. These differences could come from differential interpretation or differential pre-announcement beliefs. Regardless, more studies need to be conducted in the area because of trading volume's potential to yield new insights on the impact of security and privacy breach areas. Only one study by Nicholas-Donald et al. (2011), as stated earlier, have been conducted on this topic in the information systems area. The authors found that trading volume decreased as a result of a privacy breach. Trading volume is relatively unexplored in capital market research even in the accounting and finance areas (Bamber et al., 2010). Nevertheless, there are a few studies that examine abnormal trading volume. Biktimirov et al. (2004) found, for example, a clear and significant evidence of abnormally high volume for a large sample of publicly traded companies that are added to or deleted from the small cap Russell 2000 index. Bali and Francis (2010) found evidence of an increase of about 26% on trading volume, using cumulative standardized excess volume, as a result of capital gains tax rate reductions. Similarly, Bamber et al. (2010) found trading volume surges as a result of earning announcements. Therefore, the following hypothesis is proposed:

H6: *The security breach incidents will result in a significantly higher abnormal volume than privacy incidents.*

These hypotheses put forward will be tested using a variety empirical analysis. In the next chapter, the research method and sample selection used in order to test the aforementioned hypotheses are put forward.

Chapter 4: Research Method and Sample Selection

This Chapter is also divided into multiple Sections. The first Section (i.e.4.1) explains the process of collecting the data for this dissertation. This is followed by several Sections explaining each of the different methods used to test the hypotheses put forward in Chapter 3. Section 4.2 explains how abnormal and cumulative abnormal returns are calculated using the one factor market model. Section 4.3 describes an alternate process of calculating abnormal and cumulative abnormal returns using Fama and French's three factor model. In Section 4.4 the process followed to compute cumulative abnormal returns is put forward. Section 4.5 illustrates the process followed in order to estimate risk shifts. Lastly, Chapter 4 concludes the Section in 4.6 by putting forward how abnormal trading volume is calculated.

4.1. Data Selection

The data for the present dissertation was found by searching the Lexis-Nexis Academic database for possible security or privacy breaches between the years 1999 and 2009. Major US publications were selected as the sources of the events. The events were collected using the following search strings to identify the events: 1) Cybersecurity; 2) Hacker Attack; 3) Information Security (breach or incident); 4) Computer Security (breach or incident); 5) Network Security (breach or incident); 6) Internet Security (breach or incident); 7) Privacy (breach or incident); and, 8) Denial of Service.

For a firm to be included in the sample, it is required that financial statement of the firm be available in the Compustat database, and returns be available in the Center for Research in Security Prices (CRSP) database. The firms were also analyzed for confounding events, such as earning announcements during the event window. Using the above filters, a sample of 114 security (65) and privacy (49) breaches was selected in the present dissertation research. The sample consisted of events that occurred between June 23, 1997 and October 28, 2009. The rest of this chapter describes the different methodologies employed in order to test the proposed hypotheses.

4.2. One Factor Market Model

In this Section, the process of estimating abnormal returns using a one factor model is explained. Abnormal stock returns in this dissertation, is based on a one-factor model and Fama-French's three

factor model (see Section 4.3) to estimate expected returns. The market model is based on the Capital Asset Pricing Model (CAPM). Estimation of expected returns uses an ordinary least squares (OLS) regression where the dependent variable is the return for stock (*i*) at time (*t*) and the independent variable is the market index for the same time (*t*) (see Equation 1 below).

$$R_{i,t} = \alpha + \beta_i R_{m,t} + \varepsilon_{i,t} (1)$$

where, R_i,t is the return for firm *i* on day *t;* $R_{m,t}$ is the return on the market portfolio on day *t;* a_i and b_i are parameters in the model; and, $\varepsilon_{i,t}$ is the disturbance term.

An estimation period of at least 120 days is required for each entry in the sample, beginning 251 trading days (a full calendar year) before the event day identified as day 0 (Benninga, 2008). All but 1 of the 33 sample firms used in the present research has a full 250 days of return data (i.e. [-251, -1]). The CRSP value-weighted index is used as a proxy for the market portfolio. The value-weighted index is weighted by the market capitalization and contains the returns, including all distributions of a portfolio. Once the regression coefficients are estimated, the expected returns are subtracted from the observed returns to obtain the abnormal returns (see Equation 2 below):

$$AR_{i,t} = R_{i,t} - (\hat{\alpha} + \beta_i R_{m,t}) (2)$$

where, $AR_{i,t}$ is the abnormal return for firm *i* on day *t;* R_i,t is the return for firm *i* on day *t;* $R_{m,t}$ is the return on the market portfolio on day *t;* and a_i and b_i are the parameters estimated in the model.

4.3. Fama-French's Three-factor Model

An alternative model to the one-factor market model in estimating returns is the Fama-French's three-factor model. The three-factor model was introduced by Fama and French (1993, 1996). This model builds from one-factor model and adds two more factors (i.e. firm size and value), hence known as the three-factor model. This model was introduced with the purpose of developing a methodology that could better explain returns. Firm size is operationalized by market capitalization and value by the book-

to-market ratio. The Equation (3) is used to estimate expected returns based on Fama and French's three-factor model:

$$R_{it} - RF_t = a_i + \beta_i(RM_t - RF_t) + s_i SMB_t + h_i HML_t + e_{it} (3)$$

where, R_{it} is the return for firm *i* on day *t;* RF_t is the risk-free rate on day *t*; RM_t is the market return on day *t;* SMB_t is the difference between the return on a portfolio of small stocks and the return on a portfolio of large stocks on day *t* (small minus big); HML_t is the difference between the return on a portfolio of high-book-to-market stocks and the return of on a portfolio of low-book-to-market stocks on day *t*; a_i, b_i, s_i, h_i are the Fama and French parameters estimated in the three-factor model for firm *i*; and, e_{it} is the disturbance term from the regression.

A few studies in the past have used the three-factor by Fama and French (e.g. Goel & Shawky, 2009; Gordon et al., 2011) as a robustness test. The purpose of a robustness test is to explain the same phenomena with alternative models. The idea is that if the results are similar, then the model should be robust. Once the expected returns are calculated using the Fama-French's three factor model, abnormal returns are calculated as explained at the end of Section 4.2. This model was used as a robustness test of the one-factor market model as also explained in Section 4.2. The following Section explains how cumulative abnormal returns are calculated.

4.4. Cumulative Abnormal Returns

Abnormal returns may occur over a multi-day period. This is because of the fact that markets may not fully absorb information instantaneously, and/or that the event may not be reported immediately. Cumulative abnormal returns are computed in the following fashion to account for this phenomenon:

$$CAR = \sum_{t}^{t+n} AR_{i,t} (4)$$

Two variations of CAR, for robustness purposes, are computed. First, CARs are estimated using the market model. Second, CARs were also calculated using the Fama-French's three factor model. The

CARs, were also transformed using two techniques, winsorization, and natural log of CAR + 1. Winsorization is a process of handling extreme observations with the purpose of reducing its possible effect in the results.

4.5. Beta Changes (Measure of Risk)

This Section explains the process in estimating the risk incurred as a result of a privacy or a security breach. Beta changes are used in the finance and accounting literature as a measure of risk shifts (e.g. (Barberis et al., 2005; Patton & Verardo, 2009; Yun & Kim, 2010)

The calculation of beta changes follows a similar process explained in the Abnormal Returns Section 4.2. A one-factor model (Equation 1) and the Fama-French's three factor model (Equation 3) are employed to estimate the firm's beta both before [-251, -1] and after [1, 251] the event. Then, the post-event beta is standardized by the pre-event beta (Equation 5), producing a ratio that should equal one if the event had no impact on the risk of the firm.

$$\beta_{ratio,i} = \frac{\beta_{post,i}}{\beta_{pre,i}} (5)$$

4.6. Abnormal Trading Volume

Finally, abnormal volume is calculated as a third measure of abnormal activity in the firm's equity during the event. Abnormal trading volume is calculated as suggested by Yun and Kim (2010) and Beneish and Whaley (1996). The authors scaled the average event daily volume (see Equation 6) by the average pre-event (see Equation 7) daily volume (the present research used a 60-day period [-61, -2]). If trading volume in the event period is normal, the ratio should equal one (see Equation 8). The following Equations (6-8) were used in order to estimate the trading volume as per Yun and Kim (2010) and Beneish and Whaley (1996) method:

$$During - event_{volume,i} = \frac{\sum_{t=-1}^{t=-1} tradingvolume_{i,t}}{3} (6)$$

$$Pre - event_{volume,i} = \frac{\sum_{t=-61}^{t=-2} tradingvolume_{i,t}}{60} (7)$$

$$Volume_{ratio,i} = \frac{During - Event_{volume,i}}{Pre - event_{volume,i}} \quad (8)$$

Chapter 5: Results

In this Chapter, the results and a discussion of the results is put forward. The results are centered on the theme of the proposed hypotheses described in Chapter 2. The first Section 5.1 puts forwards the results pertaining the publicly announced privacy breaches. This is followed by Section 5.2, where the results related to the publicly announced security breaches are shown. The third and last Section 5.3 of this Chapter provides a comparative analysis of privacy and security breaches.

5.1. Results of Publicly Announced Privacy Breaches

Table 1 provides the results for H1a for the present dissertation research. The empirical analysis of 49 privacy breaches provided an average CAR of +1.22%. This positive abnormal return is statistically significant at an acceptable p-value. The results shown in Table 1 were calculated using the one-factor market model.

Table 5.1: The Means Test for Cumulative Abnormal Returns for Privacy Breaches

N	Mean	t-value	Pr > |t|
49	0.0122	1.7404	0.0882

The risk shift was observed by analyzing the changes on pre-and post-betas. A one-factor CAPM model, as explained by Yun and Kim (2010), was used to calculate pre- and post-betas. Both, the pre- and post-betas were calculated using the 250 trading days surrounding the event announcement day. The means test results for the prior-and post-event betas are shown in Table 5.2. The analysis shows that the risk of firms that experienced a privacy breach has decreased after its announcement. This risk decrease is observed in the beta ratio (see Equation 5 in Section 4.5), where the expectation for normal trading volume is a ratio of 1. In this case, the ratio is below 1, indicative of a decrease in risk as measured by betas.

Table 5.2: The Means Test for Beta (Privacy Breaches)

N	Mean	t-value	Pr > |t|	Description
49	1.5790	15.1074	<0.01	Pre-event beta
49	1.4741	16.6022	<0.01	Post-event beta
49	0.8808	10.4524	<0.01	Beta ratio

In order to test H2a, the abnormal trading volume experienced by the companies suffering a privacy related breached firms is analyzed. In the present research, as aforementioned, abnormal trading volume is calculated based in the work of Beneish and Whaley (1996) and Yun and Kim (2010). Abnormal trading volume is estimated using Equation 8 in Section 4.6. As previously mentioned, the average trading volume for the 60 pre-event trading days is compared with the volume of the event window (i.e. [-1, 1]) for each privacy breached firm. The privacy breached firms experienced a significant abnormal trading volume of about 7.7% (decrease) during the event window (see Table 5.3).

Table 5.3: Abnormal Trading Volume (Privacy Breaches)

N	Mean	t-stat (p-value)	Method
49	0.9226	14.8882 (<0.01)	Beneish & Whaley, 1996; Yun & Kim, 2010

In this Section, the results obtained related to privacy breaches were presented. In the following Section the results related to publicly announced security breaches will be discussed.

5.2. Results of Publicly Announced Security Breaches

First, the results for the test of Cumulative Abnormal Returns are presented. Second, the results testing the risk shifts are put forward. The third and the last set of results pertain to the abnormal trading volume.

In Table 5.4. the results related to H1b are provided. The empirical analysis of 65 security breaches provided an average CAR of -1.31%. This negative abnormal return has a p-value of 0.1123. The results shown in Table 4 were calculated using the one-factor market model.

Table 5.4: The Means Test for Cumulative Abnormal Returns for Security Breaches

N	Mean	t-Value	Pr > |t|
65	-0.0131	-1.6100	0.1123

The risk shift was observed by analyzing the changes in pre-and post-betas. A one-factor CAPM model, as explained by Yun and Kim (2010) was used to calculate pre- and post-betas. The test results for the prior-and post-event betas, and beta ratio are shown in Table 5.5 below. The analysis shows that the risk of firms that experienced a security breach has significantly increased after its announcement. This risk increase is observed in the beta ratio (see Equation 5 in Section 4.5), where the expectation for normal trading volume is a ratio of 1. In this case, the ratio is above 1, indicative of a decrease in risk as measured by betas due to a security breach.

Table 5.5: The Means Test for Beta (Security Breaches)

N	Mean	t-stat	Pr > |t|	Description
65	1.0476	19.8976	<0.01	Pre-event beta
65	1.0772	18.1182	<0.01	Post-event beta
65	1.1188	11.0369	<0.01	Beta ratio

In order to test H2b, the abnormal trading volume experienced by the companies suffering a security related breached firms are analyzed. In order to estimate abnormal trading volume, the method of Beneish & Whaley (1996) and Yun and Kim (20120) was used (see Equation 8 in Section 4.6). As previously mentioned, the average trading volume for the 60 pre-event trading days is compared with the volume of the event window (i.e. [-1, 0, +1]) for each security breached firm. Using this technique, the security breached firms observed a statistically significant abnormal trading volume of about 1.1% increase in volume during the event window (see Table 5.6).

Table 5.6: Abnormal Trading Volume (Security Breaches)

N	Mean	t-stat (p-value)	Method
65	1.0109	16.5158 (<0.01)	Beneish & Whaley, 1996; Yun & Kim, 2010

In this Section the analyses of publicly announced security breaches are put forward. The analyses followed the theme of the hypotheses. In the following Section a comparative analysis of privacy and security breaches are put forward.

5.3. Comparative Results of Privacy and Security Breaches

In this Section, the comparative results of privacy and security breaches are put forward. Table 5.7 shows that the average cumulative abnormal return for the entire sample is -0.23% (for the three-day [-1, 1]). Similarly, the ratio of the post-event beta over the pre-event beta, for the entire sample, was 1.02. Both abnormal volume measures (mean CSEV = -0.14 and Volume Change Ratio = 0.97) indicate that trading volume around the event is below normal.

Table 5.7: Descriptive Statistics

Variable	**N**	**Mean**	**Median**	**Std. Dev**
Cumulative abnormal return (CAR)	114	-0.0023	0.0040	0.0601
Beta change ratio	114	1.0170	0.9568	0.7349
Cumulative standardized excess volume (CSEV)	114	-0.1446	-0.9480	4.5312
Volume change ratio	114	0.9730	0.9009	0.4688

In Table 5.8 the sample is bifurcated based on whether the event was a security breach or a privacy breach. Panel A shows the mean cumulative abnormal returns. On average, firms experiencing a security breach had a -1.31% CAR while firms that had a privacy breach had a 1.22% increase in CAR. The difference of the CAR averages between the two types of breaches is statistically significant, supporting H1. The results are quantitatively similar when winsorising and log transformation of the data are performed.

The ratio of post-event over pre-event beta is presented in Panel B. The security breach sample has a ratio of 1.12, which is statistically different from the null of 1. The privacy breach group mean ratio is 0.88. The difference between the security and privacy group ratios is statistically significant, at

the 7% level. Clearly it appears that the security group firms suffered an increase in risk and this increased risk is significantly higher than the privacy group. This increase seems to be persistent for the 250 days following the event, as indicated by the beta change ratio. An increase in beta can have a serious impact on the firm's cost of capital and thus lead to lower profitability in the future.

Table 5.8: Comparative Analysis of Study Variables

	N	Mean	t-stat (p-value)
Panel A: Cumulative Abnormal Returns [-1, 1]			
i) Security Breaches	65	-0.0131	-1.61 (0.11)
ii) Privacy Breaches	49	0.0122	1.74 (0.09)
Mean (i) = mean (ii): t-stat = 2.36, p-value = 0.02			
Panel B: Beta Change Ratio			
i) Security Breaches	65	1.1188	11.04 (<0.01)
ii) Privacy Breaches	49	0.8808	10.45 (<0.01)
Mean (i) = mean (ii): t-stat = -1.81 p-value < 0.07			
Panel C: Volume Change Ratio			
i) Security Breaches	65	1.0110	16.52 (<0.01)
ii) Privacy Breaches	49	0.9226	14.89 (<0.01)
Mean (i) = mean (ii): t-stat = -1.01 p-value = 0.31			

Panel C present the abnormal volume measures for each type of event. The ratio of the average daily event volume over the average daily pre-event volume is 1.01 and 0.92 for security and privacy breaches, respectively. This measure suggests that privacy events result in significantly less daily volume. Similar results were obtained when cumulative abnormal returns are calculated using Fama and French's three factor model.

Chapter 6: Discussion and Conclusion

In this Section, the discussion and conclusions of the present research are put forward. This Section is divided in two parts. First, Section 6.1 provides a discussion of the findings. Second, a conclusion of present dissertation research is presented in Section 6.2.

6.1. Discussion

Previous studies attempted to explain the impact of information privacy and security breaches. The results were mixed and there was no definite consensus on whether privacy and security incidents had significant impacted a firm value as measured by its stock prices. In addition, no comparative analysis of privacy and security breaches was conducted. The present dissertation research defines privacy and security breaches using NIST standard. This lessens the ambiguity in the area. In addition, a comparative analysis of privacy and security breaches was undertaken. In this Section, the results from the present research are compared and contrasted to the findings of previous studies.

The present research finds a positive and significant (p=.09) cumulative abnormal returns on the firm value for privacy breaches and, therefore it failed to support H1a. This is in line with studies by Hovav and D'Arcy (2003; 2004) and Ishiguro et al. (2006) who find similar results. This also means that the present research contradicts a number of recent studies (Acquisti et al. (2006), Khansa and Liginlal (2011), and Nicholas-Donald et al. (2011)) that find negative impact on the firm value as a result of a privacy breach. Overall, this may be indicative that investors do not perceive a significant increase in firm risk due to a privacy breach.

In the area of security breaches, the present research find that the security breaches result in a negative but not at a highly significant level. The present research, therefore, moderately supports H1b (p-value of 0.11). Some of the recent research studies found a statistical significant relationship between security breaches and firm value (Bose & Leung, 2008; Chen et al., 2011; Gatzlaff & McCullough, 2010; Goel & Shawky, 2009; Gordon et al., 2011; and Malhotra & Malhotra, 2011; Morse et al., 2011).

The risk shift for the privacy breaches (H2a) were tested, as stated earlier, by analyzing the changes on pre- and post-betas. The analysis for the privacy group shows the risk of firms that

experienced a privacy breach has decreased significantly after its announcement. Once again, this may be an indicative that investors do not perceive a significant increase in firm risk due to a privacy breach. These results are not aligned with the findings of Nicholas-Donald et al. (2011), where an increase in risk was observed. It is important to mention here that the authors, however, did not test if this risk shift was statistically significant. No other studies in the area of Information Systems analyzed risk shifts as a result of a privacy breach. In the finance and accounting areas, however, risk shifts were analyzed in different contexts. Risks shifts, for example, were calculated when a firm's stock is added to a market index (e.g. (Barberis et al., 2005; Yun & Kim, 2010) and when firms issue convertible debt on systematic equity risk (Kleidt & Schiereck, 2009). Both studies found a significant risk increase for the events the authors scrutinized.

In the area of security breaches, the test results show that post-event betas has increased but this increase is not significant (H2b). The present dissertation research is the first empirical study in the information systems area that analyzed the risk shifts due to security breaches. No comparisons can, therefore, be made with other studies in the aforementioned area. Similar findings were, however, observed in the finance area. A study by Amihud, DeLong, and Saunders (2002), for example, found no significant increase or decrease in risk for the acquirers when the authors examined the effects of cross-border bank mergers. The expectation was to observe a risk shift for the acquirers. The study by Howe and Madura (1990) is another example where risk shifts were expected and not observed. In this study, the authors analyzed the risk shifts due to international listings of stocks.

Another important contribution of the present research lies in analyzing the significant impact of privacy breaches on abnormal trading volume (H3a). The present research found support to the hypothesis that privacy breaches resulted in significant abnormal trading volume. The results of the present research agree with the findings of Nicholas-Donald et al. (2011) who found abnormal trading volume as a consequence of a privacy breach. The present research, therefore, support H3a. This phenomenon has been previously studied in the areas of accounting and finance. Studies in these areas have found abnormal trading value as a result of earnings announcements (e.g. Bamber et al., 2010;

Frazzini & Lamont, 2007), capital gains tax rate reductions (e.g. Bali & Francis, 2010), additions to stock indexes (e.g. Biktimirov et al., 2004; Joseph et al., 2011), among others.

Abnormal trading volume with regard to security breaches (H3b) in the present research has increased by 1.1% (p-value < .01). In the area of information security breaches, the present research is the first in testing abnormal trading volume due to a security incident. In the areas of finance and accounting, studies have, however, observed abnormal trading volume as a result of various events. Abnormal trading volume, for example, was detected around capital gains tax rate reduction announcements (Bali & Francis, 2010), around earning announcements (Bamber et al., 2010; Hope et al., 2009), and approximately close to national elections (Bialkowski et al., 2008).

The present research also sheds light in establishing that there are differences between how the market reacts differently to security and privacy breaches. As previously mentioned, the comparison takes into consideration three different aspects: abnormal returns, risk shifts, and abnormal trading volume. These are discussed next.

Hypothesis 4 posits that security breaches will result in significantly higher abnormal returns compared to privacy breaches. This hypothesis is supported in the present research. The results allows me to go one step further and say that cumulative abnormal returns for the security group are also significantly higher than the privacy group. This means the present research is able to agree with Garg et al. (2003a, 2003b, 2003c) when they stated that security breaches have the highest negative impact. The present research is the first of its kind in comparing the impact of security and privacy breaches on abnormal returns.

The second hypothesis comparing the two previously defined, security and privacy breaches is related to risk shifts (H5). These risk shifts occur for both, privacy and security breaches. Security breaches, as previously discussed, resulted in a significant increase in risk whereas privacy breaches caused a decrease in risk. This supports H5, indicating that security breaches result in significantly higher firm risk than privacy breaches. This means that the market differentiates between the two types of breaches. No previous study has observed and explained this market behavior.

The last hypothesis that compares privacy and security breaches is H6. This hypothesis posits that security breaches will result in significantly higher abnormal trading volume. This hypothesis is not supported. Both, security and privacy breaches resulted in abnormal trading volume. There is no significant difference, however, in how the market reacted between the two groups. Therefore, H6 is not supported. Since the present research is the first of its kind, I am unable to compare it with other research studies.

6.2. Recommendations for Future Research

An opportunity for future research, as previously mentioned, is to collect a bigger sample and retest the hypotheses. Another possible venue for future research lies in dividing the sample into time periods. These time periods could be dictated by important events that may have contributed on how investors react to security and privacy breaches. These events may be, for example, the 9/11 tragedy, the dot-com bubble, among others. An additional venue for future research is to investigate the impact of firm characteristics on abnormal trading volume. Some of these characteristics, for example, could be firm size, industry, and traditional versus net-firms, among others. The firm characteristics may play a role in diminishing or enhancing the effect of security and privacy breaches on the stock market behavior.

The present dissertation research will be divided in three different articles for publication. The first essay is an empirical analysis of privacy breaches. The economic impact of privacy breaches essay will be submitted to an information systems conference and to an academic journal for publication. The second essay consists of an empirical analysis of security breaches. A portion of this second essay has been already presented and published in the proceedings of the 2012 Americas Conference on Information Systems. This second essay will be improved and submitted to an academic journal for publication. The third essay is a comparative analysis of security and privacy breaches. Similarly to the aforementioned two essays, this essay will also be submitted to an information systems conference and to an academic journal for publication.

6.3. Conclusion

In this Section, the concluding remarks of the present research are put forward. Firstly, the conclusions related to the first three hypotheses are put forward. The first three hypotheses analyzed the privacy and security breaches as separate groups. Secondly, the conclusions for hypotheses 4 to 6 are put forward. These last set of hypotheses established the differences between privacy and security breaches. Thirdly, an explanation of how the present research advanced the areas of information security and privacy is presented. Lastly, some of the limitations of the present research are explained.

Taken together, abnormal returns and risk shifts, investors did not penalize firms for suffering a privacy breach. The fact that privacy breaches resulted in abnormal trading volume is not indicative of a negative market reaction. Abnormal trading volume has to be taken into consideration in combination with abnormal returns, which in this case are not significantly negative. Firms that suffered a publicly announced security breach, on the other hand, were penalized by investors. The fact that security breaches resulted in abnormal trading volume and negative abnormal returns, is an indication that the market penalize firms suffering such breaches. The observed increase in risk, also, supports the hypotheses that investors perceived firms that suffer a security breach to be more risky. Again, it is believed that the present research results are the first in establishing this effect on abnormal returns, risk shifts, and abnormal trading volume in the information privacy and security area.

The present research goes one step further and conducts a comparative study between security and privacy breaches in these three measures. Taken together, the tests indicate that security breaches appear to have a greater impact on a firm's stock price, riskiness of the firm, as well as its trading volume. Negative abnormal returns were significantly higher for those firms suffering a security breach. This result is indicative that indeed, security breaches are more severe than privacy breaches in terms of abnormal returns. In particular, an important finding of the present research is that the riskiness of the firm (as measured by its beta) is significantly higher for firms that suffered a security breach than those that suffered a privacy breach. Around the event announcement, however, there is no indication that abnormal trading volume is higher for security breaches than privacy breaches. This is an indication that the market does not react differently to security and privacy breaches, in terms of the volume selling and

buying stocks. Taken the results separately, however, the market does react differently for security and privacy breaches.

The present research advances the area of information systems privacy and security. These advances are in the context of sample size and statistical methods used to test the proposed hypotheses. Similar studies in the area of information systems security and privacy used an average sample size of around 85 events. The present research consisted of a sample of 114 events. In the context of statistical methods, the present research calculated abnormal returns using two alternative models, the market model and the Fama-French's model. The use of two models to calculate abnormal returns increased the robustness of the results. The present research, also, used an estimation window of 250 trading days to calculate abnormal returns. Previous research studies were inconsistent with the use of estimation windows, however, most of the studies relied in a estimation window of 120 days. A longer estimation window provides a more accurate calculation of expected returns.

The present research also has some limitations. The sample size, although it is higher than the average used in prior studies, is still small compared to studies conducted in the areas of finance and accounting. The sample size, therefore, is still a limitation of the present research. A second limitation of the present research is that only public companies are analyzed. Public companies are used because the data used is only available for public companies. Again, this is a limitation for all event studies. Another limitation of any event study is that privacy and security breaches must be publicly announced. In this capacity, it is well known that firms are not always as forthcoming in announcing security and privacy breaches. This is in part attributed to the fact that the Security and Exchange Commission does not require firms to disclose these breaches. Firms that suffered a security or privacy breach, also, may not disclose the breaches in order to preserve their reputation. It is very likely, therefore, that there are undisclosed privacy and security breaches that were not included in the sample used for the present research.

The present seminal research, in summary, contributes to the information privacy and security breach areas in a number of ways: first, it clearly distinguishes between the security and privacy breaches following the guidelines suggested in the literature, establishing clearly defined privacy and

security groups. Second, the results show that, on average, publicly traded companies experiencing a security breach had significantly higher negative cumulative abnormal returns than those companies that suffered a privacy breach incidents. Third, the results show that the firms in the security breach group experienced a significant increase in risk during the year after the breach. This risk is also significantly higher for the security breach. The present research is the first in conducting abnormal trading volume and abnormal risk analyses in the information privacy and security area. By completing the aforementioned, the present research moved forward the literature in the areas of information security and privacy breaches.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? an Event Study. *The 27th International Conference on Information Systems*. Milwaukee, WI.

Amihud, Y., DeLong, G. L., & Saunders, A. (2002). The Effects of Cross-Border Bank Mergers on Bank Risk and Value. *Journal of International Money and Finance*, *21*(6), 857–877. doi:10.1016/S0261-5606(02)00026-8

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

Andoh-Baidoo, F. K., & Osei-Bryson, K.-M. (2007). Exploring the Characteristics of Internet Security Breaches That Impact the Market Value of Breached Firms. *Expert Systems with Applications*, *32*(3), 703–725.

Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., Ostertag, D., et al. (2010). *2010 Data Breach Investigations Report*.

Bali, R., & Francis, J. (2010). Trading Volume Around Ex-Dividend Days. *Applied Economics Letters*, 1–4.

Ball, R., & Brown, P. (1968). An Empirical Evaluation of Accounting Income Numbers. *Journal of Accounting Research*, *6*(2), 159–178.

Ball, R., & Kothari, S. P. (1991). Security Returns Around Earnings Announcements. *The Accounting Review*, *66*(4), 718–738.

Bamber, L. S., Barron, O. E., & Stevens, D. E. (2010). Trading Volume Around Earnings Announcements and Other Financial Reports: Theory, Research Design, Empirical Evidence, and Directions for Future Research*. *Contemporary Accounting Research*.

Barberis, N., Shleifer, A., & Wurgler, J. (2005). Comovement. *Journal of Financial Economics*, *75*(2), 283–317.

Beaver, W. H. (1968). The Information Content of Annual Earnings Announcements. *Journal of Accounting Research*, *6*, 67–92.

Beneish, M. D., & Whaley, R. E. (1996). An Anatomy of the "S&P Game": The Effects of Changing the Rules. *The Journal of Finance*, *51*(5), 1909–1930.

Benninga, S. (2008). *Financial Modeling* (3rd ed.). Cambridge, MA: MIT Press.

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of Information Technology Failures on the Market Value of Firms. *The Journal of Strategic Information Systems*, *18*(2), 66–79.

Bialkowski, J., Gottschalk, K., & Wisniewski, T. P. (2008). Stock Market Volatility Around National Elections. *Journal of Banking & Finance*, *32*(9), 1941–1953.

Biktimirov, E. N., Cowan, A. R., & Jordan, B. D. (2004). Do Demand Curves for Small Stocks Slope Down? *Journal of Financial Research*, *27*(2), 161–178.

Bolster, P., Pantalone, C. H., & Trahan, E. A. (2010). Security Breaches and Firm Value. *Journal of Business Valuation and Economic Loss Analysis*, *5*(1), 1.

Bose, I., & Leung, A. (2008). Assessment of Phishing Announcements on Market Value of Firms. *Information Technology, 2008. ICIT '08. International Conference on* (pp. 304–307). Presented at the Information Technology, 2008. ICIT '08. International Conference on.

Brennan, M. J., & Copeland, T. E. (1988). Beta Changes Around Stock Splits: A Note. *The Journal of Finance*, *43*(4), 1009–1013.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, *11*(3), 431–448.

Cardenas, J., Coronado, A. S., Nicholas-Donald, A., Parra, F., & Mahmood, M. A. (2012). The

Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation. *Eighteenth Americas Conference on Information Systems*. Presented at the Americas Conference on Information Systems, Seattle, Washington.

Carhart, M. M. (1997). On Persistence in Mutual Fund Performance. *The Journal of Finance*, *52*(1), 57–82. doi:10.2307/2329556

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. *Congressional Research Service Documents, CRS RL32331 (Washington DC)*.

Cavusoglu, H., Mishra, B., & 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*, *9*(1), 69–104.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior. *Decision Support Systems*, *50*(4), 651–661. doi:10.1016/j.dss.2010.08.017

Chen, X., Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the Severity of Phishing Attacks: A Hybrid Data Mining Approach. *Decision Support Systems*, *50*(4), 662–672. doi:10.1016/j.dss.2010.08.020

Ettredge, M. L., & Richardson, V. J. (2003). Information Transfer Among Internet Firms: The Case of Hacker Attacks. *Journal of Information Systems*, *17*(2), 71–82.

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, *25*(2), 383–417.

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustment of Stock Prices to New Information. *International Economic Review*, *10*(1), 1–21.

Fama, E. F., & French, K. R. (1993). Common Risk Factors in the Returns on Stocks and Bonds. *Journal of Financial Economics*, *33*(1), 3–56.

Fama, E. F., & French, K. R. (1996). Multifactor Explanations of Asset Pricing Anomalies. *The Journal of Finance*, *51*(1), 55–84.

Fama, E. F., & French, K. R. (2004). The Capital Asset Pricing Model: Theory and Evidence. *The Journal of Economic Perspectives*, *18*(3), 25–46.

Farahmand, F., Navathe, S., Sharp, G., & Enslow, P. (2004). Evaluating Damages Caused by Information Systems Security Incidents.

Frazzini, A., & Lamont, O. A. (2007). The Earnings Announcement Premium and Trading Volume. *SSRN eLibrary*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=986940

Garfinkel, J. A., & Sokobin, J. (2006). Volume, Opinion Divergence, and Returns: A Study of Post–Earnings Announcement Drift. *Journal of Accounting Research*, *44*(1), 85–112. doi:10.1111/j.1475-679X.2006.00193.x

Garg, A., Curtis, J., & Halper, H. (2003a). Quantifying the Financial Impact of IT Security Breaches. *Information Management and Computer Security*, *11*(2/3), 74–83.

Garg, A., Curtis, J., & Halper, H. (2003b). The Real Cost of Being Hacked. *Journal of Corporate Accounting & Finance*, *14*(5), 49–52. doi:10.1002/jcaf.10183

Garg, A., Curtis, J., & Halper, H. (2003c). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Security Journal: A Global Perspective*, *12*(1), 22–33.

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

Gillet, R., Hübner, G., & Plunus, S. (2010). Operational Risk and Reputation in the Financial Industry. *Journal of Banking & Finance*, *34*(1), 224–235.

Goel, S., & Shawky, H. A. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, *46*(7), 404–410.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The Impact of Information Security Breaches: Has There

Been a Downward Shift in Costs? *Journal of Computer Security*, *19*(1), 33–56.
Hope, O.-K., Thomas, W. B., & Winterbotham, G. (2009). Geographic Earnings Disclosure and Trading Volume. *Journal of Accounting and Public Policy*, *28*(3), 167–188.
Hovav, A., Andoh-Baidoo, F. K., & Dhillion, G. (2007). Classification of Security Breaches and Their Impact on the Market Value of Firms. *Proceedings of the Sixth Annual Security Conference, Las Vegas* (pp. 1–11).
Hovav, A., & Binder, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97–121.
Hovav, A., & D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Security Journal: A Global Perspective*, *13*(3), 32.
Hovav, A., & D'Arcy, J. (2005). Capital Market Reaction to Defective IT Products: The Case of Computer Viruses. *Computers & Security*, *24*(5), 409–424.
Howe, J. S., & Madura, J. (1990). The Impact of International Listings on Risk: Implications for Capital Market Integration. *Journal of Banking & Finance*, *14*(6), 1133–1142. doi:10.1016/0378-4266(90)90004-L
Ishiguro, M., Tanaka, H., Matsuura, K., & Murase, I. (2006). The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market. *International Workshop on the Economics of Securing the Information Infrastructure (WESII)*.
Joseph, K., Babajide Wintoki, M., & Zhang, Z. (2011). Forecasting Abnormal Stock Returns and Trading Volume Using Investor Sentiment: Evidence from Online Search. *International Journal of Forecasting*.
Kannan, K., Rees, J., & Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91.
Karafiath, I. (2009). Detecting Cumulative Abnormal Volume: A Comparison of Event Study Methods. *Applied Economics Letters*, *16*(8), 797–802.
Khansa, L., & Liginlal, D. (2011). Predicting Stock Market Returns from Malicious Attacks: A Comparative Analysis of Vector Autoregression and Time-Delayed Neural Networks. *Decision Support Systems*, *51*(4), 745–759. doi:10.1016/j.dss.2011.01.010
Kleidt, B., & Schiereck, D. (2009). Systematic Risk Changes Around Convertible Debt Offerings: A Note on Recent Evidence. *Global Finance Journal*, *20*(1), 98–105.
Ko, M., & Dorantes, C. (2006). The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation. *Journal of Information Technology Management*, *17*(2), 13–22.
Kothari, S. P. (2001). Capital Markets Research in Accounting. *Journal of Accounting and Economics*, *31*(1-3), 105–231.
Krishnamurthy, B., & Wills, C. E. (2010). On the Leakage of Personally Identifiable Information Via Online Social Networks. *ACM SIGCOMM Computer Communication Review*, *40*(1), 112–117.
Lintner, J. (1965). The Valuation of Risk Assets and the Selection of Risky Investments in Stock Portfolios and Capital Budgets. *The Review of Economics and Statistics*, *47*(1), 13–37.
MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, *35*(1), 13–39.
Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, *14*(1), 44 –59. doi:10.1177/1094670510383409
Markowitz, H. M. (1959). *Portfolio Selection: Efficient Diversification of Investments, Cowles Foundation Monograph# 16*. Yale University Press, New Haven.
Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market Price Effects of Data Security Breaches.

Information Security Journal: A Global Perspective, *20*(6), 263–273. doi:10.1080/19393555.2011.611860

Nicholas-Donald, A., Matus, J. F., Ryu, S., & Mahmood, A. M. (2011). The Economic Effect of Privacy Breach Announcements on Stocks: A Comprehensive Empirical Investigation. Presented at the Americas Conference on Information Systems, Detroit, Michigan. Retrieved from http://aisel.aisnet.org/amcis2011_submissions/341

NIST. (2004, February). FIPS Pub 199.

Patton, A. J., & Verardo, M. (2009, March 17). *Does Beta Move with News?: Systematic Risk and Firm-Specific Information Flows*. Monograph. Retrieved from http://eprints.lse.ac.uk/24421/

Richardson, R. (2009). *CSI Computer Crime and Security Survey*. Computer Security Institute (CSI).

Sharpe, W. F. (1964). Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk. *The Journal of Finance*, *19*(3), 425–442.

Singhal, A., Winograd, T., & Scarfone, K. (2007). Recommended Security Controls for Federal Information Systems. *NIST Special Publication*, *800*, 53.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276.

Telang, R., & Wattal, S. (2007). An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. *Software Engineering, IEEE Transactions on*, *33*(8), 544–557.

von Solms, B. (2001). Corporate Governance and Information Security. *Computers & Security*, *20*(3), 215–218.

Yadav, P. K. (1992). Event Studies Based on Volatility of Returns and Trading Volume: A Review. *The British Accounting Review*, *24*(2), 157–184.

Yun, J., & Kim, T. S. (2010). The Effect of Changes in Index Constitution: Evidence from the Korean Stock Market. *International Review of Financial Analysis*, *19*(4), 258–269.

Zafar, H., Ko, M., & Osei-Bryson, K.-M. (2012). Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors. *Information Resources Management Journal*, *25*(1), 21–37. doi:10.4018/irmj.2012010102

Vita

Adolfo S. Coronado earned his Bachelor of Business Administration in Information Systems and Finance at the University of Texas at El Paso. He received his Master of Information Technology in 2007 from the University of Texas at El Paso. In 2008 he joined the doctoral program in International Business with a research concentration in Information Systems.

Dr. Coronado was a recipient of the 2012 Graduate School's Dodson Dissertation Fellowship from the University of Texas at El Paso. He is also a member of Beta Gamma Sigma, an international honor society recognizing business excellence.

While pursuing his degree, Dr. Coronado worked as an Instructor for the department of Information and Decision Sciences. In this capacity, he taught courses in fundamentals of business statistics, quantitative methods in business, introduction to information security theory and practice, business systems analysis and design, and programming with visual basic. In 2009 he was invited as a visiting research scholar in the Information Systems Security Research Center at the University of Oulu Finland.

Dr. Coronado presented his research at international conference meetings, including the 2009 and 2012 Americas Conference on Information Systems and the 2012 Decision Sciences Institute Conference.

Dr. Coronado's dissertation entitled "Market Reactions to Publicly Announced Security and Privacy Breaches Suffered by Companies Listed on the United States Stock Exchanges: A Comparative Analysis" was supervised by Dr. M. Adam Mahmood. Dr. Coronado will continue his career in Academia in the area of Information Systems.

Permanent address: 500 West University Avenue, PMB 564
El Paso, TX 79968

This dissertation was typed by Adolfo S. Coronado.