THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

WP # 0015IS-299-2012

Date April 9, 2012

Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors

Humayun Zafar, Ph.D.* (Corresponding author)
Department of Information Systems
Kennesaw State University
1000 Chastain Road. MD 1101
Kennesaw, GA 30144
hzafar@kennesaw.edu

Myung S. Ko, Ph.D.
Department of Information Systems and Technology Management
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249
myung.ko@utsa.edu

3. Kweku-Muata Osei-Bryson, Ph.D.
Department of Information Systems
Virginia Commonwealth University
kmosei@vcu.edu

Title

Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors

Authors

1. Humayun Zafar, Ph.D.* (Corresponding author)
Assistant Professor of Information Security and Assurance
Department of Information Systems
Kennesaw State University
1000 Chastain Road. MD 1101
Kennesaw, GA 30144
hzafar@kennesaw.edu
(770) 420-4424 (voice)
(770) 423-6731 (fax)

2. Myung S. Ko, Ph.D.
Associate Professor of Information Systems
Department of Information Systems and Technology Management
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249
myung.ko@utsa.edu

3. Kweku-Muata Osei-Bryson, Ph.D.
Professor of Information Systems
Department of Information Systems
Virginia Commonwealth University
kmosei@vcu.edu

Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors

ABSTRACT

Information security breaches pose a growing threat to organizations and individuals, particularly those that are heavily involved in e-business/e-commerce. An information security breach can have wide-ranging impacts, including influencing the behaviors of competitors and vice versa within the context of a competitive marketplace. Therefore, there is a need for further exploration of implications of information security breaches beyond the focus of the breached firm. This study investigates the financial impact of publicly announced information security breaches on breached firms and their non-breached competitors. While controlling for size and the industry the firm operates in, we focus on specific types of information security breaches (Denial of Service, Website Defacement, Data Theft, and Data Corruption). Unlike previous studies that have used event study methodology, we investigate information transfer effects that result from information security breaches using the matched sampling method. Our study reveals statistically significant evidence of the presence of intra-industry information transfer for some types of security breaches. We also found evidence of contagion effects, but no similar evidence concerning competition effect.

KEYWORDS: *information security breach, information transfer, contagion effect, competition effect, organizational impact, financial impact.*

JEL Classification: General (L20)

INTRODUCTION

Over the past decade, more and more organizations and individuals have been using the Internet to conduct business transactions. While this e-business/e-commerce trend has provided important benefits to both organizations and individuals, it has also offered increased opportunities for hackers to breach information systems. So it is not surprising that information security breach incidents have also risen sharply (Bagchi & Udo, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Claburn, 2009; Gatzlaff & McCullough, 2010; Hovav & D'Arcy, 2004; Khansa & Liginlal, 2011) For example, when malware compromised IT systems at Heartland Payment Systems in 2008, over 94 million credit card accounts were compromised (Claburn, 2009). It is estimated that about 85 percent of all U.S. companies have experienced one or more information security breaches (Riddell, 2011). Costs associated with information security breaches have also increased. The Ponemon Institute in its annual study in 2010 reported that the average cost of a data breach for a firm was $7.2 million, an increase of seven percent from the year before (Ponemon, 2010). The report also stated that lost business represented 63 percent of the total cost in the U.S. A study by McAfee also estimated that global economic losses due to information security breaches in 2008 amounted to over $1trillion (Mills, 2009).

Given the potentially significant impact that an information security breach may have on individuals and organizations, several researchers have previously investigated implications of this phenomenon on organizational performance (Acquisti, Friedman, & Telang, 2006; Bass, 2000; Cavusoglu, et al., 2004; Kim, Lacina, & Park, 2008; Straub & Nance, 1990; Whitworth & Zaic, 2003). For the most part, these studies have focused on the short-term impact of publically announced security breaches on the stock market value of the breached firm (Campbell, Gordon, Loeb, & Zhou, 2003; Ettredge & Richardson, 2003). Some studies have also focused on the

medium term impact on the breached firm via accounting performance measures (Ko & Dorantes, 2006; Ko, Osei-Bryson, & Dorantes, 2009).

Events such as information security breaches in firms have a wide-ranging impact. For example, they can influence the behavior of competitors and vice versa within the context of a competitive marketplace. Therefore, there is a need for further exploration of implications of information security breaches beyond the focus of the breached firm. As observed by previous researchers (e.g. Kim et al., 2008; Aharony & Swary, 1983; Foster, 1981), information transfer exists between a firm making a public announcement regarding an event, and industry counterparts that are its close competitors. The subject of information transfer effect has been investigated at length in various fields including accounting, economics, and finance (Clinch & Sinclair, 1987; Kim, et al., 2008; Szewczyk, 1992), but has been relatively unexplored in information systems (IS) research. Also, past research on the effects of information transfer has shown disparate results (Coroama & Röthenbacher, 2003; Helal et al., 2003), thus suggesting the need for further research on this topic, particularly in regard to IS security.

In this study, we explore the intra-industry information transfer effects of publicly announced information security breaches. An intra-industry information transfer exists when information released by one firm affects the performance of other non-announcing firms in the same industry. For example, in September 2008, when Lehman Brothers announced its bankruptcy, the share prices of Morgan Stanley, Goldman Sachs, and Citigroup also dropped 13.5%, 12.1%, and 15.1% respectively (Shen, 2008). Such information transfer can occur in two ways: *contagion* and *competition* effects (Floerkemeier & Siegemund, 2003; Szewczyk, 1992). A *Contagion Effect* occurs when a non-announcing firm's financial performance reaction is in the same direction as that of the announcing firm. It also usually arises from industry commonalities.

A *Competition Effect* occurs because of shifts in the industry's competitive balance and tends to be in the opposite direction.

In the following section, we review previous studies on information security breaches and intra-industry information transfer effects. After that, we discuss this study's research hypotheses, research method including financial performance indicators, and data collection. Then we report results from our analysis and provide interpretation, implications, and limitations of our results. In the final section, we conclude our study with the inclusion of some suggestions for future studies.

LITERATURE REVIEW

Previous research has noted the importance of information security in organizations (Baskerville, 1993; Dhillon & Backhouse, 2001; Hsu, 2009; Siponen, 2005). Since users interact with information systems on a regular basis in their business activities, how they use the systems, and whether they follow established policies will ultimately influence the overall security of a firm's information systems. Ponemon's 2010 annual survey revealed that security breaches led to a loss of existing customers due to diminished customer confidence and trust in organizations. While decreased productivity due to disruption of business operations and costs to repair or replace systems are short-term costs, revenue lost due to loss of existing or future customers, and decline of investor confidence due to a negative reputation of the organization are examples of long-term costs. These can have serious financial consequences on organizations (Campbell, et al., 2003; Cavusoglu, et al., 2004).

Information Security Breaches and Financial Impact on Organizations

Several previous studies that have investigated the financial impact on a breached firm employed event study methodology, which focuses on abnormal returns attributed to a security

breach event reflected in the market value of the firm (Acquisti, et al., 2006; Campbell, et al., 2003; Cavusoglu, et al., 2004; Hovav & D Arcy, 2004). Cavusoglu et al. (2004) found that breached firms lost on average 2.1 percent of their market value within two days of the announcement. Acquisti et al. (2006) investigated information privacy breaches, and concluded that there was a statistically significant negative impact on a firm's market value on the day of the information security breach announcement although it decreased over the days following the incident announcement. In contrast, other studies have shown that there was no statistically significant financial impact from an information security breach. Hovav and D'Arcy (2004) investigated the impact of virus attack announcement on market reaction. They concluded that there was no statistically significant impact on the firm's market value over the 25 days following the announcement. Although Campbell et al. (2003) found a significant negative market reaction regarding security breaches that are associated with unauthorized access to confidential data, the authors did not find much of a reaction with other types of security breaches.

Unlike studies that employed event study methodology, Ko et al. (2009) used matched-sampling methodology to explore this issue. They matched firms by size and their operating industry. In addition, they categorized data into types of security breaches based on the Confidentiality, Integrity, and Availability (CIA) principle. The authors concluded that the direction of the impact was dependent on the type of security breach, and the impact of IT intensive firms was different from non-IT intensive firms. In another study that used the matched-sampling methodology, Ko and Dorantes (2006) investigated the impact on financial performance of breached firms that have experienced security breaches with confidential data.

Using the subsequent four quarters after the security breach, the authors concluded that non-breached firms outperformed breached firms.

Intra-Industry Information Transfer Effects

An intra-industry information transfer can occur if information released by a firm has important implications for the future profitability of other non-announcing firms that operate in the same industry. Evidence about these information transfers improves our understanding of the sophistication and economics of markets related to information security incidents. This phenomenon has been researched for many different types of news releases including management forecasts, mergers, sales announcements, industrial accidents, and regulatory actions (Bardram, 2003; Otchere, 2005). For example, the bankruptcy of a bank, especially a large one, may lead to the loss of public confidence in the banking system as a whole, and thus likely setting off runs on other banks (Aharony & Swary, 1983). Most of the previous studies that have investigated the effect of information transfer have used event study methodology, and are in the areas of accounting, finance, and economics (Clinch & Sinclair, 1987; Foster, 1981; Kim, et al., 2008; Szewczyk, 1992). However, these studies have shown mixed results.

Foster (1981) investigated the impact of a firm's earning releases on stock prices. The results showed that for an identifiable sub-set of firms, earning releases of a firm have a statistically significant contagion effect on the stock price of other firms. Clinch and Sinclair (1987) tested the three hypotheses outlined by Foster (1981) by studying the extent of intra-industry information transfers associated with the half-yearly earnings announcements of a sub-set of Australian firms. Their study supported the existence of a contagion effect associated with a firm's earnings releases. In another study, Kim et al. (2008) also found presence of a contagion effect when earnings forecasts were released. The authors concluded that when firms forecasted

good news, it positively influenced other firms. Conversely, negative information transfers were present between forecasting and non-forecasting competitor firms when preceded by negative news. Szewczyk (1992) studied whether initial announcements of corporate security offerings affected share prices in the capital markets and found the presence of 'negative abnormal returns' (actual returns are less than expected returns) in the shares of both announcing and non-announcing firms. This suggests that investors draw inferences about the prospects of the industry as a whole rather than narrowly viewing the given security breach event as a shift in competitive advantage between the announcing firm and its industry competitors.

In one of the few IS research studies that addressed the information transfer phenomenon, Ettredge and Richardson (2003) used event study methodology to focus on Internet firms that were subject to *Denial of Service* (DoS) attacks. The authors assumed that if a firm in the same industry announced lower-than-expected earnings, then the firm was more likely to experience negative abnormal returns. They found that there were negative mean abnormal returns among Internet firms not attacked (*contagion* effect of information transfer).

Information Security Breaches and Intra-Industry Information Transfer Effects

Our review of the research literature suggests that the issue of information transfer effects that result from information security breaches needs exploration in IS. Furthermore, the previous study that addressed this issue focused only on Denial of Service (DoS) attacks, and so possible information transfer effects from other types of security breaches (i.e. *Website Defacement, Data Theft, and Data Corruption*) were previously unexplored. Given the increase in the frequency of security breach incidents and the possibility that information transfer effects that result from such breaches could have significant financial impacts on organizations, studying this issue is important. The lack of evidence-based analysis of this phenomenon provides motivation and

justification for this study, which explores the information transfer effects that result from each type of security breach (e.g. *Denial of Service, Website Defacement, Data Theft, and Data Corruption*). It should be noted that unlike previous studies that have used event study methodology, we investigate information transfer effects in the case of information security breaches using the matched sampling method.

RESEARCH HYPOTHESES

We formulate two sets of hypotheses, the *Naive View Hypotheses* and the *Sophisticated View Hypotheses*. The two views aim to provide a complete picture of an organization's assessment of a security breach, because they not only consider initial reactions to announcement of security breaches but also consider magnitude of the "ripple effects." The next two sub-sections provide a more detailed description. The expression of these hypotheses involve a four category classification of security breach incidents that was obtained by collapsing an overarching set defined by Richardson (2008). For example, Richardson provided a granular representation of information security breaches that involve the theft of data: theft of data from mobile devices (such as cellular phones), theft from wireless networks, and theft from laptops, etc. We combined these breaches into a more general *Data Theft* category. Richardson's target is an audience who wants to ascertain the overall information security environment, and how to counter different types of security breaches. In this study, we intend to gauge the financial impact of information security breaches on the breached firms and their competitors. Our final list includes four categories: *Denial of Service (DoS)*, *Website Defacement*, *Data Theft*, and *Data Corruption*. *Denial of Service* attacks aim to make a resource unavailable for users. *Website Defacement* involves alteration to the visual appearance of a website. *Data Theft* includes

unauthorized access to information, whereas *Data Corruption* is an intentional change to data integrity

Naive View Hypotheses

The naïve view involves a relatively simplistic view of an information security breach, regarding it simply as bad news for the breached firm. This is particularly true with regard to a breached firm's competitors. Kim et al. (2008) hypothesized that when firms announced bad news, information transfers to competitor firms were negative. Based on this perspective, the announcement of the security breach (bad news) of the firm should lead to negative intra-industry information transfer (competition) effect to its competitors since a competitive relationship exists between the breached and its non-announcing competitor firms. This would suggest the following hypotheses:

H_{1N}: The information transfer from a firm's *Denial of Service (DoS)* security breach incident has a *Competition Effect* on competitor firms.

H_{2N}: The information transfer from a firm's *Website Defacement* security breach incident has a *Competition Effect* on competitor firms.

H_{3N}: The information transfer from a firm's *Data Theft* security breach incident has a *Competition Effect* on competitor firms.

H_{4N}: The information transfer from a firm's *Data Corruption* security breach incident has a *Competition Effect* on competitor firms.

Sophisticated View Hypotheses

The sophisticated view involves a view of an information security breach, where both the breached firm and its competitors regard the breach as a wake-up call to action against a common enemy (i.e. the attacker). This suggests that even though a competitive relationship

exists between the breached and its non-announcing competitor firms, the information transfer resulting from the public announcement of an information security breach may not have a *Competition* effect.

Consider this, once a security breach occurs, the breached firm becomes even more aware of its vulnerability and of the importance of adequately addressing the issue in a cost effective manner. This may involve the breached firm improving its business practices in a manner that results in greater efficiency and thus greater relative profitability. The bottom line is that information security breaches, particularly severe ones such as *Data Theft*, may serve as an alert, a wake-up call to the breached firm that leads to greater efficiency. It is also reasonable to expect that the competitor firms would view the security breach on one of their competitors as a catalyst leading to greater efficiency. Thus, both the breached firm and its competitors would take actions that would result in increased efficiency and profitability due to the breach event. However, why should the competitor firm not outperform the breached firm? There could be several potential reasons. Firstly, a breached firm could have a head start in improving relevant business practices and infrastructure, including taking long and short-term corrective measures. This is because the firm would be aware of its vulnerability before its competitors become aware after public announcement of the breach. Secondly, given the sensitivity of investors and other stakeholders to information security breaches, the breached firm has greater motivation to address this matter that provides comfort to these stakeholders.

This more sophisticated view of information security breaches suggests the following hypotheses:

H_{1S}: The information transfer from a firm's *Denial of Service (DoS)* security breach incident has an *Upward Contagion Effect* on its competitor firms.

H_{2S}: The information transfer from a firm's *Website Defacement* security breach incident has an *Upward Contagion Effect* on its competitor firms.

H_{3S}: The information transfer from a firm's *Data Theft* security breach incident has an *Upward Contagion Effect* on its competitor firms.

H_{4S}: The information transfer from a firm's *Data Corruption* security breach incident has an *Upward Contagion Effect* on its competitors firms.

RESEARCH METHOD, MEASURES & DATA COLLECTION

Research Method

We used matched-sampling methodology, which previous studies (Bharadwaj, 2000; Hunton, Lippincott, & Reck, 2003; Ko, et al., 2009) have employed to select competitor firms for each breached firm. We measured the difference in firm performance between breached firms and non-breached competitor firms, while controlling for size and industry.

Firm Financial Performance Indicators

To investigate the financial impact of information security breaches, we employed financial ratio analysis, which is a useful method of measuring financial performance. Several previous studies also used this approach (Hitt & Brynjolfsson, 1996; Nicolaou, 2004). Altman (1968) used discriminant analysis to conclude that traditional ratio analysis is an important analytical technique in the academic environment.

In this study, we used two profit ratios (i.e. *Return on Assets*, *Return on Sales*), and two cost ratios (i.e. *Cost of Goods Sold to Sales*, *Selling and General Administration Expenses to Sales*) to measure the firm's financial performance. These measures have been used in previous studies (Bayus, Erickson, & Jacobson, 2003; Bharadwaj, 2000; Dehning, Richardson, & Zmud, 2007; Ko & Dorantes, 2006; Stanford, 2002). *Return on Assets* (ROA) provides a snapshot of

how efficient management is at using its assets to generate earnings; *Return on Sales* (ROS) evaluates a firm's operational efficiency; *Cost of Goods Sold to Sales* (COGS/S); and *Selling and General Administration Expenses to Sales* (SGA/S) measures the percentage of sales used to pay for total operating costs. We believe that the use of these four ratios provides a very holistic view of a firm's performance. Table 1 presents the ratios and their formulas.

Table 1: Firm Performance Ratio

Profit Ratios Formula	
ROA	Net Income / Total Assets
ROS	Net Income / Net Sales
Cost Ratios Formula	
COGS/S	Cost of Goods Sold / Net Sales
SGA/S	Selling and General Administration Expenses / Net Sales

Data Collection

Selecting Breached and Competitor Firms

We selected firms that had publicly announced information security breaches between 1997 and 2007 using the Lexis/Nexis Academic database. The keywords used to search the database were "attack", "breach", "break-in", "hacker", "Internet", "security", "virus", "computer", and "information." This approach is similar to methods used by previous studies (Andoh-Baidoo & Osei-Bryson, 2007; Cavusoglu, et al., 2004). Then using the breached firm's 4 digit SIC code, we extracted its competitors (control firms) using Hoover's Handbook of American Businesses (Biesada, 2008) and Mergent Online Database. Mergent offers financial data for each organization and its competitors through Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.

The initial data set included 158 breached firms. As we pulled each breached firm's competitors, we ended up with 4229 non-breached competitor firms in total. Then we selected

competitors whose financial information was available in Compustat or EDGAR. We also ensured that a competitor's size was comparable to that of the breached firm in order to remove any statistical bias in the results that would be caused by comparing firms of varying sizes. We used total assets as a surrogate measure for size and selected competitor firms whose total assets were within 70-130% of the breached firm's. This is an established and frequently used approach in finance and accounting (Barber & Lyon, 1996). As a result, the final data set included 119 breached firms and 867 non-breached competitors. There were several reasons for the drop in the number of firms. In certain cases, financial information was not available because an organization is a private firm or no longer existed. In other cases, either there were no corresponding competitors comparable in size, or there were no financial values for either breached or competitor firms.

Industry Performance

After collection of annual financial data for the year before and after the breach for each breached firm and its industry competitors, we considered industry average performance during the year of security breach. This accounted for any change in average industry performance in that year. The change in industry average performance (Δ*IndAvgPerformance*) is the difference between industry's pre-incident ($year_{t-1}$) performance and post incident ($year_{t+1}$) performance, where t is the year of the breach. Pre-incident periods have been given due importance in past studies. Kim et al. (2008) looked at cumulative abnormal returns (CAR) for a few days before and after the announcement. Barber and Lyon (1996) state that when sample firms experience pre-event performance that is different from control firms, test statistics are well specified when sample firms are matched to control firms with similar pre-event performance. The reader may note that we were already doing this based on our selection criteria (i.e. 70-130% of a breached

firm's TOA at year$_{t-1}$). Also according to Barber and Lyon (1996) industry benchmarks should be considered in conjunction with pre-incident performance statistics. In our study, the industry average plays a similar role. Industry matching assumes that some of the cross-section variation in operating performance is explained by an industry benchmark. Barber and Lyon (1996) consider it a drawback if in computing expected performance (without any pre-event performance measures) a benchmark does not take overall industry performance into account. Therefore, for each performance ratio, we calculated the change in each industry's average performance, shown as follows:

$$\Delta IndAvgPerformance = IndAvgPerformance_{t+1} - IndAvgPerformance_{t-1} \quad (1)$$

Since each breached firm had multiple competitors, for each set of competitors we computed the average performance. This resulted in each breached firm's performance ratio being compared to the average performance ratio representing all competitor firms in the same industry. Though it may be argued that annual returns of each competitor firm may vary in terms of profit and loss, we contend that overall the industry average will exhibit a consistent direction.

We then computed the difference between the actual and expected performance of each breached and competitor firms. The actual performance of a breached firm is its reported financial performance a year after the breach. The expected performance of a breached firm is calculated financial performance a year after the breach in the absence of a breach incident. It is computed by adding the financial performance of the breached firm a year before the breach to the change in the industry average performance from year t - 1 to year t + 1 Therefore for each performance ratio, we calculated expected performance as follows:

$$ExpectedPerformance_{t+1} = ActualPerformance_{t-1} + \Delta IndAvgPerformance \quad (2)$$

Hence, there is no change in performance if actual performance equals expected performance.

For each pair of breached and competitor firms, we computed this difference in financial performance as follows:

$$Difference_{B\ or\ C} = ActualPerformance_{t+1} - ExpectedPerformance_{t+1} \quad (3)$$

where "B" represented a breached firm, and "C" represented the non-breached competitors.

We then computed the difference in differences in the financial performances of breached and non-breached competitor firms as follows:

$$DifferenceInDifferences = Difference_B - Difference_C \quad (4)$$

Table 2 provides descriptive statistics of the total assets for the breached and competitor firms for the year before the breach. As shown in the Table 2, the breached firm and selected competitor firms are comparable to each other.

Table 2: Descriptive Statistics

Variable	Mean	Median	Min.	Max.
Breached Firms' Total assets ($million)	20,383.29	6,853.98	0.24	29,3673.12
Competitor Firms' Total assets ($million)	16,846.19	5,169.29	0.13	20,1571.92

To gauge the significance of the differences in financial performance between the breached and competitor firms, a paired-sample t test can be employed. However, this test assumes that data is normally distributed. Since we were not able to ascertain normality of data using Shapiro-Wilk's normality test, we used non-parametric Wilcoxon matched-paired (Z) test, which compares differences between two measurements without making assumptions about normality (Mynatt, Essa, & Rogers, 2000).

Table 3 presents the information transfer decision chart that was used for each of the profit and cost ratios. For example, if the breached firm's actual ROA at $year_{t+1}$ was less than its expected ROA at $year_{t+1}$, and if the competitor's actual ROA at $year_{t+1}$ was less than its expected ROA at $year_{t+1}$, then information transfer existed. These results point to a *Downward*

Contagion effect because both firms performed less than what was expected, and they were in the same direction. On the other hand, if the breached firm's actual ROA at $year_{t+1}$ was greater than its expected ROA at $year_{t+1}$, and if its competitor's actual ROA at $year_{t+1}$ was greater than its expected ROA at $year_{t+1}$ it showed presence of an *Upward Contagion* information transfer effect. However, if the breached firm's actual ROA at $year_{t+1}$ was less than its expected at $year_{t+1}$, and its competitor's actual ROA at $year_{t+1}$ was greater than its expected at $year_{t+1}$, it presented a *Competition* information transfer effect.

Table 3: Information Transfer Decision Chart

Performance at Year (t+1)		**Information Transfer Effect**
Breached Firm	**Competitor Firms**	
Profit Ratios		
Actual < Expected	Actual < Expected	Downward Contagion effect
Actual < Expected	Actual > Expected	Competition effect
Actual > Expected	Actual > Expected	Upward Contagion effect
Actual > Expected	Actual < Expected	No effect
Cost Ratios		
Actual > Expected	Actual > Expected	Downward Contagion effect
Actual > Expected	Actual < Expected	Competition effect
Actual < Expected	Actual < Expected	Upward Contagion effect
Actual < Expected	Actual > Expected	No effect

RESULTS

Tables 4 – 7 present the results from each security breach category. In each table, we include the Z value (which is calculated using the difference between the actual and the expected performance of a breached firm and its competitors' average performance), its significance, and the actual and expected mean for the both firms. To test each pair of hypotheses, naïve view and sophisticated view by each type of security breaches we performed two steps. First, we reviewed the significance of Z value of each financial ratio. If significant, we inspected whether

information transfer is a *Competition Effect*, an *Upward Contagion Effect, or No information transfer*, based on the chart in Table 3.

Table 4 presents the results for *Denial of Service (DoS)* security breaches. None of the financial ratios were significant as shown in Table 4. Thus, there was no information transfer.

Table 4: Results of Denial of Service (Testing Hypotheses 1N and 1S)

Ratio	Group	Actual	Expected	Z	Signif.	Hypothesis 1N	Hypothesis 1S
ROA	Breached	-0.12	-0.34	1.61	0.87	N	N
	Competitors	-0.16	-0.31				
ROS	Breached	-0.70	-6.80	1.53	0.13	N	N
	Competitors	-0.31	-0.89				
COGS/S	Breached	0.54	-0.53	-0.44	0.66	N	N
	Competitors	0.48	-0.49				
SGA/S	Breached	0.34	8.54	-1.55	0.12	N	N
	Competitors	0.32	2.76				

N: not supported

Table 5 presents results for *Website Defacement*. We noted that the relevant differences for the ROA and ROS ratios were statistically significant. In the case of ROA, actual means for both breached and competitor firms were higher than the expected means. This indicates presence of an *Upward Contagion* effect of information transfer. In the case of ROS, even though the actual mean of competitor firms was less than the expected mean for competitor firms, the breached firm's actual mean was higher than the expected mean. Given the information transfer decision rules described in Table 2 these results suggest that there was no information transfer effect.

Table 5: Results of Website Defacement (Testing Hypotheses 2N and 2S)

Ratio	Group	Actual	Expected	Z	Signif.	Hypothesis 2N	Hypothesis 2S
ROA	Breached	-0.01	-0.49	2.51	0.01	N	Y
	Competitors	-0.11	-0.46				
ROS	Breached	-0.46	-1.80	2.20	0.03	N	N
	Competitors	-18.15	-4.70				
COGS/S	Breached	1.12	1.92	-0.31	0.75	N	N
	Competitors	0.79	2.30				
SGA/S	Breached	0.28	1.13	-1.26	0.21	N	N
	Competitors	14.30	3.12				

N: not supported; **Y**: supported

Table 6 provides results for *Data Theft* related security breaches. Only SGA/S was significant. The actual means for SGA/S for both types of firms were less than the expected means. However, since these are cost ratios, this implies both types of firms actually performed better than the expected. This we note an *Upward Contagion* effect of information transfer in this case.

Table 6: Results of Data Theft (Testing Hypotheses 3N and 3S)

Ratio	Group	Actual	Expected	Z	Signif.	Hypothesis 3N	Hypothesis 3S
ROA	Breached	0.04	0.11	0.06	0.96	N	N
	Competitors	0.00	0.09				
ROS	Breached	0.19	0.63	0.53	0.59	N	N
	Competitors	-0.01	0.39				
COGS/S	Breached	0.84	0.91	-0.32	0.74	N	N
	Competitors	0.56	0.94				
SGA/S	Breached	0.34	1.59	-1.60	0.00	N	Y
	Competitors	0.29	0.50				

N: not supported; **Y**: supported

Table 7 presents results concerning *Data Corruption*. ROA was the only significant financial ratio and we note an *Upward Contagion* effect of information transfer. In this case, the actual means were higher than the expected means for both breached and competitor firms.

Table 7: Results of Data Corruption (Testing Hypotheses 4N and 4S)

Ratio	Group	Actual	Expected	Z	Signif.	Hypothesis 4N	Hypothesis 4S
ROA	Breached	-0.22	-0.32	1.72	0.09	N	Y
	Competitors	-0.06	-0.24				
ROS	Breached	-0.67	-1.61	0.90	0.37	N	N
	Competitors	-0.15	-0.49				
COGS/S	Breached	0.52	0.60	-0.41	0.68	N	N
	Competitors	0.56	0.64				
SGA/S	Breached	0.29	1.23	-0.78	0.44	N	N
	Competitors	0.26	0.76				

N: not supported; **Y**: supported

INTERPRETATION OF RESULTS, IMPLICATIONS, AND LIMITATIONS

Interpretation of Results

Table 8 shows the summary of results for each type of security breach. It is notable that while the results of our analysis do not support any of the *Naive View Hypotheses* (i.e. offer any evidence that information security may result in *Competition* effects), they do provide support for the *Sophisticated Hypotheses* (i.e. evidence that security breaches may result in *Contagion* effects) on some of the performance measures. The reader may raise a question as to why if there is evidence of a *Contagion* effect for a particular information security breach, corresponding evidence does not surface on all of the measures? This may be because different measures may have different levels of sensitivity to a given event. Furthermore, in some cases while a given measure might have provided evidence of a *Contagion* effect the evidence was just not statistically significant at the 10% significance level.

Table 8: Summary of Results: Supported Hypotheses

Ratio	Denial of Service		Website Defacement		Data Theft		Data Corruption	
	H_{1N}	H_{1S}	H_{2N}	H_{2S}	H_{3N}	H_{3S}	H_{4N}	H_{4S}
ROA				√**				√*
ROS								
COGS/S								
SGA/S						√**		

√*: Statistically Significant at 10% level; √**: Statistically Significant at 1%

Our results do provide some statistically significant evidence of *Contagion* effects but no statistically significant evidence of *Competition* effects. But if the public announcement of an information security breach is beneficial to both the breached firm and its competitors while not giving any relative benefit to the competitor, then what is the advantage that the breached firm has in making an announcement in the first place? Could it be advantageous for the breached firm not to make a public announcement, and in doing so not alert its competitors? Another type of '*competition* effect' may in fact occur in such a situation in which the breached firm outperforms its competitors because it takes action to improve relevant business practices and infrastructure while its competitors are in some sense 'asleep' with regard to the need to take appropriate action. However, we must emphasize that typically there are laws, rules, and guidelines that dictate reporting responsibilities after a security breach. Therefore, we are not implying that legitimate advantage can be gained by ignoring or breaking this type of law, guideline, or rule, even if it was possible.

Our study has some additional interesting findings. For example, out of four significant financial ratios, two of the profit ratios (*Website Defacement*: ROA; *Data Corruption*: ROA) and one cost ratio (*Data Theft*: SGA/S) indicated that actual performance of the breached firms was better than the expected after the breach. This is somewhat consistent with the study by Ko et al. (2009), which found that *Data Corruption* and *Website Defacement* breaches did not have long-

term negative impact on a firm performance. A possible reason for this could be that breached firms may invest heavily in their IT security infrastructure, thereby preventing future attacks and competitor firms would follow the breached firms in a similar manner. This investment would make both sets of firms more effective and efficient when it comes to information security protocols and overall business operations. This would result in an improvement in overall firm performance. Another reason that could be used from the previous precedence of bad news being followed by surprisingly positive financial results for organizations would be either the presence of strong leadership or trusting consumers who did not panic. A classic example of this is the Tylenol recall case in 1982 (Rehak, 2002). Johnson & Johnson recalled all Tylenols when seven people died after taking cyanide laced Tylenol tablets. The company immediately released information regarding the tainted tablets to the public, and against all odds was able to continue with positive long-term growth.

Implications for Research and Practice

Our study presents important implications for both academics and practitioners. We have extended research stream of IS security research that uses matched-sampling methodology along with empirical support and introduced intra-industry information transfer effect in IS security literature. By integrating a theory (intra-industry information transfer) from accounting and economics, we believe that our study have provided a more holistic way of gauging financial impacts of information security breaches on breached firms and their competitors. In addition, we were able to observe *Upward Contagion* effects of information transfer from firms announcing an information security breach. This suggests that an information security breach incident is also viewed as bad news to its competitors in the same industry and thus, both the

breached firm and its competitor firms strive to improve their overall company image and industry image as a whole.

For practitioners, we offer an in-depth way of investigating the financial impact of information security breaches that result from information transfer effects. Outlets such as CSI/FBI Computer Crime and Security Surveys present financial impact figures (CSI, 2009) that are based on surveying hundreds of computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities. Our approach provides another more direct method of computing financial impact of information security breaches using published financial data. It may be noted that this approach avoids the need to consider the response bias of subjects, an issue that is commonly associated with survey or questionnaire based research methods.

Limitations of the Study

There are some potential limitations of our study. First, we only considered publicly traded firms. This was necessary due to the inability to gather financial performance data of private firms. Second, it may also be argued that events other than information security breaches (e.g. change in executive management) may have been responsible for the change in performance. However, since we are considering the industry average to compute the expected performance, as a whole over a period of an entire year it is unlikely that other events have a similar effect on the entire industry. Third, for each breached firm we matched its financial performance against the average financial performance of its multiple competitor firms. Given the possibility that some of the breached firm's competitors may have experienced contagion effects while others experienced competition effects, then it is possible that these two types of effects could have canceled each other out in the calculation of the average performance of the

breached firm's competitors. We tried to counter this potential problem by using the entire industry's average performance in computing the expected performance.

CONCLUSION AND FUTURE RESEARCH

In this study, we investigated intra-industry information transfer effects on firms that suffered from an information security breach. This study contributes to IS literature in several ways. First, information transfer as shown in this study is an area that has been under-researched in IS in general, and in the IS security domain in particular. However, it has been explored extensively in areas such as finance and accounting. Second, this study provides additional insight on information security breaches beyond the financial impact of breached firms by extending them to their industry counterparts. Third, our study provides statistically significant evidence of the existence and magnitude of the effects by studying different types of security breaches. In this study, we categorized information security breaches into different categories (i.e. *Denial of Service*, *Website Defacement*, *Data Theft*, and *Data Corruption*). Our study suggests that a security breach announcement is not just an incident to the breached firm but it has a ripple effect to the industry as a whole. Therefore, this provides important implications to top managers. An announcement of an information security breach by the breached firm should not be disregarded by other firms in the same industry. Rather it should be taken as an alert to all firms in the same industry, obviously including the breached firm itself, to address relevant security issues so that they might not suffer damage from any similar security attacks in the future.

In addressing our research problem, we specified two sets of hypotheses: a *naïve view* set, and a *sophisticated view* set. We also explored each hypothesis with respect to four financial measures. This resulted in what may appear to be a large number of hypotheses. However, this

approach was based on deliberation. While we believed that the hypotheses in the *naïve view* set were not likely to be valid, we also suspected that different financial measures may have different levels of sensitivity to information transfer effects. Also, given the absence of previous studies that investigated the full *naïve view* set of hypotheses, we took the position that it was important to investigate not only the *naïve view* set of hypotheses empirically with respect to each performance measure, but also the *sophisticated view* set of hypotheses, which are worthy of consideration.

As stated earlier, exploration of information transfer effects that result from information security breaches is important to both practice and research. We believe, there are several important sub-topics that appear to be worthy of exploration in future research. First, in certain cases for our statistically significant results, we noted that actual performance of the breached firm was better than that of its competitors. That seems to imply that certain types of information security breaches may actually have beneficial long-term impacts on the breached firm's performance. This issue appears to require further focused exploration. Second, it may be useful to do an analysis based on quarterly financial performance data as the impact of some information security breaches may have a short-term effect on an organization's performance. Third, it may be also valuable to do a study that focuses on pure Internet (or click) firms that only have an Internet presence. Due to the nature of these firms, information security breaches suffered by them may result in more discernable evidence of information transfer effects. Fourth, results from previous research suggest that public declaration of a security breach will often adversely affect the value of an organization in the short term. It may also affect similar organizations in the market space. Therefore, researchers should also consider carrying out longitudinal studies to determine the true financial impacts of information security breaches on

organizations. Fifth, although this study focused on the presence of intra-industry information transfer effects, it is entirely probable that cross-industry impact of information security breach incidents may also exist. Therefore, it may be also useful to investigate the presence or absence of statistically significant inter-industry information transfers.

ACKNOWLEDGEMENT: This research was supported in part by a grant from Summer Research Grant Program of the School of Business of Virginia Commonwealth University and also was supported in part by a grant from the College of Business at UTSA. We would like to thank the anonymous reviewers and the associate editor for their valuable comments.

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). *Is there a cost to privacy breaches? An event study.* Paper presented at the Twenty-Seventh International Conference on Information Systems, Milwaukee, Wisconsin.

Aharony, J., & Swary, I. (1983). Contagion effects of bank failures: Evidence from capital markets. *Journal of Business, 56*(3), 305-322.

Altman, E. I. (1968). Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *Journal of Finance, 23*(4), 589-609.

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.

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. *Communications of the Association for Information Systems, 12*, 684-700.

Barber, B., & Lyon, J. (1996). Detecting abnormal operating performance: The empirical power and specification of test statistics. *Journal of Financial Economics, 41*(3), 359-399.

Bardram, J. E. (2003). *Hospitals of the future–ubiquitous computing support for medical work in hospitals.* Paper presented at the Second international workshop on ubiquitous computing.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375-414.

Bass, T. (2000). Intrusion detection systems and multisensor data fusion. *Communications of the ACM, 43*(4), 99-105.

Bayus, B. L., Erickson, G., & Jacobson, R. (2003). The financial rewards of new product introductions in the personal computer industry. *Management Science, 49*(2), 197-210.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly, 24*(1), 169-196.

Biesada, A. (2008). *Hoover's Handbook of American business*: Austin, TX: Hoover's Business Press.

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.

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), 70-104.

Claburn, T. (2009). Heartland Payment Systems Hit By Data Security Breach Retrieved April 2, 2009, from http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212901505

Clinch, G., & Sinclair, N. (1987). Intra-industry information releases: A recursive systems approach. *Journal of Accounting and Economics, 9*(1), 89-106.

Coroama, V., & Röthenbacher, F. (2003). *The Chatty Environment–providing everyday independence to the visually impaired.* Paper presented at the Ubihealth.

CSI. (2009). CSI. Computer Science Institute. Retrieved May 02, 2009, from http://www.gocsi.com/

Dehning, B., Richardson, V. J., & Zmud, R. W. (2007). The financial performance effects of IT-based supply chain management systems in manufacturing firms. *Journal of Operations Management, 25*(4), 806-824.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Ettredge, M., & Richardson, V. (2003). Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems, 17*(2), 71-82.

Floerkemeier, C., & Siegemund, F. (2003). *Improving the effectiveness of medical treatment with pervasive computing technologies.* Paper presented at the Ubicomp, Seattle, WA.

Foster, G. (1981). Intra-industry information transfers associated with earnings releases. *Journal of Accounting and Economics, 3*(3), 201–232.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61-83.

Helal, S., Giraldo, C., Kaddoura, Y., Lee, C., El Zabadani, H., & Mann, W. (2003). *Smart phone based cognitive assistant.* Paper presented at the UbiHealth.

Hitt, L. M., & Brynjolfsson, E. (1996). Productivity, business profitability, and consumer surplus: Three different measures of information technology value. *MIS Quarterly, 20*(2), 121-142.

Hovav, A., & D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. *Information Systems Security, 13*(3), 32-40.

Hovav, A., & D Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. *Information Systems Security, 13*(3), 32-40.

Hsu, C. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems, 18*(2), 140-150.

Hunton, J. E., Lippincott, B., & Reck, J. L. (2003). Enterprise resource planning systems: comparing firm performance of adopters and nonadopters. *International Journal of Accounting Information Systems, 4*(3), 165-184.

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, Forthcoming*, 15.

Kim, Y., Lacina, M., & Park, M. (2008). Positive and Negative Information Transfers from Management Forecasts. *Journal of Accounting Research, 46*(4), 885-908.

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.

Ko, M., Osei-Bryson, K., & Dorantes, C. (2009). Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms. *Information Resources Management Journal, 22*(2), 1-21.

Mills, E. (2009). Cybercrime cost firms $1 trillion globally. Retrieved September 25, 2009, from http://news.cnet.com/8301-1009_3-10152246-83.html

Mynatt, E. D., Essa, I., & Rogers, W. (2000). *Increasing the opportunities for aging in place*. Paper presented at the CUU '00 Proceedings on the 2000 conference on Universal Usability

Nicolaou, A. I. (2004). Firm performance effects in relation to the implementation and use of enterprise resource planning systems. *Journal of Information Systems, 18*(2), 79-105.

Otchere, I. (2005). Do privatized banks in middle-and low-income countries perform better than rival banks? An intra-industry analysis of bank privatization. *Journal of Banking & Finance, 29*(8-9), 2067-2093.

Ponemon. (2010). 2010 Annual Study: U.S. Cost of a Data Breach. Retrieved April 20, 2011, from http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

Rehak, J. (2002). Tylenol made a hero of Johnson & Johnson : The recall that started them all. Retrieved October 1, 2009, from http://www.nytimes.com/2002/03/23/your-money/23iht-mjj_ed3_.html

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.

Riddell, K. (2011). Security-Breach Costs Climb 7% to $7.2 Million per Incident. Retrieved May 10, 2011, from http://www.bloomberg.com/news/print/2011-03-08/security-breach-costs-climb-7-to-7-2-million-per-incident.html

Shen, R. (2008). The Role of Analysts in Intra-industry Information Transfer. *Seminars Accountancy* Retrieved May 10, 2011, from http://www.ckgsb.com/userfiles/doc/ck_faculty_researchSeminar_10.pdf

Siponen, M. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

Stanford, V. (2002). Pervasive health care applications face tough security challenges. *IEEE Pervasive Computing*, 8-12.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly, 14*(1), 45-60.

Szewczyk, S. H. (1992). The intra-industry transfer of information inferred from announcements of corporate security offerings. *Journal of Finance, 47*(5), 1935-1945.

Whitworth, B., & Zaic, M. (2003). The WOSP model: Balanced information system design and evaluation. *Communications of the Association for Information Systems, 12*, 258-282.