EFFECT OF SECURITY BREACHES ON OPERATING PERFORMANCE: EVIDENCE FROM FINANCIAL INSTITUTIONS

Shofiqur Rahman, College of Business Administration,
University of Texas at El Paso, 500 W. University, COBA 205, El Paso, TX 79912
srahman@utep.edu, 915-747-5496

Godwin Udo, Ph.D., College of Business Administration
University of Texas at El Paso, 500 W. University, COBA 205, El Paso, TX 79912
gudo@utep.edu, 915-747-5496

Fernando Parra, College of Business Administration
University of Texas at El Paso, 500 W. University, COBA 205, El Paso, TX 79912
parra@utep.edu, 915-747-5496

ABSTRACT

The main purpose of this paper is to investigate the operating performance of financial firms that experienced information security attacks. Our findings suggest that breached firms experience an increase in assets, a decrease in sales, and an increase in operating expenditure in the quarter immediately after the security breaches.

Keywords: Security Breach, Event Study, Operating Performance

INTRODUCTION

As the magnitude of the use of information technology (IT) (e.g. internet or intranet and network between suppliers and firms such as LAN or WAN) increases, security breaches have become a major issue and concern for corporate managers. Based on Forrester's survey on 410 IT decision makers, 75 percent report a concern on security breaches and more than 80 percent report financial losses as the aftermath of security breaches (Muncaster, 2006). Another survey conducted on managers of various U.S. and European firms shows that information security breaches have been a top concern in corporate decision making (Hovav, 2003). A number of studies looked at market reaction of information security breaches announced publicly (e.g. Campbell et al., 2003; Cavusoglu et al., 2004; Garg et al. 2003a, 2003b; Hovav et al., 2003; Hovav et al., 2004). In general, most of these studies use event study methodology and find that market discriminates breached firms in first few days and that breached firms experience financial losses. Given that industries are different in terms of products and services, customer base, and business processes, the impact of information security breaches may be perceived to be different. Since companies in financial industries mostly deal with money and maintain a database of customers' identity information and the consequence of security breaches is severe, it is quite reasonable to believe that managers and customers in financial industry are more likely to be sensitive to security breaches. Therefore, the main purpose of this paper is to examine the operating performance of financial firms and subsequent market reactions to them.

Most of the studies to date examine the impact of security breaches on market value and stock returns of firms. To the best of our knowledge, no prior studies, except Myung and Carlos (2006), look at the operating performance after the information security breach, a performance measure that relies on the operating income before depreciation. In addition, we also analyze the assets, sales, goodwill, short-term investment, and operating expense after the security breaches. Actions taken by the managers of breached firms in terms of increased spending on security after the events deserve more attention. Given that security breaches are major concerns of managers, firms are more likely to take costly steps to recover the loss and to avoid potential security threats. Further studies regarding this issue may answer the question as to whether investment and operating expense of breached firms increase after the events. Moreover, it would be valuable to examine if breached firms suffer an impairment of their goodwill after the event. In order to illuminate the above mentioned issues, this study attempts to investigate the operating performance of firms after the security breaches. The study also analyzes the initiatives of breached firms in terms of increase in operating expenditure and the reaction of investors in terms of changes in stock price after the public announcement of a security breach.

Our study is different from Myung and Carlos (2006) in three ways namely (a) our sample includes only financial firms; (b) sample period, and (c) methodology. Myung and Carlos' (2006) study examines financial performance, which is considered to be the closest match to operating performance. By using quarterly data for sample firms, we find a decline in operating performance of breached firms in the quarter next to the announcement quarter for security breach. We follow the methodology of Loughran and Ritter (1997) in which abnormal operating performance is measured on the basis of reference portfolio formed in each quarter. Using event study methodology, we also calculate abnormal returns of stocks and, as predicted, find negative abnormal stock returns, about 0.60%, of breached firms in (0, +1) window. This study contributes to the literature by trying to answer the following questions: Do security breaches have different implications on financial firms? When does the operating performance of breached firms decline? Do breached firms take initiatives in terms of increase in investment or operating expenditure to normalize business operation?

The remainder of this paper is organized into the following sections: literature review, hypotheses, data and methodology, results and discussion, and conclusion.

LITERATURE REVIEW

The stream of literature in information systems security has demonstrated increasing interest on the financial impact of security breaches based on the alarming escalation of the rate and severity of theft of intellectual property and personal data as described by Chief Operating Officer of the Information Assurance Directorate of the U.S. National Security Agency (Sager, 2011). Despite various attempts, scholars have struggled to measure the actual losses incurred on publicly traded companies based on different types of attacks (Cavusoglu et al., 2004). The results, mostly based on cumulative abnormal returns from publicly traded companies, have been mixed. While certain scholars find support of significant abnormal returns associated with security breaches (e.g. Andoh-Baidoo et al., 2010; Cavusoglu et al., 2004; Goel & Shawky, 2009; Goldstein et al., 2011; Gordon et al., 2011), others have not been able to find overall support (e.g. Campbell et al., 2003; Kannan et al., 2007).

The CIA (confidentiality, integrity and availability) framework

A good deal of variances in the findings among this type of studies is due to variety of security breaches involved. There are a several parameters and frameworks that can be used to analyze the nature of any security breach including Howard's Framework (Andoh-Baidoo et al., 2010) and LeVeque's Framework (LeVeque, 2006). LeVeque (2006) developed a framework by which all these events can be comprehensively classified based on the overall result of such breaches. This CIA framework can be explained as follows: (1) confidentiality breaches involving security breaches that attempt to acquire sensitive information in violation of authorization privileges; (2) integrity breaches aiming to corrupt the proper functionality of systems or data; (3) availability breaches focused on rendering a system unreachable for authorized users or resources (Chen et al., 2011). As such, most event studies have aimed to collect different type of security breaches based on the above referenced definition. Table 1 provides a summary of findings of studies in the information systems security field based on the CIA framework; almost half of these studies have demonstrated conflicting results based on their CIA framework classification.

Confidentiality Security Breaches

As displayed in Table 1, scholars have given confidentiality security breaches the most attention. Given that federal and certain state laws require companies to disclose disclosure of private identifiable information to victimized customers, it is easier to find public information regarding media announcements of security breaches involving confidential information. In addition, scholars have argued that the lost trust can be reflected in the loss of market valuation of publicly-traded companies (e.g. Garg et al., 2003a; Goel & Shawky, 2009). Studies that have focused specifically on the confidentiality security breaches reflect significant abnormal returns (see Table 1, e.g. Acquisti et al., 2006; Bose & Leung, 2008; Gatzlaff & McCullough, 2010; Malhotra et al., 2011). Of all the previous studies, only Patel (2010) and Gordon et al. (2011) dissent from the consensus. It is not surprising to find that events like the TJX data breach, which impacted an estimated 94 million records in 2007, or the Heartland Payment Systems in 2008 with 130 million records illegally disclosed, have exerted influence on the focus of scholarly research on this area.

Integrity Security Breaches

Integrity breaches have been scarce in the literature and are often challenged by the lack of public announcements regarding software vulnerabilities, viruses, or other malware that is aimed at corrupting the proper functionality of internal systems or data. Unless private identifying information is exposed, companies are not required to disclose this security breach publicly. As displayed in Table 1 Cavusoglu et al. (2004) and Goel and Shawky (2011) are the only studies that find statistically significant impacts on specific integrity security breaches. Campbell et al. (2003), Hovav and D'Arcy (2004, 2005), and Gordon et al. (2011) found no support for this premise.

TABLE 1. SUMMARY OF FINDINGS IN THE INFORMATION SYSTEMS SECURITY LITERATURE

Source	Confidentiality	Integrity	Availability	Overall	Significant Issues	Non-Significant
Campbell et al. (2003)	*	X	X	X		
Garg et al. (2003)	*		*			
Hovav & D'Arcy (2003)			*		eFirms	non-efirms
Cavusoglu et al. (2004)	*	*	*	*		
Hovav & D'Arcy (2004)		X				
Hovav & D'Arcy (2005)		X				
Acquisti et al. (2006)	*					
Kannan et al. (2007)				X	Post Dot-Com Era; Smaller Firms	
Bose & Leung (2008)	*					
Goel & Shawky (2009)	*	*	*	*		
Andoh-Baidoo et al.(2010)				*	Howard's Framework	Firm Size
Gatzlaff & McCullough (2010)	*				Response, Mkt-to-Book, Subsidiary	Repeated Attack, Stolen, Lost Data
Patel (2010)	X					
Chen et al. (2011)				*		
Goldstein et al. (2011)	*		*		Records #, eFirms, Tobin's Q	Article Size, Debt Ratio, Firms Size
Gordon et al. (2011)	X	X	*	*	Pre 9/11	Post 9/11
Malhotra et al. (2011)	*					

* = Statistically Significant Negative Abnormal Returns, X=Not Statistically Significant

Availability Security Breaches

Since the security breaches that brought Yahoo, Amazon and other major retailers' websites down in 2000, denial-of-service attacks have become common methods of attack. While some of the attacks are motivated by hacktivism, others are motivated by international conflict and state sponsored rivalries (Shackelford, 2009). As such, scholars have specifically focused on the effects of these types of attacks. Campbell et al.'s (2003) study is the only one that finds insufficient evidence supporting the notion that availability security breaches matter. Nonetheless, most authors agree that this has a significant negative effect on abnormal returns (e.g. Andoh-Baidoo et al., 2010; Cavusoglu et al., 2004; Garg et al., 2003a; Goel & Shawky, 2009; Goldstein et al., 2011; Gordon et al., 2011; Hovav & D'Arcy, 2003).

Overall, given the previous mixed results in the literature, it is imperative to provide a methodology that does not only look at an event study, but also provides a better picture of impact of security breach on firms' operating performance while taking into account the subsequent steps breached firms initiate. The present study attempts to do just that.

HYPOTHESIS DEVELOPMENT

The cost of information security breaches can be classified as short term and long term costs. Examples of short term costs include cost of repairs, cost of installing new systems, lost business due to temporary disruption, and lost productivity. Long-term costs may arise as the lost customers, lost partners, and costs associated with the legal liabilities. These costs are tangible or intangible in nature. Due to these costs, financial performance of the breached firms may decline after the events. Garg et al. (2003a) finds that breached firms experience decline in sales from 0.5 to 1 percent. Campbell et al. (2003) also finds highly negative market reaction to security breaches. Myung and Carlos (2006) reports that breached firms return on assets decreased in the fourth quarter. In order to be in line with these studies we propose the following hypotheses:

> *H1: The security breach incident will result in a decrease in operating performance of breached firms.*
>
> *H2: The security breach incident will result in an increase in operating costs of breached firms.*

Although test of market efficiency is a joint test, studies in finance, accounting, and information systems have been using it extensively. Market efficiency assumes that publicly available information is reflected in security price fairly quickly. Since the market tends to view security breach as negative, it should have negative impacts on stock price. The breached firms are more likely to have negative abnormal returns after the event. Empirical evidence of stock price performance is mixed: while Gordon et al. (2011), Chen et al. (2011), and Gatzlaff and McCullough (2010) find significant negative abnormal returns; Kannan et al. (2007), Bolster et al. (2010); and Patel (2010) find no such impact on security prices. This leads us to test stock price performance around the security breach. We, therefore, offer the following hypothesis:

H3: The security breach incident will result in a decrease in stock price of the breached firms, meaning that investors react to a security breach announcement negatively.

DATA AND METHODOLOGY

Based on The National Institute of Standards and Technology 800-95 guidelines, we define security breaches as any security violation that compromises the confidentiality, integrity and availability of an organization's information systems (2007). The Identity Theft Resource Center (www.idtheftcenter.org) is used as a primary source of identifying security breaches in the financial industry. Events are cross-referenced using LexisNexis and Google News to determine the first public disclosure of a security breach in a major publication. From the original sample, this study eliminates all those events that are not connected to a financial institution. Thus, our sample contains 122 financial institutions that experienced security breaches during 2005 to 2011. We aim to construct a sample that is free from the influence of the wave of DOS attacks in 2000 and all other subsequent attacks. Financial statement information of these firms is collected from COMPUSTAT database. In order to be included in the sample, a breached firm has to have SIC code of 6000 to 6799, information available in COMPUSTAT, and security attacks have to be at least one year apart. Appendix A lists all the financial firms that are used in the analysis. We measure operating performance of firms by assets, sales, investment, operating income, and operating expense on a quarterly basis. The ratio variables are scaled by asset and sales. Following Loughran and Ritter (1997), we measure raw operating performance and unexplained (abnormal) operating performance based on matching portfolio approach. In each quarter, we form quintile size portfolios using all available COMPUSTAT financial firms over the sample period and calculated median operating performance. The abnormal quarterly operating performance of a firm is the difference between the performance of sample firm and the median performance of the size matched portfolio.

In order to assess investors' reaction, we follow an event study that employs the market model. This model gives positive or negative abnormal returns based on the problems at hand. Following Wei et al.'s methodology (2011), our estimation period consists of 150 days (-171 to -22) and the event period consists of 1 to 3 days.

$$R_{it} = \propto_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

Where R_{it} is the return on firm i at time t, R_{mt} is the return for the market at time t. α and β are the regression constant and coefficient terms for the model. Once we estimate the model we predict the returns and subtract it from the observed return of the stocks. Following equation gives us the abnormal returns.

$$AR_{it} = R_{it} - (\propto_i + \beta_i R_{mt}) \quad (2)$$

Market returns and returns of individual stock are collected from Center for Research in Security Prices (CRSP). We use returns on S&P 500 as the market returns. Abnormal returns are calculated using three approaches- market model, mean adjusted returns, and market adjusted returns.

RESULTS AND DISCUSSION

Table 2 presents the distribution of information security breaches by calendar year and two digit industry classification based on two-digit SIC code. In Panel A, the year 2010 consists of 23.8 percent of the security breaches included in this paper. In addition, the year 2006, 2007, and 2011 also seem to have high number of security breaches. The distribution of breaches does not display any observable pattern. Panel B classifies security breaches in different industry groups based on a two-digit SIC code. The depository institutions, which mainly include banking and nonbanking financial institutions, face 61 threats, the highest number of security attacks.

TABLE 2: DISTRIBUTION OF SECURITY BREACHES BY CALENDAR YEAR AND INDUSTRY

Panel A: Number of security breaches by calendar year

Year	Number of Sample Security Breaches	Percentage of Sample
2005	9	7.4%
2006	24	19.7%
2007	18	14.8%
2008	13	10.7%
2009	10	8.2%
2010	29	23.8%
2011	19	15.6%
Total	122	100.0%

Panel B: Number of security breaches by industry classification

Industry	SIC code	Number of breaches
Depository Institutions	60	61
Non-depository Credit Institutions	61	12
Security And Commodity Brokers, Dealers, and Exchanges	62	15
Insurance Carriers	63	25
Insurance Agents, Brokers, And Service	64	2
Holding And Other Investment Offices	67	5
Others	--	2

Insurance carriers experienced 25 security breaches. Since banks and insurance companies are more likely to have identity information along with credit cards, social security, and other confidential information, these financial institutions are the main targets of hackers for potential identity theft.

In Table 3, the mean and median of financial variables of breached firms are presented on a quarterly basis. The assets mean (median) ranges from 412 to 446 (49.49 to 51.37) in billions of dollars. Firms show the highest sales in the second quarter. Operating expense, as a percentage of assets, increases from first quarter (6.94%) to fourth quarter (7.07%). Firms' operating incomes as percentage of assets also show a gradual increase in quarter to quarter, an increase from 1.15 percent to 1.28 percent. We also present information on all other financial variables related to firms operating performance to make a point that a firm's performance does not change abruptly over the quarters.

TABLE 3: DESCRIPTIVE STATISTICS ON BREACHED FIRMS

	Quarter-1	**Quarter-2**	**Quarter-3**	**Quarter-4**
	Mean (Median)	**Mean (Median)**	**Mean (Median)**	**Mean (Median)**
Assets-Total	412.22	445.59	427.99	446.09
	(51.18)	(51.37)	(49.49)	(50.79)
Invested Capital	98.16	103.60	102.77	86.46
	(11.95)	(11.95)	(9.52)	(9.50)
Operating Income	2.66	3.01	2.67	2.37
	(0.50)	(0.46)	(0.46)	(0.39)
Sales/ Turnover	8.20	9.01	8.28	8.29
	(1.96)	(2.20)	(1.91)	(1.95)
Operating Expense	5.53	6.19	5.60	6.07
	(1.08)	(1.49)	(1.05)	(1.29)
Goodwill (net)	13.16	13.23	12.80	11.71
	(2.39)	(2.19)	(1.77)	(1.68)
Operating Income/Assets	1.15%	1.21%	1.22%	1.28%
	(0.68)	(0.74)	(0.69)	(0.68)
Operating Income/Sales	9.97%	17.35%	13.52%	-17.72%
	(32.75)	(33.08)	(32.11)	(30.34)
Operating Expense/Assets	6.94%	7.06%	7.07%	7.07%
	(1.26)	(1.28)	(1.32)	(1.36)
Invested Capital/Assets	31.65%	31.52%	32.03%	28.71%
	(24.28)	(24.37)	(24.39)	(20.37)
Goodwill (net)/Assets	8.09%	8.38%	8.81%	7.51%
	(3.19)	(3.18)	(3.23)	(2.34)

Non-ratio numbers in parenthesis are median billion (USD $)

In Table 4, a firm's operating performance is measured in quarters relative to the event. It is reasonable to observe few changes in the operational variables of firms after the security breach. First, assets and investments may increase because of the fact that firms may tighten their security to keep them protected from future attacks by investing in capital expenditure or by improving network security. We observe that both assets and investment ratio increases from $52,329 to $51, 032 and 22.73% to23.62% respectively in the first quarter after the attack. Second, the security breach may result in lost sales. The reason is that customers may lose confidence in doing business with the company. We show that sales decline from $2,183 to

$2,111 in the quarter immediately after the breach. Finally, a firms' operating income (expense) is likely to decrease (increase) after the attack as the firm tries to recover the data loss.

TABLE-4: MEDIAN OPERATING PERFORMANCE MEASURES

Qtr. relative to breach	Assets	Sales	Goodwill /Assets	Inv /Assets	OIBDP Q/Assets	OIBDP Q /Sales	Op. Expense /Sales
-4	51,484.20	2,082.00	2.85%	22.87%	0.73%	31.85%	1.30%
-3	51,199.05	1,920.50	3.02%	23.08%	0.69%	32.02%	1.36%
-2	50,166.90	1,988.00	3.26%	22.29%	0.69%	32.34%	1.38%
-1	51,049.45	1,975.50	2.93%	24.62%	0.73%	32.10%	1.27%
0	52,329.75	2,183.30	2.62%	22.73%	0.70%	33.58%	1.25%
+1	51,032.40	2,111.00	3.06%	23.62%	0.67%	32.61%	1.27%
+2	51,787.25	2,116.00	3.23%	22.15%	0.66%	29.75%	1.31%
+3	35,216.28	1,718.50	3.23%	23.29%	0.71%	31.62%	1.29%
+4	50,317.90	2,250.00	3.14%	22.57%	0.69%	32.05%	1.45%

Numbers in million (USD $)

Figure 1 depicts the patterns of operating performance as hypothesized. The reason for company goodwill to rise after the attack is that firms take positive actions to improve their data security, which is perceived as good initiative by the market.

FIGURE-1: MEDIAN OPERATING PERFORMANCE M EASURES

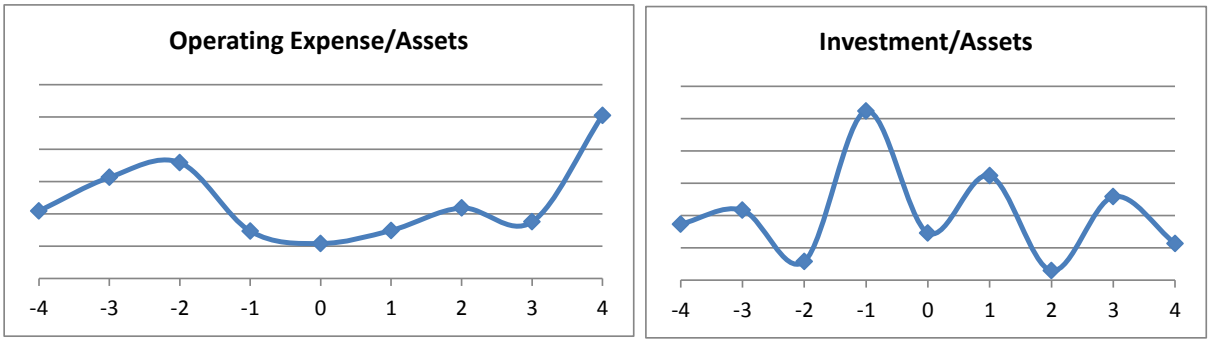

TABLE-5: ABNORMAL OPERATING PERFORMANCE BASED ON REFERENCE PORTFOLIO

Qtr. relative to breach	Assets	Sales	Goodwill	Inv/ Assets	OIBDPQ /Assets	OIBDPQ /Sales	Op. Expense/ Sales
-4	359.41**	6.81**	4.16%**	-1.69%	0.36%**	4.89%	3.58%**
	(5.10)	(5.71)	(3.22)	(-0.76)	(2.07)	(1.09)	(2.28)
-3	363.19**	6.71**	4.35%**	-2.16%	0.40%**	7.78%**	3.46%**
	(5.09)	(5.87)	(3.32)	(-0.98)	(2.15)	(2.07)	(2.41)
-2	342.20**	6.36**	4.73%**	-1.65%	0.18%	3.25%	3.51%**
	(4.85)	(5.45)	(3.51)	(-0.72)	(0.82)	(0.46)	(2.33)
-1	374.33**	6.99**	4.24%**	-1.96%	0.59%	-19.44%	3.91%**
	(5.20)	(5.85)	(3.41)	(-0.89)	(1.53)	(-0.81)	(2.58)
0	384.13**	6.89**	3.64%**	-2.43%	0.14%	-29.48%	3.22%**
	(5.28)	(5.84)	(3.10)	(-1.11)	(0.57)	(-1.08)	(2.36)
+1	389.45**	6.72**	4.23%**	-1.97%	-0.07%	-33.09%	3.55%**
	(4.98)	(5.62)	(3.26)	(-0.86)	(-0.16)	(-0.90)	(2.38)
+2	354.90**	6.41**	4.64%**	-2.20%	0.26%	4.24%	3.73%**
	(4.46)	(5.40)	(3.41)	(-0.89)	(1.18)	(0.59)	(2.39)
+3	352.42**	6.32**	5.07%**	8.81%	0.47%*	-12.34%	3.87%**
	(4.44)	(5.03)	(3.48)	(0.69)	(1.91)	(-0.99)	(2.39)
+4	364.96**	6.40**	5.13%**	5.84%	0.73%*	-18.14%	3.26%**
	(4.63)	(5.19)	(3.53)	(0.64)	(1.86)	(-0.72)	(1.99)

** 5% level and * 10% level; Assets and sales are in billion (USD $). T-values are in parenthesis.

In Table 5, we present the unexplained (abnormal) operating performance of breached firms. This was calculated by forming quintile size portfolios in each quarter and matching the sample firm with their respective portfolio. The difference in performance of sample firms and median portfolio performance is the abnormal performance. Among the variables, assets, sales, and operating expense clearly show an increasing pattern in the quarter immediately after the security breach. To be specific, sales decline from $6.99 billion to $6.89 billion and operating expense increases from 3.22% to 3.55%. We also find firms' asset increases from $384.13 billion to $389.45 billion from event quarter to the next quarter. However, we did not find any significant decrease in abnormal operating income though the associated signs come out as negative. On

average, we can conclude from this table that a firm's operating performance went down after the security breach.

The purpose of this section is to investigate how prices of financial institutions react to publicly announced security attacks and the results in Table 6 were generated for this purpose. To obtain the results in Table 6, we employ three approaches. First, using market model we measure CAR. Second, we measure abnormal returns using mean adjusted process. Finally, we measure abnormal returns using market adjustment. We do not find any pronounced impact of public information on security prices except for mean adjusted abnormal returns in 0 to +1 window. The breached firms lose about 0.57% of their value in two days including event day. This result is consistent in the sense that we find similar results in market adjusted abnormal returns. On average, a negative abnormal return of 0.60% is found in firms that experience information security breaches.

Table 6 documents one interesting result. Abnormal returns of breached firms are model or method sensitive. Mean adjusted and market adjusted abnormal returns shows negative performance of stock price after the security breach, while CAR shows almost zero abnormal returns. Given that past studies show mixed results in stock price performance and that results are sensitive to the approach abnormal returns are calculated, it corroborates the idea that test of market efficiency is a joint hypothesis.

TABLE-6: ABNORMAL RETURN MEASURES OF BREACHED FIRMS

Abnormal Returns	(-2 to +2)	(-1 to +1)	(0 to +1)	(0 to +2)	(0 to +3)
CAR (%)	1.00%*	0.18%	-0.15%	0.89%*	1.36%**
	(1.34)	(0.44)	(-0.50)	(1.51)	(1.64)
Mean adjusted (%)	-0.56%	-0.20%	-0.57%*	-0.53%	-0.21%
	(-0.80)	(-0.57)	(-1.51)	(-1.12)	(-0.44)
Market adjusted	0.42%	-0.21%	-0.60*	0.16%	0.63%
(%)	(0.70)	(-0.55)	(-1.51)	(0.45)	(1.18)

****** Significant at 5% level (one tailed) and ***** significant at 10% level (one tailed)

CONCLUSIONS

As the use of information technology has been more pronounced in the business world, firms are increasingly experiencing information security threats. Business managers seem to be concerned with this issue as firms incur costs associated with it. The main purpose of this study is to investigate the operating performance of financial firms that experience information security attacks. Our findings suggest that breached firms encounter an increase in assets, a decrease in sales, and an increase in operating expenditures in the quarter immediately following the security breaches. These results seem to be consistent when we create size portfolio and compare the sample firm's operating performance with the median performance of size-matched portfolio. Our conclusions support the conclusions reached by previous studies (e.g. Andoh-Baidoo et al., 2010; Cavusoglu et al., 2004; Chen et al., 2011; Goel & Shawky, 2009), but contradicts the

findings of other studies that found no support (e.g. Campbell et al., 2003; Kannan et al., 2007). More importantly, this study expands the previous literature by utilizing operating performance metrics to determine if there is indeed an impact on a financial firm when its security is breached.

Motivated by the mixed results of previous studies on stock price performance to publicly announced attacks, we also investigated price reactions of breached firms by employing three approaches to measure abnormal returns. The mean adjusted abnormal returns show negative price reactions to breached firms. On average, breached firms have about 0.60% negative abnormal returns in a two-day window after the security attacks. Investigation on firms' operating performance and reactions of investors will shed more light on the potential consequences of security breaches in financial industries. Given that measuring entire costs of security breaches is difficult and that operating performance has varieties of measurement scales, this study could be useful in further exploring the impact of security attacks on firms' operating performance.

Our findings indicate that abnormal returns of breached firms are model or method sensitive. This suggests that the results of any study on information security breaches should be interpreted in the light of the models or methods used. Another implication is that practitioners should examine alternative models in order to obtain a full picture of the impact of a breach on their abnormal returns.

APPENDIX A: LISTS OF FIRMS THAT EXPERIENCE INFORMATION SECURITY BREACHES OVER 2005 TO 2011

1st Source Corp	Fifth Third Bancorp	People's United Finl Inc
Aflac Inc	Firstfed Financial Corp/Ca	Piper Jaffray Cos Inc
Allied Irish Banks	Firstmerit Corp	PNC Financial Svcs Group Inc
Allstate Corp	Franklin Resources Inc	Premier Financial Bancorp
American Express Co	Great Florida Bank	Price (T. Rowe) Group
American International Group	Hartford Financial Services	Principal Financial Grp Inc
Ameriprise Financial Inc	Health Net Inc	Progressive Corp-Ohio
Assurant Inc	Heartland Financial Usa Inc	Prudential Financial Inc
Babson Capital Partn Invstrs	Heartland Payment Systems	Prudential Plc
Banco Santander Sa	HSBC Hldgs Plc	Regions Financial Corp
Bank Of America Corp	Humana Inc	Schwab (Charles) Corp
Bank Of New York Mellon Corp	Huntington Bancshares	Suffolk Bancorp
Bankatlantic Bancorp -Cl A	ING Globl Eq Div&Prem Opp Fd	Suntrust Banks Inc
BB&T Corp	ING Groep Nv	TD Ameritrade Holding Corp
Berkshire Bancorp Inc	Jones Lang Lasalle Inc	Toronto Dominion Bank
Blackrock Invt Qulty Mun Tr	JPMorgan Chase & Co	Track Data Corp

BSB Bancorp Inc	Keycorp	Transamerica Income Shares
Capital One Financial Corp	Lincoln National Corp	Tree.Com Inc
Cigna Corp	LPL Investment Holdings Inc	US Bancorp
Citigroup Inc	M & T Bank Corp	UBS Ag
Citizens Holding Co	Mastercard Inc	Valley National Bancorp
City Holding Co	Medallion Financial Corp	Visa Inc
Columbia Banking System Inc	Metlife Inc	Wachovia Corp
Community Valley Bancorp/Ca	Metro Bancorp Inc	Wellpoint Inc
Compucredit Holdings Corp	Moneygram International Inc	Wells Fargo & Co
Credit Suisse Group	Morgan Stanley	Western Union Co
Credit Suisse Hi Yield Bd Fd	Nasdaq Omx Group Inc	WFS Financial Inc
Discover Financial Svcs Inc	National Financial Prtnrs Cp	WSB Holdings Inc
ESB Financial Corp	Omniamerican Bancorp Inc	

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? an event study. Paper presented at the *Fifth Workshop on the Economics of Information Security*.

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.

Bose, I., & Leung, A. (2008). Assessment of phishing announcements on market value of firms. Paper presented at the *2008 International Conference on Information Technology*, 304-307.

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

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(2003), 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), 69-104.

Chen, J. V., Li, H. C., Yen, D. C., & Bata, K. V. (2011). Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior*, 28(2), 456-464.

Garg, A., Curtis, J., & Halper, H. (2003a). The financial impact of IT security breaches: what do investors think? *Information Systems Security*, 12(1), 22-33.

Garg, A., Curtis, J., & Halper, H. (2003b). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(3), 74-83.

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

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

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, 12(9), 2.

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.

Hovav, A., & D'Arcy, 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 Systems Security*, 12(2), 32-40.

Hovav, A., & D'Arcy, J. (2005). Capital market reaction to defective IT products: The case of computer viruses. *Computers & Security*, 24(5), 409-424.

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.

LeVeque, V. (2006). *Information security: A strategic approach*. Hoboken, NJ: IEEE Computer Society Publications, Wiley-Interscience.

Loughran, Tim, &Jay Ritter. (1997). The operating performance of firms conducting seasoned equity offerings. *The Journal of Finance*, 52, 1823–1850.

Malhotra, A., & Malhotra, C. K. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14(1), 44.

Myung, K., & Carlos, D. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, XVII(2), 13-22.

Muncaster, P. (2006). IT Decision-makers more concerned about security. *VNU Network*, http://www.computing.co.uk/ctg/news/1850276/it-decision-makers-concerned-security.

Patel, N. (2010). *The effect of IT hack announcements on the market value of publicly traded corporations*. (Doctoral dissertation). Retrieved from Duke University Dissertations and Theses.

Sager, T. (2011). Web Interview with Tony Sager, Chief Operating Officer of the Information Assurance Directorate of the U.S. NSA. *Second Annual Trusted Computing Conference*, Orlando, FL. Sept 20-22, 2011. http://searchsecurity.techtarget.com/video/NSAs-Sager-on-cyberwarfare-likelihood-of-digital-Pearl-Harbor

Shackelford, S.J. (2009). Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks (November 4, 2009). *Journal of Internet Law*, Forthcoming. Available at SSRN: http://ssrn.com/abstract=1499849

Singhal, T., Winograd, T. & Scarfone, K. (2007). Guide to Secure Web Services. Recommendations of the National Institute of Standards and Technology (NIST). *Special Publication 800-95*. U.S Department of Commerce.

Wei, Z., Xie, F., Posthuma, R.A. (2011). Does it pay to pollute? Shareholder wealth consequences of corporate environmental lawsuits. *International Review of Law and Economics*, 31(3), *212-218.*