THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

WP # 0007IS-301-2007

February 5, 2007

Myung Ko[a], Kweku-Muata Osei-Bryson,[b,] and Carlos Dorantes [c]

. [a]Department of Information Systems and Technology Management
College of Business
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249, USA
Email: myung.ko@utsa.edu

[b]Department of Information Systems and
The Information Systems Research Institute
Virginia Commonwealth University
Richmond, VA 23284, U.S.A.
Email: Kweku.Muata@isy.vcu.edu

[c]Department of Information Systems and Technology Management
College of Business
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249, USA
Email: carlos.dorantes@utsa.edu

UTSA
COLLEGE OF BUSINESS KNOWLEDGE FOR A NEW WORLD

ONE UTSA CIRCLE
SAN ANTONIO, TEXAS 78249-0631
210 458-4317 | BUSINESS.UTSA.EDU

Investigating the impact of publicly announced information security breaches on organizational performance

Myung Ko[a], Kweku-Muata Osei-Bryson,[b,] and Carlos Dorantes [c,]

[a]Department of Information Systems and Technology Management
College of Business
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249, USA
Email: myung.ko@utsa.edu

[b]Department of Information Systems and
The Information Systems Research Institute
Virginia Commonwealth University
Richmond, VA 23284, U.S.A.
Email: Kweku.Muata@isy.vcu.edu

[c]Department of Information Systems and Technology Management
College of Business
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249, USA
Email: carlos.dorantes@utsa.edu

Investigating the Impact of Publicly Announced Information Security Breaches on Organizational Performance

Abstract

This paper examines the impact of information security breaches on organizational performance. Up to now, there are only a few previous studies that investigated the stock market reaction of security breaches over a few days from the announcement. Using a matched sample comparison group, we investigated the impact of information security breaches on breached firms' performance over a period of four quarters from the public announcement and examined whether breached firms perform worse than before the breach or worse than their peer firms in the industry. The results of our study appear to counter to initial expectations, suggesting that for some of performance measures of the breached firm were better after the breach than for the corresponding pre-breach period and also the treatment firms outperformed their peer firms in the industry for the most of performance measures. Thus, although the market value of the breached firm might drop temporarily as indicated in the previous event studies, it did not impact on its financial performance over the longer periods of time, at least, over four quarters as shown in our study**.** Our study also includes some important implications for managers and stock market investors.

Keywords: Information security, impact, security breach, organizational performance

INTRODUCTION

Today, as more organizations conduct their businesses over the Internet, exposure to security attacks is also increasing. The 2004 Global Security Survey of financial institutions by Deloitte and Touche reported that 83 percent of respondents indicated that their systems had been compromised in 2004, compared to 39 percent in the previous year, a remarkable increase of over 100% in a single year (Anonymous, 2004). Also, the 2005 Computer Crime and Security Survey by Computer Security Institute (CSI) revealed that the average loss per incident from *unauthorized access to information* has increased dramatically to $300K from 51K and also the loss from *theft of proprietary information* has also increased to $356K from $169K, which represents more than doubled from 2004 (Gordon et al., 2005; Gordon et al., 2004). Thus, a security breach incident could result in tremendous financial losses to organizations (Warren & Hutchinson, 2000; Egan & Mather, 2005).

While there are many news and surveys that have reported the magnitude of the monetary losses from the breached incidents, there have been only a few academic studies that have investigated empirically on this issue. Also, these previous studies investigated the market reaction of information security breaches announced publicly over periods of 0 to 25 days from the announcement using an event study methodology. (Garg et al., 2003a, 2003b; Hovav & D'Arcy, 2003 & 2004; Campbell et al., 2003; Cavusoglu et al., 2004). Thus, the economic impact of security breaches over the extended period is not known yet.

The main purpose of our study is to investigate the impact of information security breaches on organizational performance over a period of four quarters from the public announcement. We believe that our study is important for several reasons. First, unlike previous studies that investigated the stock market reaction of security breaches over a few days, our study investigates the impact of the breach incidents on organizational performance to determine whether the breach announcement leads to the decreased organizational performance. Second, we investigate the breach impact over the longer period than before. Third, the results of our study provide additional insight to top managers about the impact of publicly announced breach, which can help revise security measures or budget if necessary.

In the following section, we discuss the literature review. Then, we describe financial performance measures used to determine the impact of the breached firms. The research methodology and the sample selection technique are followed after that. In the subsequent section, we discussed the statistical analysis, followed by details of results, conclusion, and discussion.

LITERATURE REVIEW

Table 1 includes a brief summary of the previous studies that have investigated the economic impact of information security breaches announced publicly.

Table 1 Summary of previous event studies

Author	Period studied	Number of events	Major findings
Campbell, et al.	1995 - 2000	43 events	- significant negative return involving unauthorized

Author	Period studied	Number of events	Major findings
(2003)			access to confidential information and no changes in return for other types of breach
Cavusoglu, et al. (2004)	1996 - 2001	66 events	• negative return on the market value of the breached firms and positive return of the Internet security developer
Hovav & D'Arcy (2003)	1998 - 2002	23 events	• a significant negative impact on Internet-specific companies
Hovav & D'Arcy (2004)	1988 - 2002	186 events	• no negative abnormal returns
Garg, et al. (2003b)	1996 - 2002	22 events	• on average, the loss to a company was $17 - 28 million per incident

All of the previous studies used an event study methodology, which is based on the assumption that capital markets are efficient to evaluate the impact of the events on expected future profits of the firms (Dasgupta, et al., 1998).

Campbell et al. (2003) examined the stock market reaction to security breaches for a period of 0 to 3 days from the announcement and found that not all types of security breaches have similar economic impacts. The authors found that a significant negative reaction for those breaches that are related to confidential information and did not find any significance from the other types of breaches. Cavusoglu et al. (2004) found that announcement of an Internet security breach is negatively associated with the market value of the breached firm. Their study indicated that the breached firms lost on average 2.1 percent of their market value within two days of the announcement and the loss was larger for net firms than for conventional firms. Their study also indicated that Internet security developer realized significant positive return from the announcement. Hovav & D'Arcy (2003) investigated the market reaction to denial-of-service (DOS) attack announcements for a period from 0 to 25 days and found that there is no significant impact of DOS attacks on the capital market. However, they found that Internet-specific firms do have negative abnormal returns during the five days following the announcement. On the other hand, Hovav & D'Arcy (2004) investigated the market reaction to virus attack announcements and found that there is no significant impact over the 0 to 25 days event window. Garg et al. (2003b) also examined the market reaction to security breaches and reported that all types of security breaches realized a negative abnormal return over a three-day period from the announcement. However, their study reported that security breaches related to credit card information theft realized the most significant negative impact. In addition, the market value of security companies realized the positive impact to security breaches.

In general, publicly announced security breach incidents do have a significant impact on the market value of breached companies or other related companies over a few days from the announcement. However, up to now, the effect on the overall financial performance of the security breached firms over a longer period than a few days has not been addressed yet.

SECURITY BREACHES

Types of security breaches include virus, unauthorized access, theft of proprietary information, denial of service (DOS), sabotage, and Web site defacement, etc. The 2004 E-crime watch survey by CSO magazine reported that 43 percent of respondents noted an increase in security breaches compared to the previous year and seventy percent had experienced at least one breach incident[1]. Although these security incidents are continuously rising, more organizations have tendency not to report the breaches to law enforcement because they are concerned about negative publicity (Gordon et al., 2005).

The 2005 Survey by CSI reported that virus attacks represent the greatest financial losses and they account for 32 percent of the overall losses reported (Gordon et al., 2005). There is little doubt that the breach incident can have a significant impact on the breached company's performance or other related companies. However, assessing the impact of security breaches is very difficult because costs of security breaches are not easy to quantify (Mercuri, 2003) or because organizations are not be willing to provide financial figures (Kros et al., 2004/2005).

Costs associated with a security breach include: cost of repairs; cost of replacement of the system; lost business due to the disruption of business operations; loss of existing customers, future customers, or business partners due to a negative reputation of the organization; and potential legal liabilities from the breach (Cavusoglu et al., 2004; Tsiakis & Stephanides, 2005; D'Amico, 2000; Featherman et al., 2006). As a result, it would appear reasonable to expect decreased financial performance (i.e. decreased profit, increased cost) of a breached firm, particularly when its financial performance is compared to its performance before the breach.

[1] This was obtained at http://www.cert.org.

To measure a firm's performance, accounting measures are the most popular approach (Barney, 1997). These measures include ratios, which have been also used in previous studies (Hitt & Brynjolfsson 1996; Bharadwaj 2000; Hunton et al. 2003; Nicolaou 2004). In this study, we used four profit ratios (ROA, ROS, OI/A, and OI/S) and two cost ratios (COGS/S and TOE/S). Return on assets (ROA) is the frequently used and a useful financial measure for an overall performance indicator (Hunton et al., 2003; Grover & Saeed, 2004). Return on sales (ROS) is another indicator measuring a firm's profitability. Operating income to assets (OI/A) and operating income to sales (OI/S) consider returns on the income from operations only. Cost of goods sold to sales (COGS/S) measures the percentage of sales used to pay for expenses related to sales, and total operating expenses to sales (TOE/S) measures the percentage of sales used to pay for total operating costs. See Table 2 for the descriptions of the financial performance measures.

Table 2: Description of Financial Performance Measures

Performance Variable	**Description**
Return on Assets (**ROA**)	*Net Income / Total Assets*
Return on Sales (**ROS**)	*Net Income / Net Sales*
Operating Income to Assets (**OI/A**)	*Operating Income before Depreciation Charges / Total Assets*
Operating Income to Sales (**OI/S**)	*Operating Income before Depreciation Charges / Net Sales*
Cost of Goods Sold to Sales (**COGS/S**)	*Cost of Goods Sold / Net Sales*
Total Operating Expenses to Sales (**TOE/S**)	*Total Operating Expenses / Net Sales*

Thus given the expectation that a firm's profit ratios will be decreased and its cost ratios will be increased after a security breach, we propose the following hypotheses for evaluation:

H1A: The *Return on Assets* (ROA) of a firm that has experienced a security breach incident is lower after the breach than before the breach.

H1B: The *Return on Sales* (ROS) of a firm that has experienced a security breach incident is lower after the breach than before the breach.

H1C: The *Operating Income to Assets* (OI/A) of a firm that has experienced a security breach incident is lower after the breach than before the breach.

H1D: The *Operating Income to Sales* (OI/S) of a firm that has experienced a security breach incident is lower after the breach than before the breach.

H1E: The *Cost of Goods Sold to Sales* (COGS/S) of a firm that has experienced a security breach incident is higher after the breach than before the breach.

H1F: The *Total Operating Expenses to Sales* (TOE/S) of a firm that has experienced a security breach incident is lower after the breach than before the breach.

In addition, it seems reasonable to expect that the breached firm's profit ratios are lower and its cost ratios are higher than those of its peer firms that have not experienced any breach incident in the industry in subsequent quarters. Thus, the following hypotheses are proposed.

H2A: The *Return on Assets* (ROA) of a firm that has experienced a security breach incident is significantly lower than the ROAs of all peer firms that have not experienced a breach incident in the industry in subsequent quarters.

H2B: The *Return on Sales* (ROS) of a firm that has experienced a security breach incident is significantly lower than the ROSs of all peer firms that have not experienced a breach in the industry in subsequent quarters.

H2C: The *Operating Income to Assets* (OI/A) of a firm that has experienced a security breach incident is significantly lower than the OI/As of all peer firms that have not experienced a breach in the industry in subsequent quarters.

H2D: The *Operating Income to Sales* (OI/S) of a firm that has experienced a security breach incident is significantly lower than the OI/Ss of all peer firms that have not experienced a breach in the industry in subsequent quarters.

H2E: The *Cost of Goods Sold to Sales* (COGS/S) of a firm that has experienced a security breach incident is significantly higher than the COGS/Ss of all peer firms that have not experienced a breach in the industry in subsequent quarters.

H2F: The *Total Operating Expenses to Sales* (TOE/S) of a firm that has experienced a security breach incident is significantly higher than the TOE/Ss of all peer firms that have not experienced a breach in the industry in subsequent quarters.

RESEARCH METHODOLOGY

In this study, we used "matched sampling" methodology, which has also been used in several previous studies (e.g., Balakrishnan et al., 1996; Hunton et al., 2003; Bharadwaj, 2000). A treatment group represents firms that have experienced information security breaches and a control group represents firms that were selected to match the treatment group by size and industry.

Sample Selection

Treatment Group (Breached Firms)

Our sample includes publicly announced all information security breach incidents for the period from 1997 to 2004 but including announcements of publicly traded firms. Following procedures are taken to select our sample.

We collected data using business news articles in the Lexis/Nexis Academic database. The key words used to search the data are "attack," "breach," "break-in," "hacker," "Internet," "security," "virus," "information," and "computer." A combination of such key words, names of breached firms that were reported in previous studies, and names of viruses that were identified in previous studies were also used. This approach is similar to the method used by previous studies (Cavusoglu et al., 2004; Campbell et al., 2003; Andoh-Baidoo & Osei-Bryson, 2006). Initially, the data set includes 105 cases and then any duplicated announcements were eliminated. Then, announcements that have missing financial data from Compustat were eliminated since these announcements have insufficient data necessary for our analysis. Finally, firms that didn't have any potential matching firms were eliminated. Thus, the final treatment sample is reduced to 75 when it is matched with firms in the same primary two-digit standard industry classification (SIC) code and it is reduced to 52 when it is matched with firms in the four-digit SIC code.

For the treatment sample, we collected quarterly financial data from Compustat for past 3 years before the incidents (12 quarters) and calculated 3-year average quarterly performance for each performance measure. Then, these pre-incident performance measures were compared with corresponding post-incident measures, resulting in the "differences within the breached sample." We believe using the 3-year average quarterly performance measures is a more robust approach since it can reduce the potential variability that could arise from choosing a single quarterly performance measures.

Control Group (Non-Breached Firms)

While selecting a single benchmark firm for each breached firm can be one approach, selecting all the firms in the same industry and size as the benchmark is also another approach, which we believe, is a more robust approach to control for confounding factors in industry and/or the firm size. Thus, we followed several steps selecting a matching sample that is comparable to the treatment sample.

Initially, firms from the same primary two and four digit SIC codes were selected from Compustat as potential control firms for each treatment firm. Then, we used *annual total assets* as the size measure, which is commonly used as a proxy for the firm size, and selected control firms that are between 70% and 130 % of the treatment firm's total asset (Barber & Lyon 1996; Bharadwaj 2000; Hunton et al., 2003). Thus, for each treatment firm, one or more matching control firms were selected.

Then we calculated the 3-year average quarterly financial performance measures before the incident for each control firm. Next, we calculated the overall average performance measures before the incident of all control firms that are selected for each applicable breached firm. These pre-incident performance measures were compared with the corresponding post-incident measures, resulting in the "differences within the control sample." After that, the performance between treatment and control samples can be compared, resulting in "differences between treatment and control samples."

To check the validity of our sample selection, the treatment and control samples were compared to determine if there are any significant differences between the two samples. For this, we adopted commonly used size measure such as total assets and sales. Tables 3 and 4 present descriptive statistics of these two samples. Both t-test results and Mann-Whitney test results in the Table 4 indicate that there are no significant differences between the treatment and control samples. Further, although the Mann-Whitney test in the Table 3 might seem to indicate that the control sample differed from the treatment sample on sales reported, this difference is not statistically significant (p = 0.23). Thus, treatment and control firms appear to be well matched on the size measure.

Table 3: Descriptive Statistics (Two-Digit)

	Treatment sample		Control Sample		Mann-Whitney Test	T-test
Variable	**Mean**	**Median**	**Mean**	**Median**	**Z**	**T**
Total assets (billion$)	42.760	5.854	42.857	7.346	-0.286	0.012
Sales (billion$)	3.167	1.011	3.507	1.105	-1.210	0.703

Table 4: Descriptive Statistics (Four-Digit)

	Treatment sample		Control Sample		Mann-Whitney Test	T-test
Variable	**Mean**	**Median**	**Mean**	**Median**	**Z**	**T**
Total assets (billion$)	49.490	3.519	47.936	3.310	-0.293	0.194
Sales (billion$)	2.780	0.459	2.920	0.319	-0.021	-0.131

STATISTICAL ANALYSIS

Examining underlying distributions of the variables revealed that distributions of these performance variables are not normal and a standard t-test would not be appropriate for this study. Thus, a non-parametric test is used to compare the differences of performance variables for the treatment and control samples.

In order to test H1A to H1F, first, 3-year average quarterly performance measures for the treatment (PMT) before the incident for quarters, *Q(-1)* to *Q(-4),* are calculated and this is called PMT_{pre}. We believe that using a 3-year average performance measure is a better indicator of the firm's past performance than using a single quarter's performance measure. These calculated measures are matched against performance measures after the incident, PMT_{post}, for the corresponding quarters, *Q1* to *Q4*, and the relative change in each quarterly performance measure, ΔPMT, is calculated as follows:

$$\Delta PMT_j = PMT_{post} - PMT_{pre}$$

$$= PMT\, Y_{4j} - 1/3 \sum_{i=1}^{3} PMTYij \qquad (1)$$

where i ($i = 1, 2, 3$) represents *previous* i^{th} year, j (j = 1, ..4) represents j^{th} quarter, assuming Y_4 is the year subsequent to the incident, and Y_1 represents a year before the incident, etc.

The calculated relative change, ΔPMT_j is referred to as the "*differences within treatment sample.*" We used the Wilcoxon signed ranks test, a paired non-parametric test, since it is adequate when comparing two values, before and after the incident, of the same firm (Moore & McCabe, 2003).

For testing H2A through H2F, 3-year average quarterly performance measures of the treatment and control firms, PMT_{pre} and PMC_{pre}, for the quarters, *Q(-1)* to *Q(-4),* are calculated and they are matched against performance measures subsequent to the incident, PMT_{post}, and PMC_{post}, for the corresponding quarters, *Q1* to *Q4* to calculate the relative changes in performance measures of the treatment firms and those of the control firms. Then, the differences between the two samples, ΔPM, are calculated by subtracting the relative change in performance measures of the treatment sample, ΔPMT, from those of the control sample, ΔPMC, as follows:

$$\Delta PM_j = \Delta PMC_j - \Delta PMT_j \qquad (2)$$

where j (j = 1, ..4) represents j^{th} quarter

The calculated relative change, ΔPM_j, is referred to as the "*differences between the treatment and control samples*." For this analysis, we used the Mann-Whitney U test (or Wilcoxon rank-sum test), a non-parametric test for two independent samples, since it is adequate when comparing mean difference for the two different samples – the treatment and control firms (Kutner et al., 2005).

RESULTS

Differences within Treatment Sample

The results of the "differences within treatment sample" are presented in the tables 5 and 6. For profit ratios, a negative Z value means that the ratio of breached sample after the incident is lower than that before the incident and thus, it indicates the decrease in performance. Accordingly, a negative Z value for cost ratios means that the ratio after the incident is lower than that before the incident and thus, it indicates the increase in performance since it suggests more efficient operations after the breach (refer to equation (1) for the calculation of ΔPMT).

Table 5 Differences within Treatment Sample (Two Digit)

Performance measures	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
	Z	p value	Z	P value	Z	p value	Z	p value
Difference in ROA	-0.613	0.540	-1.800	0.072[c]	0.278	0.781	0.062	0.951
Difference in ROS	2.490	0.013[b]	2.411	0.016[b]	4.475	0.000[a]	1.611	0.107
Difference in OI/A	-1.079	0.280	-2.207	0.027[b]	-0.095	0.925	0.713	0.476
Difference in OI/ S	2.126	0.034[b]	1.179	0.238	3.020	0.003[a]	2.851	0.004[a]
Difference in COGS / S	-1.217	0.224	-2.705	0.007[a]	-2.533	0.011[b]	-1.801	0.072[c]
Difference in TOE / S	-2.538	0.011[b]	-3.411	0.001[a]	-3.627	0.000[a]	-2.811	0.005[a]

[a] 1 % level
[b] 5 % level
[c] 10 % level

Table 6 Differences within Treatment Sample (Four Digit)

Performance measures	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
	Z	p value	Z	p value	Z	p value	Z	p value
Difference in ROA	-0.887	0.375	-2.094	0.036[b]	1.650	0.099[c]	0.929	0.353
Difference in ROS	1.505	0.132	0.860	0.390	4.026	0.000[a]	1.749	0.080[c]
Difference in OI/A	0.292	0.770	-2.114	0.035[b]	1.120	0.263	1.330	0.184
Difference in OI/ S	1.657	0.097[c]	0.572	0.567	2.639	0.008[a]	2.441	0.015[b]
Difference in COGS / S	-1.342	0.180	-2.482	0.013[b]	-1.601	0.109	-1.330	0.184
Difference in TOE / S	-1.657	0.097[c]	-2.870	0.004[a]	-3.010	0.003[a]	-2.386	0.017[b]

[a] 1 % level
[b] 5 % level
[c] 10 % level

The overall results from the differences in performance within treatment sample using two and four digit industry codes are summarized as follows:

- The results indicated the decrease in ROA for the first two quarters since signs of Z values are negative in the first and second quarters although only the second quarter's decrease is statistically significant.
- It appears that return on sales (ROS) and operating income to sales (OI/S) are higher in subsequent quarters than quarters before the incident since signs of the Z values are positive. The results indicate that ROS was significant for the first three quarters and OI/S was significant for the first, third, and last quarters.
- Operating income to assets (OI/A) was significant in the second quarter, which represents the decrease in performance since a sign of Z value is negative.
- All the cost ratios have negative z values, which suggest the overall increase in performance since they represent the decrease in costs. Although cost of goods sold over sales (COGS/S) was significant except for the first quarter (Table 5) and in the second quarter (Table 6), total operating expenses to sales (TOE/S) was significant for all four quarters.

Overall, the treatment sample's financial performance in the quarters subsequent to security breach did not decrease except in the case of ROA and OI/A. In fact, our results indicated otherwise. The profit ratios, ROS and OI/S, have increased and the cost ratios, COGS/S and TOE/S, have decreased, which represent the overall increase in performance. Thus, these results appear to contradict to our initial expectations, suggesting that for some of these performance measures of the breached firm were better after the breach than for the corresponding pre-breach period. Based on the results of our analysis, we concluded that:

H1A: partly supported

H1B: not supported.

H1C: partly supported.

H1D: not supported.

H1E: not supported.

H1F: not supported.

Differences between Treatment and Control Samples

The results of differences in performance between two sample groups are presented in the Tables 7 and 8. A negative Z value means that the relative difference in performance of breached sample is higher than that of control sample (refer to equation (2) for the calculation of ΔPM).

Table 7 Differences between the Treatment and Control Samples (Two Digit)

Performance measures	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
	Z	P value	Z	p value	Z	p value	Z	P value
Difference in ROA	0.036	0.971	-0.006	0.995	0.912	0.362	0.777	0.437
Difference in ROS	1.731	0.083[c]	2.624	0.009[a]	3.625	0.000[a]	1.005	0.315
Difference in OI/A	-1.984	0.047[b]	-1.769	0.077[c]	-1.485	0.138	0.481	0.630
Difference in OI/ S	-0.652	0.515	-0.172	0.863	0.043	0.966	0.422	0.673
Difference in COGS / S	-0.283	0.777	-1.067	0.286	-1.773	0.076[c]	-0.533	0.594
Difference in TOE / S	-2.275	0.023[b]	-2.476	0.013[b]	-3.329	0.001[a]	-1.768	0.077[c]

[a] 1 % level
[b] 5 % level
[c] 10 % level

Table 8 Differences between the Treatment and Control Samples (Four Digit)

Performance measures	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
	Z	P value	Z	p value	Z	p value	Z	p value
Difference in ROA	0.334	0.739	0.387	0.699	-0.346	0.729	-1.073	0.283
Difference in ROS	-1.202	0.229	-1.368	0.171	-1.176	0.240	-1.112	0.266
Difference in OI/A	-0.225	0.822	0.991	0.322	-1.345	0.179	-1.469	0.142
Difference in OI/ S	-0.108	0.914	0.288	0.774	-1.153	0.249	-1.508	0.131
Difference in COGS / S	-0.376	0.707	0.302	0.763	-0.238	0.812	-0.228	0.820
Difference in TOE / S	0.033	0.973	0.856	0.392	1.099	0.272	0.923	0.356

[a] 1 % level
[b] 5 % level
[c] 10 % level

The overall results from the differences in performance between two groups using two and four digit industry codes are summarized as follows:

- Overall, the relative differences in profit ratios indicated that treatment sample has higher difference in performance compared to the control sample. Although the results of Table 8 indicated that none of the profit and cost ratios was significant in any quarter, their results are in agreement with those in the Table 7 in general.

- The relative differences in COGS/S indicated that treatment sample has higher difference in performance compared to the control sample. However, the differences in TOE/S indicated otherwise.

Although Tables 7 and 8 indicate the relative differences in performance between two sample groups, these results do not indicate the magnitudes of the differences. Thus, we prepared Tables 9 and 10 to compare the average performance values of the two groups and determined which sample group has higher performance. Construction of tables 9 and 10 involves multi-step procedure that is described in the Appendix.

Table 9 Comparison of Differences between Treatment and Control Samples (Two Digit)

Item	Quarter	Median value (Treatment firms)	Median Value (Control firms)	Higher Performance Group
Difference in ROA	Q2	0.0005[c]	0.0006[b]	Control
Difference in ROS	Q1	-0.014 [b]	-0.0050 (N/S)	Treatment
	Q2	-0.0199[b]	0.0004 (N/S)	Treatment
	Q3	-0.0306[a]	-0.0023 (N/S)	Treatment
Difference in OI/A	Q1	0.0010 (N/S)	-0.0020[c]	Control
	Q2	0.0033[b]	0.0006 (N/S)	Treatment
	Q3	0.007 (N/S)	0.0016[c]	Control
Difference in OI/ S	Q1	-0.0146[b]	-0.0277[b]	Treatment
	Q3	-0.0295[a]	-0.0192[b]	Control
	Q4	-0.0358[a]	-0.0341 (N/S)	Treatment
Difference in COGS/S	Q2	0.0180[a]	0.0163[b]	Control
	Q3	0.0249[b]	0.0010 (N/S)	Treatment
	Q4	0.0112[c]	0.0004 (N/S)	Treatment
Difference in TOE/S	Q1	0.0176[b]	-0.0068 (N/S)	Treatment
	Q2	0.0395[a]	0.0123 (N/S)	Treatment
	Q3	0.0298[a]	-0.0037 (N/S)	Treatment
	Q4	0.0358[a]	0.0001(N/S)	Treatment

[a] 1 % level
[b] 5 % level
[c] 10 % level
N/S: not significant

Table 10 Comparison of Differences between Treatment and Control Firms (Four Digit)

Item	Quarter	Median value (Treatment firms)	Median Value (Control firms)	Higher Performance Group
difference in ROA	Q2	-0.0015[b]	-0.0007 [b]	Control
	Q3	0.0008[c]	0.0009 (N/S)	Treatment
difference in ROS	Q3	0.0320[a]	0.0185[c]	Treatment
	Q4	0.0114[c]	0.0054 (N/S)	Treatment
difference in OI/A	Q2	-0.0008[b]	-0.0006 (N/S)	Treatment
difference in OI/ S	Q1	0.0170[c]	0.0171[c]	Control
	Q3	0.0425[a]	0.0141(N/S)	Treatment

Item	Quarter	Median value (Treatment firms)	Median Value (Control firms)	Higher Performance Group
	Q4	0.0420^{b}	0.0085 (N/S)	Treatment
difference in COGS/S	Q1	-0.0135 (N/S)	-0.0200^{b}	Control
	Q2	-0.0341^{b}	-0.0354^{a}	Control
	Q3	-0.0272 (N/S)	-0.0124^{b}	Control
	Q4	-0.0159 (N/S)	-0.0087^{b}	Control
difference in TOE/S	Q1	-0.0167^{c}	-0.0171^{c}	Control
	Q2	-0.0482^{a}	-0.0276^{b}	Breached
	Q3	-0.0491^{a}	-0.0222^{c}	Breached
	Q4	-0.042^{b}	-0.0105	Breached

^{a} 1 % level
^{b} 5 % level
^{c} 10 % level
N/S: not significant

The overall results from the differences in performance between two groups show the mixed results. We found that the differences in profit ratios, ROA, OI/A, and OI/S of the treatment sample are lower in one or more quarters. On the other hand, difference in ROS is higher for the treatment sample. For COGS/S and TOE/S, these cost ratios for the both sample groups decreased subsequent to the breach compared to those before the breach based on the results of differences within firms (see Tables 5 and 6 for the treatment sample and Tables A-3 and A-4 for the control sample). When we compared the differences of COGS/S between two sample groups, the ratio of control sample has decreased more compared to that of treatment sample in one or more quarters. When we compared the differences of TOE/S between two sample groups, the ratio of treatment sample has decreased more in general except one quarter in the Table 10.

As shown in the both Tables 9 and 10, the treatment sample was selected as higher performance group for 12 out of 17 in the Table 9 and for 9 out of 16 in the Table 10. Thus, our results indicated that the treatment sample outperformed the control firms for the most of performance measures.

So in summary, with regards to our second set of hypotheses, our analysis leads us to the conclusion that:

H2A: partially supported.

H2B: not supported.

H2C: partially supported.

H2D: partially supported.

H2E: partially supported.

H2F: partially supported.

CONCLUSION AND DISCUSSION

The information security breach incidents have grown significantly over the past few years (Egan & Mather, 2005). Despite numerous news and surveys reporting the enormous financial losses from the incidents, the results of our study did not demonstrate that there is a significant impact of publicly announced security breach incidents on the organizational performance.

Whether a firm experienced a temporary interruption of business operations or incurred financial loss from repairing or replacing the system, the overall performance of our breached firms did not decrease as a result of the breach in our study. So what is the implication of these results that appear to go against what would be our initial expectations?

While stock market investors tend to unload the breached firm's stock after a breach possibly because they believe that the breached firm has been damaged, it appears that any such damage was at most temporary and that the breached firms were able to recover and perform even better than before. One possible explanation is that the breached firm may be able to address any weaknesses in information security in a timely manner, which prevented from any damage to organizational reputation or marginal negative impact on the organization. Another one is that the breached firm may be investing resources to improve further. As a result, the organization became more disciplined, efficient, and effective after the breach. This might explain why the breached firms outperformed the control firms as well.

The evaluation of our first set of hypotheses (i.e. H1A-H1F) suggests that in general the performance of the breached firms was not worse after the breach than before the breach, and for some measures, the corresponding performance was even better. The evaluation of our second set of hypothesis (H2A-H2F) supports the belief that in general the breached firm took efforts to improve its post-breach performance so that it could be competitive with respect to the other firms, and in doing this in some cases they were able to outperform the control firms. These results also suggest the stock investors' assessment that there is severe damage to a firm when its security is breached could be an over-reaction. However, our results could also lead to the conclusion that given this reaction by the investor, the breached firm also overreacts by improving its performance in order to regain the confidence of investors, and so the net effect of the breach is improved firm performance.

Our results have important implications for top managers and stock market investors. Although the market value of the breached firm might drop temporarily as indicated in the previous event studies, it does not impact on its financial performance over the longer periods of time, at least, over four quarters as shown in our study. For top managers, any known vulnerabilities to security must be managed to prevent from any further attack. This ensures regaining the confidence of overly concerned investors.

Our study is not without limitation. We believe that the majority of breached firms included in our sample might be large firms since they are publicly known firms and they might not represent the overall breached firms in general, a fact which limits the generalizability of our results. Thus, further research might be needed to explore whether size, industry of the firm or types of the breach have a material impact on the overall financial performance.

APPENDIX

Steps to construct Tables 9 and 10: First, we performed another analysis for the differences in performance within the control sample and presented the results in the Tables A-3 and A-4. Second, for all those variables that were significant in the Tables 5, 6, A-3, and A-4, median values for these variables for both groups are selected from Tables A-1 and A-2 and included in the applicable quarters in the Tables 9 and 10. Then the magnitude of median value is compared between two groups and determined which sample group performed better. For those variables that were identified as insignificant, the sample group that has significant differences was selected as the higher performance group.

Table A-1 Average Performance Values by Quarter and Sample (Two Digit)

Item		Quarter 1			Quarter 2		
		Mean	Median	S.D.	Mean	Median	S.D.
Difference in ROA	Control	0.0038	-0.0001	0.0266	0.0071	0.0006	0.0331
	Breached	0.0006	0.0004	0.0530	0.0420	0.0005	0.2302
Difference in ROS	Control	0.0186	-0.0050	0.1861	0.1032	0.0004	0.7242
	Breached	-0.3558	-0.0141	2.1032	-1.0756	-0.0199	4.7901
Difference in OI/A	Control	-0.0122	-0.0020	0.0436	-0.0128	0.0006	0.0590
	Breached	0.0072	0.0010	0.0394	0.0048	0.0033	0.0435
Difference in OI/S	Control	-0.5128	-0.0277	0.1901	-0.0505	-0.0123	0.2395
	Breached	-0.2765	-0.0146	2.0485	-0.6126	-0.0036	3.9463
Difference in COGS/S	Control	0.0047	0.0064	0.0793	0.0318	0.0163	0.1205
	Breached	0.2656	0.0134	2.0441	0.5396	0.0180	3.8454
Difference in TOE/S	Control	-0.0237	-0.0068	0.1123	0.0178	0.0123	0.1477
	Breached	0.2937	0.0176	2.0452	0.6997	0.0395	3.9407

Item		Quarter 3			Quarter 4		
		Mean	Median	S.D.	Mean	Median	S.D.
Difference in ROA	Control	0.0047	-0.0001	0.0262	0.0074	0.0005	0.0458
	Breached	-0.0047	0.0002	0.0422	0.0108	0.0005	0.3112
Difference in ROS	Control	0.0371	-0.0023	0.2004	0.0424	-0.0041	0.2962
	Breached	-0.4962	-0.0306	2.6529	-0.1021	-0.0097	3.7553
Difference in OI/A	Control	-0.0115	-0.0016	0.0408	-0.0017	0.0008	0.0531
	Breached	-0.0032	0.0007	0.4616	-0.0064	0.0001	0.5237
Difference in OI/S	Control	-0.0402	-0.0192	0.2490	-0.0074	-0.0341	0.2388
	Breached	-0.4396	-0.0295	2.7796	-0.3179	-0.0358	1.7927
Difference in COGS/S	Control	0.0001	0.0010	0.1446	0.0146	0.0004	0.1589
	Breached	0.4369	0.0249	2.7766	0.2820	0.0112	1.7864
Difference in TOE/S	Control	-0.0191	-0.0037	0.1521	0.0037	0.0001	0.1842
	Breached	0.4820	0.0298	2.7799	0.3147	0.0358	1.7929

Table A-2 Average Performance Values by Quarter and Sample (Four Digit)

Item		Quarter 1			Quarter 2		
		Mean	Median	Std.Dev.	Mean	Median	Std.Dev.
Difference in ROA	Control	0.0004	-0.0002	0.0306	-0.0062	-0.0007	0.0321
	Treatment	-0.0014	-0.0004	0.0668	-0.0378	-0.0015	0.2025
Difference in ROS	Control	0.0667	0.0060	0.7063	-0.1691	0.0009	0.8501
	Treatment	0.7306	0.0099	3.2279	1.1416	0.0096	5.0446
Difference in OI/A	Control	-0.0012	-0.0001	0.0189	-0.0030	-0.0006	0.0252
	Treatment	0.0008	0.0003	0.0613	-0.0088	-0.0008	4.8080
Difference in OI/S	Control	0.0067	0.0171	0.2322	0.0223	0.0133	0.3362
	Treatment	0.8121	0.0170	3.4353	0.8706	-0.0008	4.8080
Difference in COGS/S	Control	-0.0436	-0.0200	0.1181	-0.0764	-0.0354	0.2800
	Treatment	-0.4385	-0.0135	2.5600	-0.7659	-0.0341	4.6880
Difference In TOE/S	Control	-0.0066	-0.0171	0.2327	-0.0683	-0.0276	0.3555
	Treatment	-0.8143	-0.0167	3.4347	-0.9805	-0.0482	4.7941

Item		Quarter 3			Quarter 4		
		Mean	Median	Std.Dev.	Mean	Median	Std.Dev.
Difference in ROA	Control	0.0052	0.0009	0.0462	-0.0028	0.0003	0.0888
	Treatment	0.0097	0.0008	0.0470	-0.0067	0.0004	0.3701
Difference in ROS	Control	0.1788	0.0185	0.7447	0.0190	0.0054	0.8954
	Treatment	0.6447	0.0320	3.2183	0.1275	0.0114	4.4185
Difference in OI/A	Control	-0.0024	-0.0007	0.0196	-0.0030	0.0001	0.0234
	Treatment	0.0089	0.0005	0.0516	0.0178	0.0018	0.0808
Difference in OI/S	Control	0.0592	0.0141	0.2688	0.1306	0.0085	0.6612
	Treatment	0.5230	0.0425	3.3214	0.4542	0.0420	2.1414
Difference in COGS/S	Control	-0.0680	-0.0124	0.1998	-0.1455	-0.0087	0.6752
	Treatment	-0.5067	-0.0272	3.3228	-0.2914	-0.0159	1.9625
Difference In TOE/S	Control	-0.0822	-0.0222	0.2860	-0.1488	-0.0105	0.6615
	Treatment	-0.5668	-0.0491	3.3211	-0.4498	-0.0420	2.1420

Table A-3 Differences within Control Sample (Two Digit)

Performance measures	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
	Z	p value	Z	p value	Z	p value	Z	p value
Difference in ROA	-0.714	0.475	-2.232	0.026 [b]	-0.997	0.319	-0.892	0.372
Difference in ROS	0.475	0.635	-0.805	0.421	-0.378	0.705	0.258	0.796
Difference in OI/A	1.659	0.097 [c]	0.503	0.615	1.839	0.066 [c]	0.135	0.893
Difference in OI/ S	2.652	0.008 [b]	1.465	0.143	2.131	0.033 [b]	1.577	0.115
Difference in COGS / S	-1.223	0.221	-2.031	0.042 [b]	-0.602	0.547	-1.291	0.197
Difference in TOE / S	1.121	0.262	-0.613	0.540	0.395	0.693	-0.522	0.602

[a] 1 % level

[b] 5 % level

[c] 10 % level

Table A-4 Differences within Control Sample (Four Digit)

Performance measures	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
	Z	p value	Z	p value	Z	p value	Z	p value
Difference in ROA	-0.619	0.536	-2.014	0.044[b]	1.111	0.267	-0.756	0.450
Difference in ROS	0.000	1.000	-0.831	0.406	1.894	0.058[c]	0.209	0.834
Difference in OI/A	-0.035	0.972	-0.711	0.477	-1.090	-0.276	-0.610	0.542
Difference in OI/ S	1.844	0.065[c]	1.099	0.272	1.344	0.179	0.747	0.455
Difference in COGS / S	-2.322	0.020[b]	-2.681	0.007[a]	-2.254	0.024[b]	-2.004	0.045[b]
Difference in TOE / S	-1.844	0.065[c]	-2.273	0.023[b]	-1.894	0.058[c]	-1.548	0.122

[a] 1 % level

[b] 5 % level

[c] 10 % level

REFERENCES

Andoh-Baidoo, F. K. & Osei-Bryson, K-M. Exploring the characteristics of Internet security breaches that impact the market value of breached firms. Expert Systems with Applications, in press, 2006

Balakrishnan, R., Linsmeier, T. J., & Venkatachalam, M. Financial benefits from JIT adoption: Effects of customer concentration and cost structure. The Accounting Review, 1996, **71**, 2, 183-205

Barber, B. M., & Lyon, J. D. Detecting Abnormal Operating Performance: The Empirical Power and Specification of Test Statistics, Journal of Financial Economics, 1996, **41**, 359-399.

Barney, J. B. Chapter 2: What is performance? In: Gaining and Sustaining Competitive Advantage, Boston, MA: Addison-Wesley, 1997, pp. 30-64.

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

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security, 2003, **11**, 431–448.

Cavusoglu, H., Mishra, B. & Raghunathan, S. 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, Fall, 2004, **9**, 1, 69-104.

Dasgupta, S., Laplante, B. & Mamingi, N. Capital market responses to environmental performance in developing countries, Development Research Group, The World Bank, http://www.worldbank.org/nipr/work_paper/market/MARKETS-htmp2.htm April, 1998.

D'Amico, A. D. What does a computer security breach really cost? Secure Decisions, A Division of Applied Visions, Inc., September 7, 2000.

Egan, M. & Mather, T. The executive guide to information security threats, challenges, and solutions, Addison-Wesley, Indianapolis, 2005.

Featherman, M. S., Valacich, J. S. & Wells, J. D. Is that authentic or artifical? Understanding consumer perceptions of risk in e-service encounters. Information Systems Journal, 2006, **16**, 107-134.

Garg, A., Curtis, J. & Halper, H. The financial impact of IT security breaches: What do investors think? Information Systems Security, 2003a, March/April, 22-33.

Garg, A., Curtis, J. & Halper, H. Quantifying the financial impact of IT security breaches, Information Management & Computer Security. 2003b, **11**, 2/3, 74-83.

Gordon, L., Loeb, M. P., Lucyshyn, W. & Richardson, R. 2004 CSI/FBI Computer crime and security survey, Computer Security Institute, 2004.

Gordon, L., Loeb, M. P., Lucyshyn, W. & Richardson, R 2005 CSI/FBI Computer crime and security survey, Computer Security Institute, 2005.

Grover, V. & Saeed, K. A. Strategic orientation and performance of internet-based businesses, Information Systems Journal, 2004, **14**, 23-42.

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

Hovav, A. & D'Arcy, J. The impact of virus attack announcements on the market value of firms. Information Systems Security, 2004, May/June, 32-40.

Hovav, A. & D'Arcy, J. The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review, 2003, **6,** 2, 97-121.

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

Kros, John R., Foltz, C. B., & Metcalf, C. L. Assessing & quantifying the loss of network intrusion, Winter, Journal of Computer Information Systems, (2004/2005), **45**, 2, 36-43.

Kutner, M.H., Nachtsheim, C.J., Neter, J., & Li, W. Applied linear statistical models. McGraw-Hill 5th ed., 2005.

Mercuri, R. Analyzing security costs. Communication of the ACM, 2003, **46**, 6, 15-18.

Moore, D.S. & McCabe, P. Introduction to the practice of statistics, W.H. Freeman and Company, 4th ed., 2003.

Muncaster, P. IT decision-makers more concerned about security, VNU Network, February 15, http://www.vnunet.com/articles/2150356, 2006.

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

Anonymous. Security attacks on IT systems more than double, according to respondents of Deloitte & Touche's global financial services survey. PR Newswire Association Inc, May 27, 2004, available at http://www.prnewswire.com.

Tsiakis, T. & Stephanides, G. The economic approach of information security. Computers & Security, 2005, **24**, 105-108.

Warren, M. & Hutchinson, W. Cyber attacks against supply chain management systems: A short note. International Journal of Physical Distribution & Logistics Management, 2000, **30**, 7, 710-716.