Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

THE IMPACT OF INFORMATION SECURITY BREACHES ON FINANCIAL PERFORMANCE OF THE BREACHED FIRMS: AN EMPIRICAL INVESTIGATION

MYUNG KO
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT
THE UNIVERSITY OF TEXAS AT SAN ANTONIO
myung.ko@utsa.edu

CARLOS DORANTES
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT
THE UNIVERSITY OF TEXAS AT SAN ANTONIO
carlos.dorantes@utsa.edu

ABSTRACT

This study investigates the impact of information security breaches on firm performance. Unlike previous studies that used an event study methodology, we used a matched-sample comparison analysis to investigate the impact of security breaches on firm performance. To investigate this impact, we considered subsequent four quarters following the security breach and determine if the breached firms' performance decreased compared to that of the peer firms (control group). Although the breached firms' sales and operating income did not decrease in the subsequent quarters following the breach, return on assets decreased in the third quarter. Also, performance of the control firms was higher compared to that of the treatment firms in general. However, the breached firms' sales increased significantly in the fourth quarter compared to those of the control firms.

Keywords: Information security, impact, security breach, performance

INTRODUCTION

As the number of organizations that conduct their businesses electronically grows continuously, information security becomes one of major concerns for top managers. According to a recent survey by Forrester, out of 410 IT decision makers, about 75 percent reported that IT security has become critical to their business planning and over 80 percent reported that they are concerned about financial losses from it [20] . In another survey taken from risk managers of the U.S and European companies, computer risk was ranked as the top concern among European companies and the number two concern among U.S. companies [14].

Information security incidents are also continuously rising. According to the 2005 computer crime and security survey by CSI/FBI, 95 percent of respondents reported that their organization experienced more than 10 Web cite incidents in 2005 compared to only 5 percent of respondents in 2004 [11,12]. The same survey also reported that the average loss per incident from the *unauthorized access to information* has increased to

$300K from 51K and loss from the *theft of proprietary information* has also increased to $356K from $169K since 2004. Thus, a security breach incident could result in tremendous financial losses to organizations [8, 22].

Employing an event study methodology, a few previous studies have investigated the market reaction of information security breaches announced publicly [5, 6, 9, 10, 14, 15]. The event study methodology is based on the assumption that capital markets are efficient to evaluate the impact of the events on expected future cash flows of the firms [7]. Overall, these previous studies found that the market discriminates breached companies in the first few days following the public announcement of the breach. However, no previous studies have investigated the impact of security breaches on long-term financial performance.

This study investigates the impact of information security breaches on the breached companies' financial performance in the subsequent four quarters following the public announcement of the security breach incidents. Our sample includes only one type of security breach, *unauthorized access to confidential data*. Campbell et al [5] found a significant negative market reaction when the breaches are related to *confidential data*. However, the same study indicated that the market did not react differently to other types of security breaches. Considering this result, we only included incidents related to unauthorized access to confidential data in our sample.

In the following section, we discuss security breaches and their impact on performance. We then describe the methodology and the sample selection technique. The next section describes financial performance measures used to determine the impact of the breached organizations. In the subsequent section, we discussed the statistical analysis, followed by details of results, conclusion, and discussion.

SECURITY BREACHES AND IMPACT ON PERFORMANCE

Types of security breaches include virus, unauthorized access, theft of proprietary information, denial of service, sabotage, and Web site defacement, etc. [12]. Although these security incidents are continuously rising and organizations have come to aware the importance of information security, assessing the impact of security breaches is very difficult because costs of security breaches are not ease to quantify [18].

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. All of these previous studies used an event study methodology and their results are summarized in the following.

Campbell et al. [5] investigated the stock market reaction of information security breaches on public firms. The authors concluded that the economic consequence of a security breach depends on the nature of the breach. They found a highly significant negative market reaction when breaches are related to unauthorized access to confidential data. However, the authors did not find any significant market reaction for other types of security breaches.

Garg et al. [9] estimated that security incidents can cost breached companies 0.5 to 1 percent of annual sales on average. The authors also tested for the spillover effects on security vendors and insurance carriers and found that security vendors experienced a share price increase between 1 to 3 percent and insurance carriers experienced 1 to 2 percent increase in a share price as a result of security breach.

Similar to the study by Garg et al. [9], Cavusoglu et al. [6] found that the security breach announcements affect the value of breached firms and also of Internet security developers. On average, the breached firms lost 2.1 percent of their market value within two days following the public announcement. On the other hand, the security developers realized an average abnormal return of 1.36 percent during this period.

Hovav and D'Arcy [14] investigated the impact of denial-of-service (DOS) attacks by examining the stock market reaction. They found no significant impact of DOS attacks on the capital market. However, their results indicated that a significant negative financial impact on "Internet-specific" companies. Hovav and D'Arcy [15] examined the impact of virus attack announcements. The authors found no negative abnormal return over any of 5 days following the event. However, they found almost half of the firms experienced negative abnormal returns 25 days after the announcement.

Based on the review of previous studies, security breach incidents do have significant impact on the breached companies or other related companies. So, what are the costs that should be considered? The costs of security breaches can be classified as short-term costs and long-term costs. Examples of short-term costs include cost of repairs, cost of replacement of the system, lost

business due to the disruption of business operations, and lost productivity of employees. These are also considered tangible costs. On the other hand, long-term costs include the loss of existing customers due to loss of trust, failing to attract potential future customers due to negative reputation from the breach, loss of business partners due to loss of trust, and potential legal liabilities from the breach [6, 21]. Most of these costs are intangible costs that are difficult to calculate but extremely important in assessing the overall security breach costs to the organization [6].

The breached firms incur tangible and intangible costs. Thus, we argue that financial performance of a breached firm decreases compared to its performance before the breach. In addition, financial performance of a breached firm is poor when it is compared to a peer firm that is in the same industry and similar in size and also has not experienced any security breach. Thus, the following hypotheses are proposed.

H1: The security breach incident will result in decreased performance of security breached firm in the long-term.

H2: The financial performance of security breached firms will be significantly lower in the long-term than that of the other firms that have not experienced the security breach.

RESEARCH METHODOLOGY

To evaluate the financial impact of security breaches related to confidential information, the "matched sample comparison group" method is used. This methodology has also been used in other previous studies [1,4,16]. Our sample includes two groups, the treatment and control samples. The treatment sample represents firms that have experienced information security breaches and the control sample represents firms that were selected to match the treatment sample by size and industry.

Sample Selection

To select firms that have security breaches related to confidential data, we obtained data on security breached firms from previous studies [5, 9]. These two studies included detailed information about all security breached firms for the period from 1997 to 2001. From these two sources, we identified 16 cases related to *unauthorized access to confidential data* and only 12 cases are included in our sample due to lack of financial data available from Compustat. To include more current data, we identified additional breached firms for the period from 2002 to 2003 from three sources - Lexis/Nexis, CNET, and ZDNET. The key words "attack," "breach," "break-in," "hacker," "Internet," and "security" were used. This approach was used in Cavusoglu et al. [6]. When breached incidents were limited to confidential data, only 7 cases were left. As a result, the final treatment sample includes 19 cases.

To control for confounding changes in industry and the firm size, we followed some steps to select a matching control firm that is comparable to the treatment sample. Initially, firms from the same primary four-digit SIC code as the treatment firm were pulled from Compustat as a list of potential control firms. From each list, we chose the firm that had reported three different size measures closest to the amounts reported by the corresponding treatment firm. In this study, we used annual total assets, annual sales, and number of employees as the size measures, which are commonly used as proxies for the firm size. To match the size, we allowed the size measures of a potential control firm to be between 70% and 130% of the treatment firm's values. When no comparable firms were available in their four-digit SIC code, we tried to match using three-digit SIC codes, and then two-digit SIC codes. Other previous studies used this method for selecting matching control sample from the same industry and similar in size as the treatment sample [1, 2, 4].

To determine if there were any significant differences between the two different sample groups, a t-test and a non-parametric test were carried out comparing total of assets, number of employees, and annual sales. No significant differences were found between the sample groups. Descriptive statistics about the characteristics of firms in the treatment and control samples and results of tests are shown in Table 1.

Table 1: Descriptive Statistics

Variables	Treatment group			Control group			Tests of mean difference	
							Mann-Whitney Test	T-test [1]
	Mean	Median	Std dev	Mean	Median	Std dev	Z	T
Total assets (billion $)	53.577	10.877	99.014	60.136	7.914	117.882	-0.34	-0.17
Sales (billion $)	9.974	5.705	10.317	8.098	5.730	9.061	-0.36	-0.36
Employees	37,280	23,200	43,150	32,680	20,030	36,420	-0.10	-0.03

[1] T-test was carried out using natural logarithm

FINANCIAL PERFORMANCE MEASURES

We used accounting measures to evaluate the impact of security breach incidents. The use of accounting measures of performance is the most popular approach to measure firm performance [3]. Accounting measures commonly rely on ratio analysis.

We used four profit based ratios (ROA, ROS, OI/A, OI/S, and two cost related ratios (COGS/S and TOE/S) to measure firm performance. In addition, we included percentage of change in sales and operating income to see if these measures are better indicators for identifying differences in performance considering the context of this study. Profit ratios have been the most commonly used as performance measures [4, 13, 16]. Descriptions of the financial performance measures are shown in Table 2.

Table 2: Description of Financial Performance Measures

Variable	Description
S	Sales in the corresponding period
OI	Operating income before depreciation
ROA	Return on assets is net income divided by the total assets
ROS	Return on sales is net income divided by sales
OI/A	Operating income divided by total assets
OI/S	Operating income divided by sales
COGS/S	Cost of goods sold divided by sales
TOE/S	Total operating expenses divided by sales

Quarterly financial performance data were collected from Compustat for both the treatment and the control samples. Performance was considered as two time periods – before the security incident and after the security incident. Therefore, for each treatment sample, the performance measures were collected for four quarters before the incident and four quarters after the incident. For each corresponding control firm, performance measures were collected for applicable quarters included in the treatment firm.

STATISTICAL ANALYSIS

We examined the normality plots to check the underlying distributions of the variables. The data are close to normal with the exception of outliers in all variables. Due to the possible influential effects of these outliers using parametric tests, we conducted non-parametric tests.

To test H1, performance measures in the time period t_{+1} to t_{+4} are matched against performance measures in the corresponding time period t_{-1} to t_{-4} and calculated the relative changes in performance measures over four quarters. This indicates the percentage of change in performance (for sales and operating income) or the difference in performance (for all ratios) of each quarter after the incident when it compared to the performance of the corresponding quarter before the incident for each firm (e.g., % difference in sales in t_{+1} – % difference in sales in t_{-1}). This is referred to as the "within firm differences" in our analysis.

To test "within firm differences," we used the Wilcoxon signed rank test, which is a paired non-parametric test since we are comparing two values for

each firm –before and after the incident. This test is much less sensitive to outliers and it tests whether the average of the differences differs from zero. This test is adequate when comparing before-and-after observations on the same subjects [19].

To test H2, performance measures in the time period t_{+1} to t_{+4} of the treatment firm are matched against performance measures in the corresponding time period t_{-1} to t_{-4} and calculated the relative changes in performance measures of the treatment firms over four quarters. This same procedure is repeated for the control firms. The differences of the treatment and control firms for these relative changes in measures are then calculated by subtracting the performance measures of the control firms from the treatment firms' performance measures. This indicates the percentage of change in performance (for sales and operating income) or difference in performance (for all ratios) between treatment firms and control firms. This is referred to as the "between firm differences" in our analysis. For this analysis, we used an independent Mann-Whitney test since we are comparing mean difference for the two samples – the treatment and control firms [17]. Table 3 describes the calculated average differences in performance as described above.

Table 3: Performance Comparison by Quarter and Group

		Quarter 1			**Quarter 2**		
		Mean	Median	Std dev	Mean	Median	Std dev
% change in sales	Control	12.71	12.47	29.73	12.03	6.10	29.53
	Treatment	7.04	4.99	26.73	9.67	5.81	19.74
% change in OI	Control	110.73	14.63	337.01	64.04	13.0	148.57
	Treatment	44.36	7.81	110.01	152.84	15.52	605.21
Difference in ROA	Control	0.39	0.04	2.45	1.28	0.12	3.16
	Treatment	-0.48	-0.02	2.83	-0.41	-0.05	1.56
Difference in ROS	Control	3.29	0.78	10.74	7.28	4.96	10.67
	Treatment	-0.61	0.68	12.88	2.64	0.78	13.60
Difference in OI/A	Control	0.16	-0.02	2.68	0.40	-0.02	1.86
	Treatment	-0.10	0.00	2.14	0.11	-0.05	1.68
Difference in OI/S	Control	3.44	0.82	10.53	4.29	1.66	6.95
	Treatment	1.86	1.21	10.99	7.28	2.78	16.03
Difference in COGS/S	Control	-3.53	-1.47	7.11	-3.08	-1.72	5.09
	Treatment	-3.90	-1.83	13.94	-4.71	-0.70	16.06
Difference In TOE/S	Control	-3.82	-1.97	11.10	-4.64	-2.12	7.29
	Treatment	-6.50	-1.45	14.10	-8.20	-2.78	16.88
		Quarter 3			**Quarter 4**		
		Mean	Median	Std dev	Mean	Median	Std dev
% change in sales	Control	10.95	9.87	29.93	-0.55	-3.38	19.07
	Treatment	12.64	5.03	32.34	19.39	7.93	42.37
% change in OI	Control	51.16	17.69	114.28	115.19	9.64	344.71
	Treatment	40.72	12.31	84.51	10.07	12.57	53.41
Difference in ROA	Control	2.33	0.23	7.57	-1.42	0.01	7.37
	Treatment	-0.75	-0.39	1.20	-0.25	0.00	0.98
Difference in ROS	Control	14.17	3.03	35.51	-3.31	3.23	29.72
	Treatment	-1.78	-0.15	7.14	-0.47	0.45	5.77
Difference in OI/A	Control	0.26	0.21	1.57	0.31	0.02	2.24
	Treatment	0.61	-0.02	3.67	-0.81	-0.19	2.62
Difference in OI/S	Control	3.59	2.84	5.01	3.02	3.21	11.14
	Treatment	5.77	2.18	15.84	-1.39	0.53	9.60
Difference in COGS/S	Control	-3.14	-3.25	3.28	1.86	-1.68	16.08
	Treatment	-5.28	-1.45	16.66	-2.17	1.35	17.26
Difference In TOE/S	Control	-3.70	-2.84	5.29	2.13	-2.11	18.96
	Treatment	-6.44	-2.48	16.89	-5.69	-1.06	15.71

RESULTS

Within Firm Differences

Table 4 summarized the results of the "within firm differences" analysis. The "within treatment firms' differences" between subsequent quarters following the incident and quarters before the incident were as follows. First, the percentage change in sales (S in table 4) was significant except for the first quarter following the breach. The percentage change in operating income (OI in table 4) was significant in the second and third quarters. The difference in ROA was significant in the third quarter. The difference in operating income to sales (OI/S in table 4) was significant in the second quarter. The difference in total operating expenses to sales (TOE/S in table 4) was significant in the first two quarters. Overall, the treatment firms' performance after the security incidents did not decrease in subsequent quarters following the breach except for ROA. Return on Assets has decreased in the subsequent quarter (quarter 3) compared to the quarter before the incident. In the case of TOE/S, although a sign of Z value is negative, it reflects the increase in performance since it represents either total expenses have decreased or sales have increased. Based on our analysis, H1 cannot be rejected.

Table 4: Within Firm Differences analysis

Results of the Treatment Samples

	Quarter 1		**Quarter 2**		**Quarter 3**		**Quarter 4**	
Item	Z	P value	Z	P value	Z	P value	Z	P value
% change in S	0.93	0.35	1.76	0.08*	2.11	0.04**	2.27	0.02**
% change in OI	1.17	0.24	2.25	0.03**	2.27	0.02**	1.10	0.27
difference in ROA	-0.52	0.60	-1.07	0.29	-2.25	0.03**	-0.51	0.61
difference in ROS	-0.04	0.97	1.42	0.16	-0.73	0.46	0.06	0.96
difference in OI/A	-0.44	0.66	-0.54	0.59	0.21	0.84	-1.16	0.25
difference in OI/ S	0.77	0.44	2.39	0.02**	1.14	0.26	0.03	0.98
difference in COGS / S	-1.05	0.30	-1.24	0.22	-1.07	0.29	0.11	0.91
difference in TOE / S	-1.86	0.06*	-2.33	0.02**	-1.04	0.30	-1.18	0.24

*** 1 % level
** 5% level
* 10% level

Results of the Control Samples

	Quarter 1		**Quarter 2**		**Quarter 3**		**Quarter 4**	
Item	Z	P value	Z	P value	Z	P value	Z	P value
% change in S	1.53	0.13	1.61	0.10	1.61	0.10	0.52	0.60
% change in OI	2.13	0.03**	2.29	0.02**	2.20	0.03**	-0.85	0.40
difference in ROA	0.64	0.52	1.93	0.05**	1.17	0.24	-0.32	0.75
difference in ROS	1.45	0.15	3.14	0.00***	2.13	0.03**	-1.49	0.14
difference in OI/A	0.04	0.97	0.44	0.66	1.02	0.31	-0.50	0.62
difference in OI/ S	2.05	0.04**	2.74	0.01***	2.85	0.00***	-1.02	0.31
difference in COGS / S	-2.09	0.04**	-2.37	0.02***	-3.03	0.00***	0.81	0.42
difference in TOE / S	-2.01	0.04**	-2.58	0.01***	-2.59	0.01***	0.00	1.00

*** 1 % level
** 5% level
* 10% level

Between Firm Differences

Table 5 summarized the results of the "between firm differences" analysis. The differences of financial performance between the treatment and control firms were as follows. First, in the first quarter, the treatment firms' performance measures were lower for all except for COGS/S compared to the control firms' measures but the differences were not statistically significant. Second, in the second and third quarters, the control firms' ROA was significant and positive, which indicates higher profit margin generated for each dollar in assets. Third, in the third quarter, the control firms' ROS was significant and positive. Fourth, the treatment firms' sales are significant and positive in the fourth quarter.

Table 5: Between Firm Differences Analysis

	Quarter 1		Quarter 2		Quarter 3		Quarter 4	
Item	Z	p value	Z	p value	Z	p value	Z	p value
% change in S	-0.66	0.51	0.12	0.90	-0.08	0.94	2.27	0.02**
% change in OI	-0.69	0.49	0.43	0.67	-0.35	0.73	0.11	0.91
difference in ROA	-0.92	0.36	-2.07	0.04**	-2.08	0.04**	-0.71	0.48
difference in ROS	-0.63	0.53	-1.61	0.11	-2.14	0.03**	-1.06	0.29
difference in OI/A	-0.28	0.78	-0.49	0.62	-0.55	0.58	-0.95	0.34
difference in OI/ S	-0.19	0.85	0.49	0.62	-0.48	0.63	-0.87	0.38
difference in COGS / S	0.60	0.55	0.91	0.36	0.89	0.37	0.54	0.59
Difference in TOE / S	-0.65	0.52	-0.55	0.58	0.33	0.74	-0.56	0.58

** 5% level

To show the magnitude of the differences in performance between treatment and control firms, Table 6 was created. From the results of "the within firm differences" analysis in Table 4, only those variables that had significant differences are included by performance measure and by quarter. Then, median value for each significant performance variables was pulled from Table 3 and compared the magnitude of the difference in median value. The last column identifies the sample group that has the higher positive significant difference in performance.

For those variables that were identified as not significant, the sample group that has significant differences was selected in the last column. For others, we compared the magnitude of the difference in median value and determine which sample group has the higher positive significant difference in performance. As shown in Table 6, 15 out of 19 values indicated that control firms had higher performance. There is one value that shows a significant negative difference (ROA in third quarter).

From this comparison table, some interesting findings are as follows. First, control firms had higher performance in sales for the second and third quarter compared to that of the treatment firms. However, the treatment firms had higher performance in sales in the fourth quarter. Second, control firms had higher performance in operating income for two quarters. Third, control firms had a significant improvement in ROA in the second quarter while treatment firms had a significant decrease in ROA in the third quarter. Fourth, control firms outperformed treatment firms in ROS, OI/S, COG/S, and TOE/S.

Based on the "between firm differences" analysis, we found that while the control firms' performance measures were significantly outperformed in general, the treatment firms' performance was significantly higher in the last quarter. Thus, H2 is partially supported.

Table 6: Comparison of Significant Differences between Control and Treatment Firms

Item	Quarter	Median value (Treatment firms)	Median Value (Control firms)	Higher performance group
% change in S	Q2	5.81 *	6.10 *	Control
	Q3	5.03 **	9.87 *	Control
	Q4	7.93 **	-3.38 (NS)	Treatment
% change in OI	Q1	7.81 (NS)	14.63 **	Control
	Q2	15.52 **	13.30 **	Treatment
	Q3	12.31 *	17.69 **	Control
difference in ROA	Q2	-0.05 (NS)	0.12 **	Control
	Q3	-0.39 **	0.23 (NS)	None
difference in ROS	Q2	0.78 (NS)	4.96 **	Control
	Q3	- 0.15 (NS)	3.03 **	Control
difference in OI/ S	Q1	1.21 (NS)	0.82 **	Control
	Q2	2.78 **	1.66 ***	Treatment
	Q3	2.18 (NS)	2.84 ***	Control
Difference in COGS / S	Q1	-1.83 (NS)	-1.47 **	Control
	Q2	-0.70 (NS)	-1.72 **	Control
	Q3	-1.45 (NS)	-3.25 ***	Control
TOE / S	Q1	-1.45 *	-1.97 **	Control
	Q2	-2.78 **	-2.12 ***	Control
	Q3	-2.84 (NS)	-2.84 ***	Control

***1% level
** 5% level
* 10% level
N/S: not significant

CONCLUSION AND DISCUSSION

The information security breach incidents have grown significantly over the past few years [8]. As a consequence, business organizations can suffer the enormous financial losses and thus, information security becomes a major concern for top managers. However, quantifying actual costs of security breaches is a challenging task. Up to date, there are only a few previous studies that have investigated the impact of the breach employing an event study methodology.

Our study investigated the impact of information security breaches on firm performance of breached firms in the subsequent four quarters following the breach. We compared financial performance of the breached firms with performance of the matching peer firms that have not experienced the breach and determined if the breached firms' performance is decreased compared to the control firms' performance. Although the treatment firms' performance did not decrease in the subsequent quarters following the breach, we found that return on assets has decreased in the third quarter. When we compared the performance between the treatment and control firms, the control firms outperformed the treatment firms in general. However, the treatment firms' sales were significantly higher in the fourth quarter than those of the control firms.

Our research findings are in line with one of competing arguments regarding the economic impact of information security breaches [5]. Our results suggested that information security breaches have minimal long-term economic impact. One possible explanation is that the breached firms respond to the breach incident by making additional security investment to prevent from any future breaches. This can lead to either help reduce the negative reputation of the firm caused by the breach or even have a positive long-term economic impact on the firm. Another explanation is that as the time passes, people forget about what happened earlier and the impact of the breach on financial performance phases out over the long-term.

We believe our study made an important contribution to security research since there are no previous studies that have investigated the impact of information security breaches on financial performance. However, our study has some limitation. Our sample includes only 19 security breaches involving confidential data. Thus, the

small sample size limits the generalizability of the results. Another limitation of our study is that accounting measures might not be the best measure to evaluate the impact of security breaches although they are the most commonly used financial performance measure in the previous studies.

Further research is needed including more current security breach events and different types of events to evaluate the impact of security breach by type. Finally, investigating these firms using a case study approach would offer additional insights about the differences.

REFERENCES

[1] Balakrishnan, R., Linsmeier, T. J. and Venkatachalam, M. "Financial benefits from JIT adoption: effects of customer concentration and cost structure," *The Accounting Review*, Vol. 71, Number 2, 1996, pp. 183-205.

[2] Barber, B. M. and Lyon, J. D. "Detecting abnormal operating performance: the empirical power and specification of test statistics," *Journal of Financial Economics*, Vol. 41, Number 3, 1996, pp. 359-399.

[3] Barney, J. B., *What is performance?*, in Gaining and Sustaining Competitive Advantage, Addison-Wesley, Boston, MA., 1997, pp. 30-64.

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

[5] Campbell, K., Gordon, L., Loeb, M. and Zhou, L. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security*, Vol. 11, Number 2003, pp. 431-448.

[6] Cavusoglu, H., Mishra, B. and 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*, Vol. 9, Number 1, 2004, pp. 69-104.

[7] Dasgupta, S., Laplante, B. and Mamingi, N. "Capital market responses to environmental performance in developing countries", *Development Research Group*, http://www.worldbank.org/nipr/work_paper/market/MARKETS-htmp2.htm, .

[8] Egan, M. and Mathen, T., *The executive guide to information security threats, challenges, and solutions*, Addison-Wesley, Indianapolis, 2005.

[9] Garg, A., Curtis, J. and Halper, H. "The financial impact of IT security breaches: what do investors think?," *Information Systems Security*, Vol. 12, Number 1, 2003, pp. 22-33.

[10] Garg, A., Curtis, J. and Halper, H. "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security*, Vol. 11, Number 2/3, 2003, pp. 74-83.

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

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

[13] Hitt, L. and Brynjolfsson, E. "Productivity, business profitability, and consumer surplus: three different measures of information technology value," *MIS Quarterly*, Vol. 20, Number 2, 1996, pp. 121-142.

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

[15] Hovav, A. and D'Arcy, J. "The impact of virus attack announcements on the market value of firms," *Information Systems Security*, Vol. 12, Number 2, 2004, pp. 32-40.

[16] Hunton, J., Lippincott, B. and Reck, J. L. "Enterprise resource planning systems: comparing firm performance of adopters and nonadopters," *International Journal of Accounting Information Systems*, Vol. 4, Number 3, 2003, pp. 165-184.

[17] Kutner, M. H., Nachtsheim, C. J., Neter, J. and Li, W., *Applied linear statistical models*, McGraw-Hill, New York, NY, 2005.

[18] Mercuri, R. "Analyzing security costs," *Communication of the ACM*, Vol. 46, Number 6, 2003, pp. 15-18.

[19] Moore, D. S. and McCabe, P., *Introduction to the practice of statistics*, W.H. Freeman and Company, New York, N.Y., 2003.

[20] Muncaster, P. "IT Decision-makers more concerned about security", *VNU Network*, http://www.vnunet.com/articles/2150356, Febrary, 2006.

[21] Tsiakis, T. and Stephanides, G. "The economic approach of information security," *Computers & Security*, Vol. 24, Number 2, 2005, pp. 105-108.

[22] Warren, M. and Hutchinson, W. "Cyber attacks against supply chain management systems: a short note," *International Journal of Physical Distribution & Logistics Management*, Vol. 20, Number 7, 2000, pp. 710-716.

AUTHOR BIOGRAPHIES

Carlos A. Dorantes is a doctoral candidate in the Department of Information Systems and Technology Management at the University of Texas at San Antonio. He has a M.S. in Computer Science from the Tecnológico de Monterrey. He has over a decade of experience in enterprise systems implementation in a multi-campus university. His work has appeared in the Data Base for Advances in Information Systems Journal, and IS conferences such as HICSS and AMCIS.

Myung Ko is an Assistant Professor in the Department of Information Systems and Technology Management at the University of Texas at San Antonio. She holds a Ph. D. in information systems from the Virginia Commonwealth University. Her research interests include impact of IT on organizations, data mining, economics of information security, and accounting information systems. Her research has appeared in journals including Information & Management, Information and Software Technology, and Information Systems Journal.