Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Intra-Industry Effects of Information Security Breaches on Firm Performance

Humayun Zafar
The University of Texas at San Antonio, hzafar@kennesaw.edu

Myung Ko
University of Texas at San Antonio, myung.ko@utsa.edu

Kweku-Muata Osei-Bryson
Virginia Commonwealth University, Kweku.Muata@isy.vcu.edu

Intra-Industry Effects of Information Security Breaches on Firm Performance

Humayun Zafar
Department of Information Systems and Technology Management
The University of Texas at San Antonio
San Antonio, TX 78249
Humayun.Zafar@utsa.edu

Myung Ko
Department of Information Systems and Technology Management
The University of Texas at San Antonio
San Antonio, TX 78249
Myung.Ko@utsa.edu

Kweku-Muata Osei-Bryson
Department of Information Systems and the Information Systems Research Institute
Virginia Commonwealth University
Richmond, VA 23284
Kweku.Muata@isy.vcu.edu

ABSTRACT

Instances of information security breaches are wide ranging, and can affect companies of different industries and sizes. We investigate the impact of publicly announced information security breaches of public organizations on their competitors that are comparable in size and operate in the same industry. This is called intra-industry information transfer, and has not been subject to extensive research in IS. We use matched-sampling methodology to measure the difference in firm performance using financial ratios, and interpret the results using paired samples t and Wilcoxon matched pair tests. Our results present a departure from intuition regarding the efficacy of security breaches on firm performance even though we do find an instance of information transfer.

Keywords

Impact, information security, breach, firm performance, information transfer.

INTRODUCTION

In 2008 total economic losses due to data theft and information security breaches were approximated to be $1 trillion. No business was immune. Kaspersky, a leading provider of security software, and the Federal Aviation Administration were one of many victims of a cyber crime (Null, 2009). Ponemon Institute in their 2007 annual study on the costs of a data breach reported that total average costs of a data breach per company ranged from $225,000 to almost $35 million (Ponemon, 2007). The report also stated that the cost of lost business increased to 65 percent of data breach costs, up from 54 percent the year before, and that breaches by third party organizations were more costly than breaches by the enterprise itself. Although computer security can have a great impact on organizations, IS research in this area is still in its infancy.

In this study we investigate the financial impact of publicly announced security breaches of firms on their competitors in the same industry. This phenomenon is referred to as intra-industry information transfer, and has been subject to minimal research in IS, though it has been investigated at length in accounting, economics, and finance. Past research regarding this phenomenon has shown disparate results, thus, highlighting the need for further research in this topic, especially IS. In the following sections we provide a brief review of existing research in IS security, a description of intra-industry information transfer, a description of the firm performance indicators, data analysis, and conclusion.

INFORMATION SECURITY BREACH

Prior research on computer security has concentrated mostly on either identifying security as a socio-philosophical concern (Ratnasingham, 1998), a socio-organizational concern (Dhillon and Backhouse, 2001), or as a purely technical issue (Bass, 2000). Such delineation has possibly led to a situation where security is widely regarded as a field which lacks comprehensive research in IS (Kotulic and Clark, 2004).

Past studies that consider security breach models at the firm level relate to areas such as governance (Straub and Nance, 1990), information privacy (Greenaway and Chan, 2005), development of best practice security models (Ma and Pearson, 2005), maintaining data integrity (Ba et al., 2005), preventing unauthorized user access (Zviran and Haga, 1999), developing secure applications (Tryfonas, 2007), encouraging information security in the workplace (Whitworth and Zaic, 2003), and economics of information security (Gal-Or and Ghose, 2005).

With regard to the financial impact, most studies have investigated market reaction of information security breaches over a short period from the announcement using an event study methodology. Cavusoglu et al. (2004) found that the breached firms lost on average 2.1 percent of their market value within two days of the announcement. Campbell et al. (2003) found a significant negative market reaction regarding security breaches which involved unauthorized access to confidential data, whereas, not much of a reaction was noticed if the breach did not involve confidential data. Acquisto et al. (2006) investigated information privacy breaches, and concluded that there was a significant negative impact on a firm's market value on the day of the information security breach announcement. However this effect decreased over the day following the incident announcement. Some studies have shown that there was no significant impact of security breaches on firms. Hovav and D'Arcy (2004) investigated the impact of virus attack announcement on market reaction. They concluded that there was no significant impact on the firm's market value during the 25 days following the announcement. Some studies have used matched-sampling methodology and explored this issue (Ko et al., 2009). They conclude that the direction of the impact is dependent on the type of security breaches, and the impact of IT intensive firms is different from non-IT intensive firms.

Intra-Industry Information Transfer

An intra-industry information transfer is said to exist when information released by one firm affects the performance of other non-announcing firms in the same industry. This is because such information can have important implications for the future profitability of other non-announcing firms operating in the industry. For example, research has shown that earnings information disclosed by one firm in an industry conveys information about other firms in the same industry (e.g. Foster, 1981). However, depending on the nature of the information, signs of the differences in performance of the announcing firms and non-announcing firms in the industry need not be the same (Szewczyk, 1992). Accordingly, intra-industry information transfer consists of two types: contagion and competition effects. Contagion effects occur when non-announcing firms' stock price reactions tend to be in the same direction (positive or negative) as the announcing firm's price reaction and usually arise from industry commonalities. Competition effects occur as the result of shifts in the industry's competitive balance and tend to be in the opposite direction (Kim et al, 2008). Evidence about these information transfers improves our understanding of the sophistication, and economics of markets related to information security incidents. This phenomenon has also been researched for other news releases including sales announcements, management forecasts, mergers, industrial accidents, and regulatory actions. However, results regarding intra-information transfer have been mixed. Some studies have concluded that there is a presence of an intra-industry information transfer effects (Baginski, 1987; Dietrich, 1989), where as some have provided evidence which raised questions regarding the ambiguity which exists with regard to information transfer effects (Hertzel, 1991). This is due to the nature of information transfer, and how it attempts to investigate events which are well researched in variety of areas such as accounting (Kim et al., 2004), economics (Szewczyk, 1992), and finance (Eckbo, 1983).

Information transfer has not thoroughly researched in the IS security realm. Ettredge and Richardson (2003) presented an event study which looked at stock market reaction to denial of service attacks on six Internet firms. They assumed that if a firm announced lower-than-expected earnings, then the firm was more likely to experience negative abnormal returns. They concluded that there were negative mean abnormal returns (information transfer) in industries in which some firms were attacked. They also found that information transfer occurred across industry lines, that is, negative abnormal returns occurred in industries in which no firms were attacked. Another important conclusion was that firm size appeared to have played a role in information transfer. However, the authors found that one industry where firms provide Internet security products and services experienced positive mean abnormal returns, which indicated that investors expected these firms to benefit from future hacker attacks.

Presently, to the best of our knowledge no research has been carried out which investigates intra-industry information transfer to explain the impact of security breaches on firm performance. Herein is the main contribution of our work. Firm performance is measured through several financial ratios which are then analyzed through paired samples t and Wilcoxon matched pair tests to answer the following research question: "Do information security breaches result in intra-industry information transfer effects, and if so which type?"

FIRM PERFORMANCE INDICATORS

Previous studies have commonly used financial ratios as measures indicating firm performance (e.g. Nicolaou, 2004; Bharadwaj, 2000). In this study, we used five profit ratios; return on assets (ROA), return on sales (ROS), operating income to assets (OI/A), operating income to sales (OI/S), and operating income to employee (OI/E) to measure firms performance. We also used two cost ratios; cost of goods sold to sales (COGS/S), and selling and general administration expenses to sales (SGA/S). ROA provides a snapshot of how efficient management is at using its assets to generate earnings. ROS evaluates an organization's operational efficiency. OI/A, OI/S, and OI/E consider returns on the income from operations only. COGS/S and SGA/S measure the percentage of sales used to pay for the operating costs. We believe that the use of these seven ratios provides a more holistic view of an organization's used financial ratios as measures indicating firm performance. Also, due to the lack of empirical research in measuring firm performance after a breach incident, it is possible that not all impacts are captured by all performance ratios. The ratios and their formulas are shown in Table 1.

Profit Ratio Formulas	
ROA	Net Income / Total Assets
ROS	Net Income / Net Sales
OI/A	Operating Income before Depreciation / Total Assets
OI/S	Operating Income before Depreciation / Net Sales
OI/E	Operating Income before Depreciation / Employee
Cost Ratio Formulas	
COGS/S	Cost of Goods Sold / Net Sales
SGA/S	Selling and General Administration Expenses / Net Sales

Table 1: Firm Performance Ratios

RESEARCH METHOD AND DATA COLLECTION

Using the Lexis/Nexis Academic database, we selected publicly traded firms from different industries (e.g. airlines, financial, entertainment etc.), which publicly announced that an information security breach occurred during 1997 to 2004. The keywords used to search the data were "attack", "breach", "break-in", "hacker", "Internet", "security", "virus", "computer", and "information". This approach is similar to methods used by previous studies (Cavusoglu et al., 2004; Andoh-Baidoo and Osei-Brysom, 2006). Once duplicated announcements and non-public firms were eliminated, firms with missing values from Compustat were removed from the sample and the final breached firm sample reduced to 79. After that, for each breached firm, we retrieved information of all of its competitor firms (control firms) in the same industry using Hoover's Handbook of American Businesses (Biesada, 2008). The initial data set for non-announcing competitor firms had a total of 1809 records. Then we only selected competitors whose financial information was available in Compustat. We also ensured that a competitor's size was comparable to a breached firm. To match the firm size, we selected competitor firms that were within 70-130% of a breached firm's total assets (TOA). This is an established and frequently used approach in finance and accounting (Barber and Lyon, 1996). The final data set was reduced to 68 breached firms and a total of 247 competitors once the mentioned TOA criterion was applied to the competitors. The reason we saw a drop in the number of breached firms was that there were no corresponding competitors for those firms that were matched by size, and therefore had to be removed from the dataset. Also, an observation was removed in the analysis if a missing value existed in either firm, whether it was breached or a competitor firm. In our data set there were only four such instances.

To compute the performance ratios, we collected annual financial data for the year before and after the breach for each breached firm and its industry competitors, as well as the industry average for the year of the breach. The change in industry average performance ($\Delta IndustryAveragePerformance_t$) is the difference between an industry's pre-incident (*year t – 1*) performance and post incident (*year t + 1*) performance. Therefore for each performance ratio,

$$\Delta IndustryAveragePerformance_t = IndustryAveragePerformance_{t+1} - IndustryAveragePerformance_{t-1}$$

where *t* is a year of the security breach.

Since each breached firm had multiple competitors, for each set of competitors, we computed the average performance for each performance ratio. This resulted in each breached firm performance ratio being compared to a single performance ratio representing all competitor firms in the same industry. Though it may be argued that annual returns of each competitor firm may vary in terms of profit and loss, similar to Szewczyk (1992), we contend that overall the industry average will exhibit a consistent direction.

We then computed the difference between the actual and expected performance of each breached and competitor firm. The actual performance of a breached firm is its reported financial performance a year after the breach. The expected performance of a breached firm is calculated financial performance a year after the breach in the absence of an incident. It is computed by adding the financial performance of the breached firm a year before the breach to the change in industry average performance for the year of the breach. Therefore for each performance ratio,

$$ExpectedPerformance_{t+1} = ActualPerformance_{t-1} + \Delta IndustryAveragePerformance_{t}$$

Hence there is no change in performance of the firm if actual and expected performance ratios are equivalent. The difference in financial performance is calculated as the difference between the actual post-incident performance and the expected post-incident performance. Therefore, for each performance ratio,

$$Difference = Actual\,Performance_{t+1} - Expected\,Performance_{t+1}$$

For each pair of breached and competitor firms, we computed the difference in financial performance. The results are presented in the next section.

STATISTICAL ANALYSIS AND RESULTS

Table 2 provides descriptive statistics of the total assets (both in millions of dollars) for the breached and competitor firms for the year before the breach. We can see that the mean of both the breached and competitor firms is fairly close to each other. .

Variable	Mean	Median	Minimum	Maximum
Breached Firms' Total assets	13,579.85	3,961.50	0.36	16,2558.00
Competitor Firms' Total assets	14,939.35	4,079.83	0.54	20,1571.92

Table 2: Descriptive Statistics of Breached and Competitor Firms

To gauge the significance of the differences in differences between the breached and competitor firms, we used paired-sample t and Wilcoxon matched pair tests. A paired-sample t-test compares the means of the differences in the ratios of breached firms to those of competitor firms. The null hypothesis is that there is no significant difference between the means of the two difference ratios. We check for significance at the 95% confidence interval. An assumption of this test is that both the difference ratios are normally distributed. Based on the results of the Shapiro-Wilk's normality test we found that that was not the case. Therefore, we also used the non-parametric Wilcoxon matched-pairs test. Similar to the t-test the Wilcoxon test involves comparisons of differences between two measurements without making assumptions about normality. However, this can only be the case if the sample size is greater than 30, otherwise the distribution should be normal if the Wilcoxon method is used. Since our sample size is greater than 30, Wilcoxon is an appropriate method.

Table 3 shows the results of t and z-tests. If the value of the profit ratios is positive and significant then it means that the difference in performance of a breached firm is greater than that of the competitor firm. In the case of the cost ratio, the opposite is true.

Ratio	Difference in Performance	Mean	Median	Paired t-test (2-tailed)		Wilcoxon (2-tailed)	
				T	Signif.	Z	Signif.
ROA	Difference in Breached firm's Performance	0.20	0.07	0.87	0.39	0.64	0.52
	Difference in Competitor firm's Performance	0.22	0.04				
ROS	Difference in Breached firm's Performance	2.63	0.02	1.49	0.14	1.86	0.06
	Difference in Competitor firm's Performance	-2.24	0.01				
OI/A	Difference in Breached firm's Performance	0.14	0.02	2.12	0.04	1.79	0.07
	Difference in Competitor firm's Performance	0.12	0.01				
OI/S	Difference in Breached firm's Performance	3.70	0.03	1.71	0.09	2.08	0.04
	Difference in Competitor firm's Performance	-1.56	0.00				
OI/E	Difference in Breached firm's Performance	96.52[a]	2,755.32[a]	3.74	0.00	4.94	0.00
	Difference in Competitor firm's Performance	-44,1521.00[a]	-78,821.00[a]				
COGS/S	Difference in Breached firm's Performance	0.09	0.04	0.76	0.45	-0.28	0.78
	Difference in Competitor firm's Performance	0.06	0.04				
SGA/S	Difference in Breached firm's Performance	-3.04	0.00	-1.48	0.15	-2.67	0.01
	Difference in Competitor firm's Performance	1.31	0.00				

Table 3: t- and Z-test Results at 95% Confidence Interval a: in thousands

Table 3 provides us results which check if the difference in differences ratios a significant or not. If they are significant at the 0.05 level, then in order to show if there was any information transfer, we need to compare the means of the actual and expected performances for both the breached and competitor firms (shown in Table A in the Appendix). Since the public announcement of a security breach represents negative publicity, we would expect a decrease in actual performance of the breached firm than the expected performance. If the mean of the actual performance is less than the expected performance for the competitor firms then we can predict that there was a positive information transfer (contagion effect). However, if the actual performance is greater than expected performance for the competitor firms, it shows negative information transfer (competition effect). Table 4 provides a description of how the results can be interpreted to gauge for the two types of intra-industry information transfer effects.

Breached Firms	Competitor Firms	Information Transfer?
Actual Performance$_{t+1}$ < Expected Performance$_{t+1}$	Actual Performance$_{t+1}$ < Expected Performance$_{t+1}$	Yes. Contagion effect
Actual Performance$_{t+1}$ < Expected Performance$_{t+1}$	Actual Performance$_{t+1}$ > Expected Performance$_{t+1}$	Yes. Competition effect
Actual Performance$_{t+1}$ > Expected Performance$_{t+1}$	Actual Performance$_{t+1}$ > Expected Performance$_{t+1}$	No effect
Actual Performance$_{t+1}$ > Expected Performance$_{t+1}$	Actual Performance$_{t+1}$ < Expected Performance$_{t+1}$	No effect

Table 4: Information Transfer Decision Chart

For the difference in the breached and competitor firms' ROA we did not achieve significant results. The difference in differences of the breached and competitor firms' ROS was close to being significant according to the Wilcoxon test. However, similar to the case of ROA, we did not notice any information transfer after looking at the post-incident actual and expected performance values.

In the case of OI/A the t-test gave us significant results, where as the Wilcoxon test did not. The actual performance for breached and competitor firms had means of 0.09 and 0.13. The expected performance for both was -0.12, and -0.09 respectively. Based on Table 4 we do not witness any information transfer and the close proximity of both firms' expected and actual means may provide a different result if data is gathered for a larger number of firms.

According to the Wilcoxon test we had a significant result for OI/S. The breached firm' actual and expected means were 0.08 and 2.52 respectively. For competitor firms they were -2.65 and 1.09 respectively. This is an interesting result since the breached and competitor firms performed worse than expected. Therefore, based on Table 4 both exhibited a contagion effect. An interesting pattern was seen in the case of OI/E which was significant in both tests. The mean of the actual performance for both firms was 120532.51 and 78040.49 respectively. Breached firms had an expected performance of

109760.14 compared to the competitors, which had a mean of 519562.25. Even though in this case there was no information transfer, a firm which publicly announced a security breach performed far better than a non-announcing firm. This can provide insights as to how people may perceive breached firms as being more open about security breaches. It is also plausible that breached firm performance improved due to publicity albeit over a security breach.

For the COGS/S ratio, we did not achieve a significant result. However in this case it was intriguing to note that the actual costs of breached (0.61) and competitor (0.60) firms was higher than their expected costs figures – 0.42 and 0.54 respectively. Thus, performance of the breached firms is slightly worse than that of the competitors although it was not significant.

Wilcoxon result was significant for SGA/S. For breached and competitor firms the actual performance means were 0.30 and 3.04 respectively, whereas the expected performance means were 3.27 and 1.72. Here we see that even though there was no information transfer the breached firms incurred less costs than the competitor firms. This may reflect the breached firm in being better equipped in not only dealing with security breaches, but also streamlining its performance after the incident.

We also considered the impact of possible outliers in our dataset. Figure 1 indicates the presence of outliers in the northeast and northwest of center. It also shows that performance differences for a majority of breached and competitor firms is fairly close.

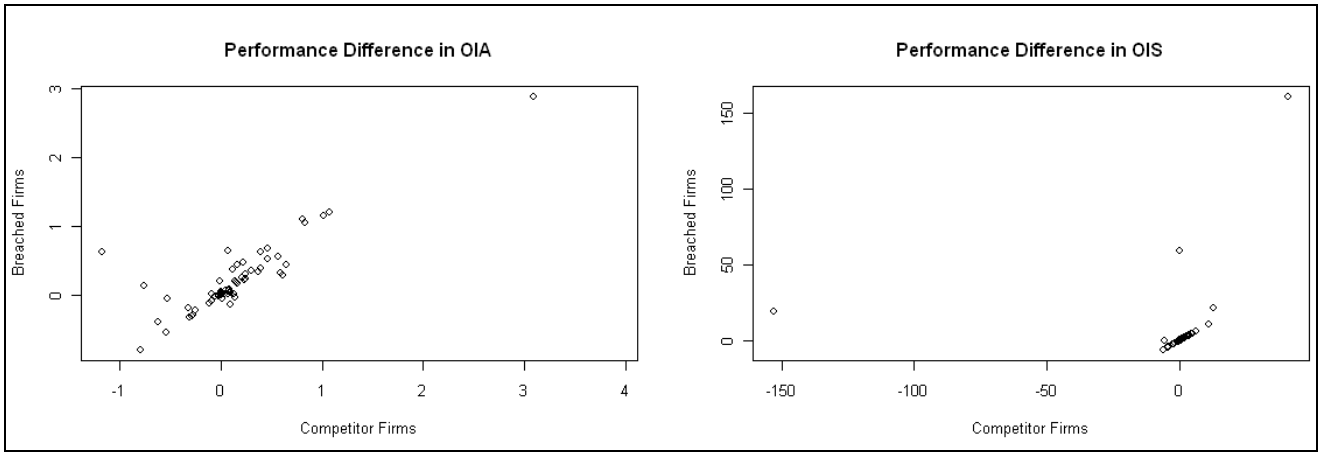

Figure 1: Performance Difference in OIA and OIS

Once two extreme outliers were removed, z statistics show that only two performance indicators (OIE and SGA/S) displayed significance (0.00 and 0.02 respectively) compared to the five in Table 3, with no change in the absence of information transfer. This indicates that only a few breached firms performed extremely better and these firms' performance overshadowed the other firms' performance. In other words, performance for the rest of other firms is very close to each other whether the firm is breached or competitor.

Based on our overall results it is difficult to ascertain the presence of information transfer effects. The general absence of negative information transfer seems to imply that information security breach incidents do not have a long term impact on firm performance. We believe the results of this study are very valuable to managers. Although some previous studies found a short term impact from the security breach, the impact might not last a year, at least in our study comparing to its competitors.

Considering the general public at large is inundated with news and events which cover instances of various types of information security breaches, it is possible that the public then becomes accustomed to such events. This would provide an interesting avenue for future research, since it would consider situations when information security breaches impact an individual level and when they do not. More possible reasons for our results along with the limitations of the study are explained in the next section.

LIMITATIONS AND CONCLUSION

As instances of security breach incidents grow, organizations continue to suffer from losses such as lost business and negative effect on reputation. Considering the actual dollars lost in these cases, it is essential to gather empirical evidence to

quantify losses incurred by organizations due to security breaches. We presented a technique to analyze possible intra-industry information transfer effects. Though we were unable to detect contagion or competition effects for all but one performance indicator, we do suggest that future research to further investigate this phenomenon.

Our study does have certain limitations. We only considered publicly traded firms which reduced the sample size of breached firms. This was necessitated by the inability to gather financial performance data for private firms. Some may also argue that events other than information security breaches may be responsible for the change in performance. However, since we are considering the industry average to compute the expected performance, as a whole it is unlikely that other events have a similar effect on the entire industry.

It may also be more prudent to consider quarterly financial performance data and not annual. Some information security breach incidents may have a short term effect on an organization's performance and may capture the impact better. It may also be the case that in order to check for information transfer, we should only consider pure play firms, that is, firms which only have an Internet presence. In that case, information security breach incidents may have a direct impact on them because their business operations are intricately dependent on technology. Also for future studies, we recommend looking at information transfer by industry type. The idea of grouping can also be applied to different types of security breaches (e.g. Denial of Service), and how the nature of those attacks may result in information transfer.

In the end our sample size may impact gauging intra-industry information transfer effects. Though we agree that the sample size is not as large as it can be, lack of available public data makes it difficult to have a truly large sample size. However, once again since we are looking at industry wide data, to some extent the problem of a small sample size may have been reduced.

We believe that our study further develops the research stream of IS security research which uses the matched-sampling methodology along with empirical support. By integrating a theory from accounting and economics (intra-industry information transfer) we have provided a more holistic way of gauging financial impacts of information security breaches on the breached firms and their competitors.

REFERENCES

1. Acquisto, A., Friedman, A. and Telang, R. (2006) Is There a Cost to Privacy Breaches? An Event Study, *Twenty-Seventh International Conference on Information Systems*, 1563-1580.
2. Andoh-Baidoo, F. K. and Osei-Bryson, K-M. (2007) Exploring the Characteristics of Internet Security Breaches that Impact the Market Value of Breached Firms, *Expert Systems with Applications*, 32, 3, 703-725.
3. Ba, S. et al. (2005) Choice of Transaction Channels: The Effects of Product Characteristics on Market Evolution, *Journal of Management Information Systems*, 21, 4, 173-197.
4. Baginski, S. (1987) Intra-Industry Information Transfer Associated with Management Forecasts of Earnings, *Journal of Accounting Research*, 25, 2, 196-216.
5. Barber, B. M. and Lyon, J. D. (1996) Detecting Abnormal Operating Performance: The Empirical Power and Specification of Test Statistics, *Journal of Financial Economics*, 41, 3, 359-399.
6. Bass, T. (2000) Intrusion Detection Systems and Multisensor Data Fusion, *Communications of the ACM*, 43, 2, 99-105.
7. Bharadwaj, A. S. (2000) A Resource-Based Perspective in Information Technology Capability and Firm Performance: An Empirical Investigation, *MIS Quarterly*, 24, 1, 169-196.
8. Biesada, A. (2008) Hoover's Handbook of American Business 2008, Hoovers Inc.
9. Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Society*, 11, 431-448.
10. Cavusoglu, H., Mishra, B. and 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.
11. Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*, 11, 2, 127-153.
12. Dietrich, J. R. (1989) Discussion of Voluntary Disclosure Choice and Earnings Information Transfer, *Journal of Accounting Research,* 27, 106-110.

13. Eckbo, B. E. (1983) Horizontal mergers, collusion, and stockholder wealth, *Journal of Financial Economics*, 11, 241-273.
14. Ettredge, M. and Richardson, V. J. (2003) Information Transfer Among Internet Firms: The Case of Hacker Attacks, *Journal of Information Systems*, 17, 2, 71-82.
15. Foster, G. (1981) Intra-Industry Information Transfers Associated with Earnings Releases, *Journal of Accounting and Economics*, 3, 201-232.
16. Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information, *Information Systems Research*, 16, 2, 186-208.
17. Garg, A. Curtis, J. and Halper, H. (2003) The Financial Impact of IT Security Breaches: What do Investors Think?, *Information Systems Security*, 22-33.
18. Gordon, L. A. and Loeb, M. P (2001) A framework for using information security as a response to competitor analysis systems, *Communications of the ACM*, 44, 9, 70-75.
19. Greenaway, K. E. and Chan, Y. E. (2005) Theoretical Explanations for Firms' Information Privacy Behaviors, *Journal of the Association for Information Systems*, 6, 6, 171-198.
20. Hertzel, M. (1991) The Effects of Stock Repurchases on Rival Firms, *Journal of Finance*, 46, 2, 707-716.
21. Hovav, A. and D'Arcy, J. (2004) The Impact of Virus Attack Announcements on the Market Value of Firms, *Information Systems Security*, 13, 3, 32-40.
22. Kim, Y., Lacina, M. and Park, M. S. (2008) Positive and Negative Information Transfers from Management Forecasts, *Journal of Accounting Research*, 46, 4, 885-908.
23. Ko, M., Osei-Bryson, M. and Dorantes, C. (2009) Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms, *Information Resources Management Journal*, 22, 2, 1-21.
24. Kotulic, A. G. and Clark, J. G. (2004) Why There Aren't More Information Security Research Studies, *Information & Management*, 41, 597-607.
25. Ma, Q. and Pearson, J. M. (2005) ISO 17799: "Best Practices" in Information Security Management?, *Communications of the Association for Information Systems*, 15, 577-591.
26. Nicolaou, A. L. (2004) Firm Performance Effects in Relation to the Implementation and Use of Enterprise Resource Planning Systems, *Journal of Information Systems*, 18, 2, 79-105.
27. Null, C. (2009) Hackers Running Wild? Data Theft Hits $1 Trillion in 2008, Yahoo! Tech, http://tech.yahoo.com/blogs/null/120939 (Current: February 10, 2009).
28. Ponemon Institute (2007) 2007 Annual Study: U.S. Cost of a Data Breach, *Ponemon Institute*. http://download.pgp.com/pdfs/Ponemon_COB-2007_US_071127_F.pdf (Current: February 01, 2009)
29. Ratnasingham, P. (1998) Trust in Web-Based Electronic Commerce Security, *Information Management and Computer* Security, 6, 4, 162-166.
30. Straub, D. W. and Nance, W. (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly*, 14, 1, 45-60.
31. Szewczyk, S. H. (1992) The Intra-Industry Transfer of Information Inferred from Announcements of Corporate Security Offerings, *Journal of Finance,* 47, 5, 1935-1945.
32. Tryfonas, T. (2007) On Security Metaphors and How They Shape the Emerging Practice of Secure Information Systems Development, *Journal of Information System Security*, 3, 3, 21-50.
33. Whitworth, B. and Zaic, M. (2003) The WOSP Model: Balanced Information System Design and Evaluation, *Communications of the Association for Information Systems*, 12, 258-282.
34. Zviran M. and Haga, W. (1999) Password Security: An Empirical Study, *Journal of Management Information Systems*, 15, 4, 161-185.