The Impact of Virus Attack Announcements on the Market Value of Firms

Anat Hovav[1] and John D'Arcy[1]

[1] Temple University, MIS Department, Fox School of Business and Management, 1810 N. 13th Street, Philadelphia, PA 19122 USA

Abstract. The increase in security breaches in the last few years and the need to insure information assets has created an intensified interest in information security and risk within organizations. However, very little is known of the financial impact and the risk associated with the various types of security breaches. This article reports the impact of virus attack announcements on the market value of affected companies over a period of 15 years. The study was conducted using event study methodology. The results show that in general the market does not penalize companies that experience such an attack.

Keywords: information systems security, security breach, computer virus, event study

1 Introduction

Information Systems (IS) risk is a top concern for organizations [33]. These concerns are due to the fact that the consequence of a security breach can be detrimental to a company's financial performance [13]. Thus, security strategies revolve around the act of a security breach (or an attempt at one) and the need to minimize the financial loss resulting from such a breach. Gordon et al. [15] proposed a framework to manage cyber-risk. The antecedent activities involve the assessment of the risk involved in a security breach. Subsequent steps involve the preventive measures necessary to avert such an attempt. These measures are divided into technical or procedural measures (i.e., access control, firewalls) and financial measures (such as buying cyber insurance). The final step entails the maintenance of accepted level of risk.

The majority of current research on information security focuses on the preventive measures required for reducing cyber-risk. There is a large body of research that describes the technical aspects of security [14] such as encryption and secure communications, access control, and intrusion detection. This research can help managers select the technical preventive measures that best fit their organizational needs. Similarly, research addressing the behavioral aspects of security breaches (e.g., [37]) can help managers understand procedural preventive measures. However, there is a relatively small but growing body of academic research that can help managers assess the economic threats and financial vulnerabilities caused by information security breaches (for examples see [11, 14, 20, 26]). The goal of this paper is to add to this body of knowledge by assessing the financial impact of virus attack announcements on attacked companies.

In the following section, we describe the reasons for choosing market value as a measurement of the economic impact of security breaches. Section 3 describes the

Hovav A. and D'Arcy J. (2004).
The Impact of Virus Attack Announcements on the Market Value of Firms.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 146-156
DOI: 10.5220/0002668501460156

characteristics of virus attacks and defines them as unexpected events. Section 4 introduces the financial measures of unexpected events. In Section 5, we detail the methodology used. In section 6, we introduce and analyze the study's results. In section 7, we discuss the results, the study's limitations, and future research.

2 Market Value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget [15]. As the characteristics of security breaches change, companies continually reassess their IS environment for threats [23]. In the past, Chief Information Officers (CIOs) have relied on FUD – fear, uncertainty, and doubt – to promote IS security investments to upper management. Recently, some insurance companies have created actuarial tables that they believe provide ways to measure losses from computer interruptions and hacker attacks [34]. However, these estimates are questionable mostly due to the lack of historical data [15]. Some industry insiders confess that the rates for such plans are mostly set by guesswork [2]. As cited in Gordon et al., [15](p. 82): "These insurance products are so new, that the $64,000 question is: Are we charging the right premium for the exposure?" Industry experts cite the need for improved return on security investment (ROSI) studies that could be used by the organization to justify investments in security prevention strategies. However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons:

1. Many organizations are unable or unwilling to quantify their financial losses due to security breaches (for additional information see [32])
2. Lack of historical data. Many security breaches are unreported. Companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes [19], and fear of negative publicity [31]. Companies are also wary of competitors exploiting these attacks to gain competitive advantage [31].
3. Additionally, companies may be fearful of negative financial consequences resulting from public disclosure of a security breach [16].

Justifying investments in IS security using ROSI measures is difficult to accomplish. If the security measures work, the number of security incidents is low and there are no measurable returns. Accounting based measures such as ROSI are also limited by the lack of time and resources necessary to conduct an accurate assessment of financial loss when companies' IT resources are devoted to understanding the latest technologies and preventing future security threats [25]. In addition, potential intangible losses such as "loss of competitive advantage" that result from the breach and loss of reputation [8] are not included in ROSI measures because intangible costs are not directly measurable. Therefore, there is a need for a different approach to assess the economic impact of security breaches. One such approach is to measure the impact of a breach on the market value of a firm. A market value approach captures the capital market's expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself [16]. Moreover, managers aim to maximize

a firm's market value by investing in projects that either increase shareholder value or minimize the loss of shareholder value. Therefore, in this study we elected to use market value as a measure of the economic impact of security breach (virus attack) announcements on companies. In the following section we define a security breach as an unexpected event and discuss the characteristics of virus attacks.

3 Virus Attacks and their Reported Impact

An IS security breach is a violation of an information system's security policy. While security has long been a concern for IS managers, reports of serious security breaches have become more frequent in today's networked environment. The explosion of the World Wide Web (WWW) and the subsequent growth of e-commerce increase the exposure of organizations to external security breaches. Evidence of the current state of Internet security can be found in a recent CSI/FBI Computer Crime and Security Survey [32]. In the last four years, Internet connectivity has been cited as the primary source of attacks (78%). The most commonly reported security breaches are virus attacks [32]. Virus attacks reportedly cause billions of dollars in damage and have been accelerating in their scope and severity. Thus, we selected to study the financial impact of virus attacks as an upper bound exemplar of security breaches.

A virus is a small piece of self-replicating computer code that attaches itself to a larger, legitimate program [27]. While acknowledging the potential existence of harmless or even productive viruses (as described in [7]), the discussion in this paper is limited to viruses that are created with the purpose of causing damage. Early viruses were static pieces of code that copied themselves from program to program or diskette to diskette [29]. These viruses were easily contained – causing limited damage. Today's viruses are significantly more complex, which makes detection and removal more difficult. The most common types of viruses include macro viruses, e-mail viruses, trojan horses, and worms. In our discussion we term them all viruses.

While the threat of viral attacks was evident in the early 1980s, the first widely seen viruses did not occur until later in the decade. By 1988, virus attacks against IBM PCs, Apple II computers, and Macintosh computers had been reported [17]. The emergence of computer networks and the Internet in particular has created a new means for spreading computer viruses. Robert Morris is responsible for the first known viral attack against the Internet [35], which infected nearly 6,200 individual machines (about 7.3% of the Internet's computers at the time) and caused 8 million hours of lost access and an estimated $98 million in losses [26]. Since the Robert Morris worm, the Internet has been the victim of numerous viral attacks (such as Jerusalem, Chernobyl, and Michelangelo). However, until the mid 1990's access to the Internet was limited by the "Acceptable Usage Agreement", thus limiting the potential impact of virus attacks. Only after the commercialization of the Internet in 1994 was the Internet available to the general public, leading to an increasing number of virus attacks that infected a large number of commercial organizations and caused accelerated financial damage. For example, in March 1999, the Melissa virus forced a number of large companies to shut down their e-mail systems, causing an estimated $80 million in damages [5]. In May 2000, the LoveLetter worm (i.e., the I Love You virus) caused an estimated $100 million in damage by infecting some 1.27 million

computer files worldwide, with nearly 1 million in the United States [18]. In July 2001, the Code Red worm spread at an unprecedented rate, doubling its infestation rate every 37 minutes, eventually infesting over 350,000 hosts [28] and causing an estimated $2 billion in damage [30]. In January 2003, the Slammer worm infected about 90% of all vulnerable hosts on the Internet [28]. In August 2003, the Blaster worm affected nearly 500,000 computers in its first week [6]. ICSA labs estimated remediation costs (including hard, soft, and productivity costs) of $475,000 per company for the Blaster worm.

4 Financial Impact of Unexpected Event

Following the taxonomy of computer security incidents developed by Howard and Longstaff [21], a virus attack can be classified as a single computer and network security event involving an action directed against a specific target. In this case, the action is a virus attack and the target is a particular computer or a network of computers. Within the taxonomy, not all events are considered likely or even possible to occur. Therefore, we consider an Internet security breach (such as a virus attack) to be a negative computer security event that is not expected to occur on a regular basis. Prior research has assessed the financial impact of various unexpected events using both market-based measures and accounting-based measures of performance. However, the more popular research approach has been the event study. The event study examines the stock market reaction to the public announcement of a particular event and is based on the efficient market hypothesis [10]. According to the semi-strong form of the efficient market hypothesis, the market price of a firm fully reflects all publicly available information [12]. Therefore, an abnormal stock return associated with an unexpected event should be observed and measurable if the event has information content [22]. Previous research suggests that public news of an event that is generally seen as negative will cause a drop in a firm's stock price (e.g., [1]). Sprecher and Pertl [36] found that firms experiencing a loss from a catastrophic event sustained an immediate adverse effect on their stock price. Overall, prior studies of negative, unexpected events indicate that the market penalizes announcing firms in the first few days following the public disclosure of the negative event. However, it is unclear if firms suffer similar penalties following an announcement of a virus attack.

Despite the impact of IS security breaches on organizations and the heavy financial impact reported in trade magazines, there have been very few academic studies on the topic. Ettredge and Richardson [11] assessed the market risk associated with electronic commerce (e-commerce) activity. They performed a study to measure the spillover effect in the stock market response to a series of Denial-of-Service (DOS) attacks against several of the best-known Websites in February 2000. Results showed that investors do perceive risk in e-commerce activities as the DOS attacks had a larger negative spillover market impact on Internet firms than on non-Internet firms. Hovav and D'Arcy [20] found that DOS attacks have little effect on the market value of attacked companies. However, these attacks have a larger impact on E-commerce companies whose core business depends on their Web presence than on non-Internet specific companies. McAfee and Haynes [26] conducted the only study to estimate the impact of virus attacks. They calculated the damage of the Robert Morris worm

using accounting-based measures including direct programmer costs, indirect labor and burden costs, and indirect costs such as lost machine down time and user lost access time. Given the increase in the number of virus attacks over the last 15 years and the increase in their severity, it is imperative to evaluate the economic impact of these attacks. As described above, prior research found that public announcements that contain negative information cause an abnormal drop in the stock value of affected companies. Therefore, we anticipate that virus attack announcements will have a negative impact on the stock value of attacked companies.

H1: An announcement of a virus attack of a company *j* will result in negative abnormal returns on stock *j* for the day of the announcement.

Traditional event studies look at the distribution of the cumulative standardized abnormal returns (CSAR) of all affected companies. The virus attacks are expected to have a negative impact on the CSAR of the sample (i.e., the total of the actual returns << total expected returns).

H2: The cumulative standardized abnormal returns for the entire sample during the event period are significantly negative.

The following section depicts the methodology used. The data collection and analysis conform to the conventional procedures used in event studies.

5 Methodology

A procedure for sample selection similar to the method used by Subramani and Walden [38] and Im et al. [22] was followed in this study. We collected data on virus attacks using a search of business news in the Lexis-Nexis database. The search consisted of all public announcements of virus attacks between 1988 and 2002 resulting in 224 announcements. The initial list was then refined and evaluated based on the following criteria:

1. Only announcements by firms publicly traded on either the New York Stock Exchange (NYSE) or the NASDAQ stock exchange were included.
2. Announcements that might be confounded by other key firm notices such as mergers, acquisitions, earnings, stock splits, dividends, etc. within five days of the virus attack announcement were excluded.
3. To remove event day uncertainty [9], we triangulated our Lexis-Nexis search results with additional Web searches and information from financial publications.

For individual firms' stock market data, we relied on the database of the Center for Research in Security Prices (CRSP). We included in the sample only virus attack announcements for which stock return data was available. These sampling criteria yielded 186 virus attack announcements (events). The impact of announcements of virus attacks on common stock prices is computed using event study methods commonly employed in the accounting and finance literature [10]. The event of interest in this study is the public announcement of a virus attack by either the attacked firm or some other media outlet. If an announced virus attack contains new information, it should cause the markets to revalue the firm. Determining whether these events affect a firm's stock price requires that we estimate what the firm's stock price would have been had there been no announcement. We then calculate the

standardized abnormal returns. Under the null hypothesis of zero expected abnormal returns, Z is approximately unit normally distributed (see [24]). For a more detailed discussion of analytical techniques employed in event studies, see Campbell et al. [4].

6 Analysis and Results

To test hypothesis 1, we calculated the mean abnormal return for each individual company, analyzed the results, and assessed the impact. Table 1 summarizes our findings. Overall, the results indicate that the virus announcements did not result in negative abnormal returns over any of the five event periods for our sample of attacked companies, as the mean abnormal return for each event period was positive. Thus, hypothesis 1 was not supported. However, there is partial support for hypothesis 1 as almost half of the firms experienced negative abnormal returns (Table 1) for a period of 25 days after the announcement.

Table 1. Mean Abnormal Returns and Number of Negative Returns for Attacked Companies

Event Windows	Mean Abnormal Return	Median Abnormal Return	Number of Negative Abnormal Returns
[0, 0]	0.0032	0.0019	79 (42%)
[0, 1]	0.0029	0.0010	81 (44%)
[0, 5]	0.0013	0.0016	79 (42%)
[0, 10]	0.0012	0.0013	82 (44%)
[0, 25]	0.0005	0.0007	84 (45%)

To test hypothesis 2, we calculated the CSAR for the entire sample. Table 2 lists the mean CSAR for each event window as well as the results of the z-tests to test the significance of the CSAR. Average CSARs for each of the event periods are positive, indicating that the virus attack announcements did not result in lower abnormal returns for the sample over any of the time periods. These results are contrary to what was expected, and therefore we reject hypothesis 2.

Table 2. Cumulative Standardized Abnormal Returns (CSAR) for Attacked Companies

Event Windows	Mean CSAR	Z-value*
[0, 0]	0.1196	1.6317
[0, 1]	0.0787	1.0730
[0, 5]	0.0554	0.7550
[0, 10]	0.0380	0.5183
[0, 25]	0.0134	0.1829
* Z- statistic to compute the significance of the average abnormal return over each event period under the null hypothesis that the average abnormal return is zero.		

To further test hypothesis 2, we divided the virus announcements into industry sub-samples by the SIC (Standard Industrial Classification) code of the attacked company. Similar results were found analyzing the sample by industry (i.e., there is no industry impact on the results of the analysis). These results are displayed in Appendix A.

7 Discussion

Overall, the above results did not demonstrate that there is a significant impact of virus attack announcements on the share price of the attacked companies. Mean abnormal returns were positive for each of the event periods studied. In addition, CSARs were not significantly negative (for the total sample or by industry) over any of the five event periods, whereas viruses were associated with negative stock returns for about 44 - 45% of the attacked companies. These unexpected findings are contradictory to the increasing financial impact reported by trade magazines and may be due to one of the following: (1) the market anticipates the virus attacks and incorporates the projected losses into the stock value of companies; or (2) there is little awareness in the general public as to the real damage caused by virus attacks, thus the market does not react to such announcements; or (3) the financial damage reported in trade magazines is inflated and the above market analysis reflects a more rational view of the actual damages.

Our findings demonstrate that the market does not penalize firms when they are exposed to virus attacks which results in little incentives for managers to demand improved security in current Information Systems (i.e., trustworthy computing) from IT vendors[1]. This also supports Blumenthal's [3] assertion that IT vendors take little action to increase information technology security due to lack of demand from their users. Thus, the assumption that market forces can be used as means to control security breaches and to increase the trustworthiness of computer systems might be false.

The above discussion suggests the need for further research in this area. First, there is a need to better understand the actual economic and financial impact of security breaches and their reflection on the market. Second, it is unclear if other types of attacks will have a more significant impact on shareholders' value. For example, recent legislation places legal liability on companies that expose private information to unauthorized entities (e.g., HIPAA, California's Database Breach Notification Security Act –SB 1386). Liability lawsuits may introduce new costs that could be perceived (by the market) as more substantial than the cost to recover from a virus attack. Therefore, it is possible that security breach announcements that involve the exposure of private information will result in more significant negative abnormal returns. Taxonomy of security breaches and the extent of their impact will allow managers to concentrate their efforts and allocate security budgets towards breaches

[1] For example, Microsoft's trustworthy computing initiative is estimated to cost $200 million and already delayed the launch of Server 2003 by several months. These additional costs will ultimately be transferred to the customer. Given that virus attacks do not reduce shareholder value, managers will have little incentive to demand increased security from IT vendors, which will only increase firms' IT costs.

that have larger effect. Third, there is a need to understand the impact of viruses on IT vendors and the factors that will drive the IT industry to create more secure information systems. In addition, future research can examine the impact of virus attacks on small and private organizations that may not have the resources to quickly recover from such attacks.

This study has several limitations. First, our sample contained two time clusters involving the Melissa virus in March 1999 and the LoveBug virus in May 2000. Time clusters can increase the significance of the results [9]. We repeated the analyses without the announcements involving these two virus events and the overall results of the study did not change. Second, the sample consists of only publicly traded companies. Therefore, the results cannot be generalized to non-publicly traded companies. Finally, many of the attacks caused a short downtime. Therefore, it is possible that the stock value was down during the day but closed normal once the problem was fixed and the affected systems were functioning again. This is referred to as intra-day stock movement.

8 Conclusions

Reports of security breaches in the popular business press suggest that computer viruses cause substantial financial damage to attacked companies. In this paper, we assessed the impact of virus announcements on attacked companies over a period of 15 years using event study methodology. Our results indicate that in general the market does not penalize companies who are victimized by virus attacks. These results are contradictory to findings in prior research, which indicates that the market penalizes companies involved in events containing negative information. These results also suggest that market forces cannot be used as a means of controlling security breaches nor can they be used to entice IT vendors to increase the trustworthiness of computer systems. Further research is required to understand the risk associated with security breaches. In addition, recent legislation suggests the need to better understand the factors that will reduce security risks and lead to a trustworthier Information Technology environment.

References

1. Baginski, S. P., R. B. Corbett, et al. (1991). "Catastrophic Events and Retroactive Liability Insurance: The Case of the MGM Grand Fire." The Journal of Risk and Insurance 58(2): 247-260.
2. Berinato, S. (2002). Finally, a Real Return on Security Spending. CIO: The Magazine for Information Executives. 15: 42-52.
3. Blumenthal, M. (1999). "The Politics and Policies of Enhancing Trustworthiness for Information Systems." Communication Law & Policy 4(4): 513-555.
4. Campbell, J. Y., A. W. Lo, et al. (1997). Event Study Analysis. Chapter 4 in The Econometrics of Financial Markets. Princeton, NJ, Princeton University Press.

5. Chen, C. Y. and G. Lindsay (2000). Viruses, Attacks, and Sabotage: It's a Computer Crime Wave. Fortune. 141: 484-487.
6. Chen, T.M., (2003). “Trends in Viruses and Worms.” The Internet Protocol Journal 6(3): 23-33.
7. Cohen, F (1984). Computer Viruses: Theory and Experiments. Proceedings of the Second IFIP International Conference on Computer Security, Toronto, Ontario, Canada.
8. D'Amico, A. (2000). What Does A Computer Security Breach Really Cost?, The Sans Institute. 2000.
9. Dyckman, T., D. Philbrick, et al. (1984). “A Comparison of Event Study Methodologies Using Daily Stock Returns: A Simulation Approach.” Journal of Accounting Research 22: 1-30.
10. Etebari, A., J. O. Horrigan, et al. (1987). "To Be or Not To Be - Reaction of Stock Returns to Sudden Deaths of Corporate Chief Executive Officers." Journal of Business Finance & Accounting 14(2): 255-279.
11. Ettredge, M. and V. J. Richardson (2001). Assessing the Risk in E-Commerce. Twenty-Second International Conference on Information Systems, New Orleans, LA.
12. Fama, E., L. Fisher, et al. (1969). "The Adjustment of Stock Prices to New Information." International Economic Review 10: 1-21.
13. Glover, S., S. Liddle, et al. (2001). Electronic Commerce: Security, Risk Management, and Control. Upper Saddle River, NJ, Prentice Hall.
14. Gordon, L.A. and M.P. Loeb (2002). “The Economics of Information Security Investment.” ACM Transactions on Information and Systems Security 5(4): 438-457.
15. Gordon, L.A., M.P. Loeb, et al. (2003) “A Framework for Using Insurance for Cyber-Risk Management.” Communications of the ACM 46(3): 81-85.
16. Hancock, B. (2002). “Security Crisis Management - The Basics.” Computers & Security 21(5): 397-401.
17. Hayes, F. (2003). The Story So Far. Computerworld. 37: 26-27.
18. Hinde, S. (2000). "Love Conquers All?" Computers & Security 19(5): 408-420.
19. Hoffer, J. A. and D. W. Straub (1989). "The 9 to 5 Underground: Are You Policing Computer Crimes?" Sloan Management Review (Summer 1989): 35-43.
20. Hovav, A. and J. D’Arcy (2003) “The Impact of Denial-of-Service Announcements on the Market Value of Firms.” Risk Management and Insurance Review, 6(2): 97-121.
21. Howard, J. D. and T. A. Longstaff (1998). A Common Language For Computer Security Incidents. Pittsburgh, PA, CERT Coordination Center at Carnegie Mellon University: 1-33.
22. Im, K. S., K. E. Dow, et al. (2001). “A Reexamination of IT Investment and the Market Value of the Firm: An Event Study Methodology.” Information Systems Research 12(1): 103-117.
23. Kelly, B. J. (1999). "Preserve, Protect, and Defend." Journal of Business Strategy (September/October 1999): 22-26.
24. Loderer, C. and D. C. Mauer (1992). “Corporate Dividends and Seasoned Equity Issues: An Empirical Investigation.” Journal of Finance 47(1): 201-225.
25. Lyman, J. (2002). In Search of the World's Costliest Computer Virus, www.newsfactor.com/perl/story/16407.html. 2002.

26. McAfee, J. and C. Haynes (1989). Computer Viruses, Worms, Data Diddlers, Killer Programs, & Other Threats To Your System. New York, New York, St. Martins Press.
27. Montana, J. C. (2000). "Viruses and the Law: Why the Law is Ineffective." The Information Management Journal 34(4): 57-60.
28. Moore, D., G.M. Voelker, et al. (2001). “Inferring Internet Denial-of-Service Activity.” Proceedings of the 10th USENIX Security Symposium, Washington, D.C.
29. Nachenberg, C. (1997). "Computer Virus - Antivirus Coevolution." Communications of the ACM 40(1): 46-51.
30. Panko. R.R. (2003). “Slammer: The First Blitz Worm.” Communications of the Association for Information Systems. 11: 207-218.
31. Power R. (2001). “2001 CSI/FBI Computer Crime and Security Survey.” Computer Security Issues and Trends 7(1): 1-18.
32. Power, R. (2003). “2003 CSI/FBI Computer Crime and Security Survey.” Computer Security Issues and Trends 9(1): 1-20.
33. Salierno, D. (2001). Managers Fail to Address E-risk. The Internal Auditor. April 2001: 13.
34. Salkever, A. (2000). Who Pays When Business Is Hacked?, www.businessweek.com/bwdaily/dnflash/may2000/nf00523d.htm.
35. Spafford, E. (1999). "Crisis and Aftermath." Communications of the ACM 32(6): 678-687.
36. Sprecher, R. and M. Pertl (1988). “Intra-Industry Effects of the MGM Grand Fire.” Quarterly Journal of Business and Economics 27: 96-16.
37. Straub, D.W. and R.J. Welke. (1998) “Coping With Systems Risk: Security Planning Models for Management Decision Making.” MIS Quarterly 22(4): 441-469.
38. Subramani, M. and E. Walden (2001). “The Impact of E-Commerce Announcements on the Market Value of Firms.” Information Systems Research 12(2): 135-154.

Appendix A. Cumulative Standardized Abnormal Returns (CSAR) for Attacked Companies by Industry

Event Windows	Mean CSAR	Z-value*
Finance, Insurance, and Real Estate (n=25)		
[0, 0]	0.0919	0.4596
[0, 1]	0.1260	0.6300
[0, 5]	0.1309	0.6546
[0, 10]	0.0061	0.0303
[0, 25]	-0.0261	-0.1305
Manufacturing(n=78)		
[0, 0]	0.0911	0.8047
[0, 1]	0.0835	0.7374
[0, 5]	0.0242	0.2136
[0, 10]	0.0233	0.2062
[0, 25]	0.0100	0.0883
Retail Trade (n=6)		
[0, 0]	0.2835	0.6944
[0, 1]	-0.1170	-0.2866
[0, 5]	0.0440	0.1077
[0, 10]	0.0412	0.1009
[0, 25]	0.0436	0.1067
Services (n=35)		
[0, 0]	0.1462	0.8649
[0, 1]	0.0692	0.4094
[0, 5]	-0.0393	-0.2325
[0, 10]	-0.0116	-0.0687
[0, 25]	-0.0139	-0.0821
Transportation, Communications, Electric, Gas and Sanitary Services (n=42)		
[0, 0]	0.1436	0.9306
[0, 1]	0.0774	0.5017
[0, 5]	0.1488	0.9641
[0, 10]	0.1251	0.8110
[0, 25]	0.0617	0.3999

* Z statistic to compute the significance of the average abnormal return over each event period under the null hypothesis that the average abnormal return is zero.