Information & Management 46 (2009) 404–410

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

# Estimating the market impact of security breach announcements on firm values

Sanjay Goel *, Hany A. Shawky

*School of Business, University at Albany, SUNY, United States*

ARTICLE INFO

*Article history:*
Received 19 November 2008
Received in revised form 6 April 2009
Accepted 26 June 2009
Available online 18 August 2009

*Keywords:*
Security breaches
Event-study methodology
Risk analysis
Information assurance
Market valuation
Information security

ABSTRACT

Security breaches can have a significant economic impact on a firm. With public disclosure laws passed, security breaches involving disclosure of private client information can both damage the firms' reputation and lead to fines by US government agencies. We examined the impact of security breaches of US firms, as measured by their impact on the firm's market value. Data on security breaches were collected over the period 2004–2008. Reports and news articles corresponding to these breaches were obtained from public sources. Using event-study methodology, we estimate the impact of security breaches on the market value of publicly traded firms. Daily stock returns for firms impacted were obtained. Our results indicated that, on average, the announcement of a corporate security breach had a negative impact of about 1% of the market value of the firm during the days surrounding the event.



## 1. Introduction

The main goal of our research was to estimate the impact of security breaches on the market value of publicly traded firms. Data on incidents (security breaches) along with reports and news articles corresponding to them were obtained from public sources over the period 2004–2008. Event-study methodology was used to examine the market reaction surrounding the announcement of corporate security breaches. Our empirical results provide strong evidence of a statistically significant negative market price reaction at approximately the time of the corporate announcements.

Incidents of security breaches that reveal company secrets or confidential client information can affect the firm seriously. Leakage of sensitive information may lead to litigation, government sanctions, and loss of competitive edge. Organizations are often reluctant to reveal information about security breaches for fear of providing information to hackers. An even greater concern is the potential drop in market value of a firm following the revelation of a security breach [5].

Firms commonly institute managerial, technical, and operational controls to minimize exposure of their valuable assets; for example, Suh and Han [9] in presenting an IS risk analysis method proposed a three stage process: asset identification and valuation, identification of threats and vulnerabilities, and risk analysis. Noting the lack of empirical research in the area of security risk management, Kotulic and Clark [8] proposed a conceptual model to study the security risk management process in firms.

Selection of controls is an optimization problem that involves balancing the potential damage, by examining the value of each asset and the probability of it being damaged against the cost of its control. The impact of controls in reducing the potential damage is then balanced against the cost of the control. The fundamental problem of this approach is that data collection is cumbersome and its estimates rely heavily on subjective judgment of the analysts.

Measuring the changes in the market value of publicly traded companies due to security breaches provides an efficient means of evaluating *security* risks. The *efficient market hypothesis* asserts that financial markets are informationally efficient, and that stock prices reflect all publicly available information. Thus, the impact of security breaches can be measured by observing changes in the market value of firms in response to announcements of security breach incidents. In our study, mandatory data disclosures made by organizations that include the type of breach (e.g. malicious code, stolen hardware, or insider attacks) and its severity (in terms of the number of people impact) are identified.

A potential benefit of our research is in providing organizations with some general guidelines that lead to making sound business decisions about information security investments. One of the main difficulties that firms have in analyzing security risks is in quantifying the losses that may stem from regulatory fines as well as the cost of managing breaches. While, in general, firms attempt to implement security controls to minimize these losses,

* Corresponding author at: BA 310b, 1400 Washington Avenue, Albany, NY 12222, United States. Tel.: +1 518 442 4925; fax: +1 518 442 2568.
*E-mail address:* goel@albany.edu (S. Goel).

0378-7206/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.im.2009.06.005

they are not able to optimize their investment in information security due to a lack of good estimate of potential losses.

Investigating the impact of the managerial, technical and operational controls of an organization on security breaches would be immensely useful in helping management decide on the type of security controls they need, however, such an analysis would require collection of detailed data on security controls for each firm in our data set. This would require the collection of data through a survey instrument. Unfortunately, most organizations are reluctant to disclose information regarding their internal controls, because public knowledge of such controls can help hackers and competitors. Our findings on the anticipated market reaction should provide corporate executives with guidance on managing public disclosure of security breaches.

Yeh and Chang [11] recently found that industry type and organizational use of IT were the two factors that most affected firms to adopt security countermeasures. They further suggested that the scope of the countermeasures were not commensurate with the severity of the perceived threats. Using estimates presented in their paper, organizations might be able to quantify the potential loss of value resulting from a security breach, which would in turn allow them to invest in information security controls that are commensurate with the expected loss.

In previous event-study analyses, Campbell et al. [2] examined the impact of security breaches on market performance and found that firms that experience a breach of confidential information' saw a 5% drop in stock price while firms suffering a non-confidential breach saw no such effect. Cavusoglu et al. [4] found that announcement of an Internet security breach was negatively associated with the market value of the firm, and that, on average, breached firms lost approximately 2.1% of their market value within two days of the announcement of a security breach.

Hovav and D'Arcy [6,7] examined the impact of security breaches for a limited subset (viruses, worms, and denial-of-service). They concluded that the relative impact of the different types of breaches was not clear. Telang and Wattel [10] conduct a study on disclosure of the vulnerabilities of software vendors and showed that firms lose around 0.6% of their market value when the vulnerability is reported; this is equivalent to the loss of about $0.86 billion per firm for each vulnerability disclosure.

Among the most important breaches today is identity theft. This has led to the creation of public disclosure laws requiring corporations to report incidents where customers' personal information is unlawfully or accidentally revealed. Given that identity theft can jeopardize the victims' credit ratings, there is much publicity about these types of incidents. Acquisti et al. [1] investigate the impact of privacy breaches on market value of firms and demonstrate a statistically significant negative impact of such breaches on the market value of affected firms.

## 2. Analysis and empirical findings

We used event-study methodology to estimate the impact of security breaches on the stock market valuation of breached firms. The basic premise of this methodology is that in an efficient capital market, the true impact of an event will be quickly and completely reflected in the value of the firm. Thus, the event's economic impact can be measured using asset prices observed over a relatively short time period around the occurrence of the event. A detailed description of the event-study methodology is provided in Appendix A.

The data required for our research included the identification of security breach announcement dates reported in various media outlets and the comparable stock market prices. The reports were available from public sources such as Lexis Nexis, *Wall Street Journal*, PC Week, Register and others. Several states have enacted laws that require corporations to inform consumers who may have been affected by compromised personal information through breaches. For each identified security breach, media reports covering the security breach were collected and stored in a database. The data collected also included information on the severity of each incident in terms of the number of people impacted.

Using the approximate date of the security breach as a starting point, public databases like Lexis Nexis were queried for media reports; those reports that covered more than one individual security breach were associated with each security breach reported. In the event that a single report was published in numerous media outlets, it was considered a single report. To avoid any contamination of the estimation window, we excluded from our sample any firm that experienced more than one security breach within a period of one year.

In order to identify the impact, each incident was classified by the type of breach, such as, fraud, lost backup takes, malicious code, theft, etc. Similarly, industry and sector information for each company were collected to determine if the type of business affected the market's response. However, slicing the data into subsets resulted in data sets that were too small to obtain statistically significant results.

*Eventus software* (a product of Cowan Research LC [http://www.eventstudy.com]) was used for the event study analysis. In addition to information on security breach incidents gathered in our database, we use data from the Center for Research in Security[1] Prices (CRSP) to determine daily price information on each of the impacted firms. Knowing the precise date on which the public was made aware of the security breach was critical. While we identified over 250 security breach incidents, we were able to locate an approximate date (within three to four days) for only 205 incidents and exact announcement dates for 168.

While we initially examined the results using the larger sample of 205 incidents in which we could not identify an exact date for 37 of the incidents, it became apparent that we were introducing a potential bias with respect to the behavior of the residual three to four days around the event. As a result, we decided to focus our attention on the relatively smaller sample of 168 breach incidents for which we have full confidence in identifying the exact announcement date of the breach.

Table 1 presents average abnormal returns and cumulative abnormal returns for the sample of 168 observations estimated using the single index market model while Table 2 presents average abnormal returns and cumulative abnormal returns estimated using the Fama–French three factor model. The use of the Fama and French factor model incorporated observed market anomalies with respect to firm size and the value premium. As such, abnormal residuals obtained through this model were believed to be more reliable than those obtained using the standard market model. The tables present a similar picture regarding the behavior of the average abnormal returns (AR) and the cumulative abnormal returns (CAR) around the security breach announcement event.

We estimated normal model parameters using a window 255 days prior to the event period and the AR for (−119) days prior to the event and (+10) days after the event. The average and cumulative abnormal returns were found to significantly decline in the one or two days prior to the event date. While we would expect the decline to occur only after the incident, it was very likely that, significant information would be revealed to insiders and some impacted individuals, just prior to the public announcement. Even limited information might spark significant market speculation on

[1] Security is a commonly used term for stocks. In this case, security prices mean stock prices.

**Table 1**
Average abnormal market model residuals and cumulative average residuals for 168 incidents of corporate security breach events during the period 2004–2008. One, two and three asterisks denote residuals are significant at the 10, 5 and 1% levels.

| Day | AR | CAR | Patell Z | Day | AR | CAR | Patell Z | Day | AR | CAR | Patell Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| −119 | −0.0001 | −0.0001 | −0.501 | −75 | −0.0012 | 0.0048 | −0.822 | −31 | −0.0043 | 0.0082 | −3.256*** |
| −118 | 0.0006 | 0.25 | 0.535 | −74 | −0.0001 | 0.0047 | 0.256 | −30 | −0.0019 | 0.0063 | −1.239 |
| −117 | 0.0004 | 0.0009 | 1.019 | −73 | −0.0001 | 0.0046 | 0.001 | −29 | 0.0013 | 0.0076 | 1.489$ |
| −116 | 0.0008 | 0.0017 | 0.573 | −2 | −0.0005 | 0.0041 | 0.002 | −28 | 0.00982 | 0.0098 | 2.774** |
| −115 | 0.0006 | 0.0023 | 0.366 | −71 | 0.0012 | 0.0053 | 0.484 | −27 | −0.0017 | 0.0115 | −1.221 |
| −114 | −0.002 | 0.0003 | −1.744* | −70 | −0.0016 | 0.0037 | −1.667* | −26 | 0.0001 | 0.0116 | 0.13 |
| −113 | −0.0011 | −0.0008 | −1.644 | −69 | −0.0002 | 0.0035 | −0.314 | −25 | 0.001 | 0.0126 | 1.093 |
| −112 | −0.0006 | −0.0014 | −1.353 | −68 | 0.0026 | 0.001 | 2.558** | −24 | −0.0005 | 0.0121 | −0.39 |
| −111 | −0.0008 | −0.0022 | −0.266 | −67 | −0.0018 | 0.036 | −1.340$ | −23 | −0.002 | 0.0119 | −0.036 |
| −110 | 0.0018 | −0.0004 | 0.888 | −66 | −0.0003 | 0.0024 | 40.0143 | −22 | 0.0024 | 0.0143 | 1.676* |
| −109 | −0.0018 | −0.0022 | −1.743* | −65 | −0.0011 | 0.0029 | −0.1 | −21 | 0 | 0.138 | −0.138 |
| −108 | 0.0014 | −0.0008 | 1.075 | −64 | −0.0021 | 0.0008 | −1.477 | −20 | −0.0004 | 0.0139 | −0.305 |
| −107 | 0 | −0.0008 | −0.018 | −63 | 0.157 | 0.0015 | 0.001 | −19 | −0.0002 | 0.157 | −0.157 |
| −106 | −0.0015 | −0.0023 | −1.608 | −62 | 0.0005 | 0.002 | 0.353 | −18 | 0.0009 | 0.0146 | 1.039 |
| −105 | −0.0001 | −0.0022 | −0.375 | −61 | 0.0006 | 0.0026 | 0.976 | −17 | −0.0001 | 0.0156 | −1.093 |
| −104 | 0.0012 | 40.001 | 1.479 | −0.0 | 0.0008 | 0.0034 | 0.57 | −16 | 40.001 | 0.0146 | −1.194 |
| −103 | 0.0002 | −0.0008 | 0.513 | −59 | −0.0007 | 0.0027 | −1.221 | −15 | 0.0012 | 0.0158 | 0.998 |
| −102 | 0.0012 | 0.014 | 0.674 | −58 | −0.0001 | 0.0026 | −0.549 | −14 | 20.001 | 0.0148 | −1.335 |
| −101 | 0.0009 | 0.0013 | 1.169 | −57 | −0.0001 | 0.0025 | −0.195 | −13 | 10.002 | 0.0136 | −0.898 |
| −100 | −0.0007 | 0.0006 | −0.483 | −56 | −0.0002 | 0.013 | 30.01 | −12 | 0.013 | 0.0139 | 0.285 |
| −99 | 0.0007 | 0.0013 | 0.245 | −55 | 0.0012 | 0.85 | −0.85 | −11 | −0.0006 | 0.643 | −0.643 |
| −98 | 0.0011 | 0.0024 | 0.488 | −54 | 0.0013 | 0.0048 | 1.386 | −10 | −0.0006 | 0.0127 | −0.21 |
| −97 | 0.0005 | 0.0029 | 0.25 | −53 | 0.424 | 0.002 | 0.424 | −9 | 50.002 | 0.0125 | −0.367 |
| −96 | −0.0019 | 0.001 | −1.751* | −52 | 0.0134 | 0.0056 | 0.41 | −8 | 0.0009 | 0.0134 | 1.162 |
| −95 | −0.0003 | 0.0007 | −0.082 | −51 | 0.132 | 0.0058 | 0.832 | −7 | 0.0003 | 0.0137 | 0.132 |
| −94 | −0.0015 | 0.0022 | −0.113 | −50 | 0 | 0.0058 | 0.0142 | −6 | 0.0005 | 0.0142 | 1.286$ |
| −93 | 0.0001 | 0.0021 | 0.305 | −49 | 0 | 0.0058 | −0.073 | −5 | 0.305 | 0.0147 | 0.305 |
| −92 | 0.0004 | 0.0025 | 1.103 | −48 | −0.0003 | 0.5 | 10.01 | −4 | 40.00251 | 0.0146 | −0.361 |
| −91 | 0.0001 | 0.0026 | 1.414$ | −47 | 0.0003 | 0.0058 | 0.448 | −3 | 10.0026 | 0.014 | −0.264 |
| −90 | −0.0003 | 0.0029 | −0.56 | −46 | −0.0007 | 0.01 | −0.11 | −2 | −0.004 | 0.01 | −3.925*** |
| −89 | 0.0013 | 0.0042 | 1.738* | −45 | −0.0006 | 0.0045 | −0.44 | −1 | 90.0013 | 0.0113 | −1.925* |
| −88 | 0 | 0.0042 | 0.502 | −44 | 0.0098 | 0.0053 | 0.698 | 0 | −0.0015 | 0.0098 | −1.39 |
| −87 | 0.0012 | 0.0054 | 1.604$ | −43 | 20.005 | 0.0038 | −1.359 | 1 | 50.0038 | 0.007 | −2.157* |
| −86 | −0.0007 | 0.0047 | −0.451 | −42 | 0 | 0.0038 | −0.097 | 2 | 0.0084 | 0.0084 | 2.016* |
| −85 | −0.0005 | 0.0042 | −0.178 | −41 | −0.0012 | 0.0026 | −1.285 | 3 | 0.0001 | 0.0085 | 0.388 |
| −84 | 0.0011 | 0.0053 | 0.717 | −40 | 0.0012 | 0.0038 | 0.556 | 4 | −0.0016 | 0.0069 | −1.353 |
| −83 | 0.0006 | 0.0059 | 0.074 | −39 | −0.0011 | 0.0027 | −1.61 | 5 | 0.0001 | 0.007 | 0.407 |
| −82 | −0.002 | 0.0039 | −2.351** | −38 | 0.0009 | 0.006 | 0.944 | 6 | −0.0002 | 0.0068 | −0.101 |
| −81 | −0.0007 | 0.0032 | −0.433 | −37 | 0.019 | 0.0477 | 0.047 | 7 | 0.019 | 0.0069 | −0.019 |
| −80 | −0.002 | 0.0012 | −1.61 | −36 | 0.0007 | 0.0044 | 0.496 | 8 | 0.0006 | 0.0075 | 1.008 |
| −79 | −0.0001 | 0.0013 | −0.291 | −35 | 0.0023 | 6.737 | 3.624*** | 9 | 0.0047 | 0.0122 | 6.737*** |
| −78 | 0.0028 | 0.0041 | 2.230* | −34 | 0.0014 | 0.0131 | 1.665* | 10 | 0.0009 | 0.0131 | 0.652 |
| −77 | 0.0009 | 0.005 | 0.855 | −33 | −0.0016 | 0.0107 | −2.499** | | | | |
| −76 | 0.001 | 0.006 | 0.658 | −32 | 0.0018 | 0.0125 | 2.617** | | | | |

the firm's stock price, leading to the observed negative decline in the market value of the firm in the day prior to the announcement.

It should also be noted that event study results inevitably produce some significant positive and negative abnormal residuals that are scattered randomly throughout the testing period. Such significant positive or negative abnormal residuals that occur outside the examination period (similar to that one occurring on day +9) are not of much concern. Such observations are often the result of external stock market shocks that are not removed by the normal averaging process used in the event-study methodology. What was important in the tables was the preponderance of significant negative abnormal residuals in the days surrounding the event. Specifically, it is the *persistence* of the significant negative residuals around the event date that generates significant cumulative abnormal returns indicating that there were significant economic consequences revealed to the market on that date.

In general, we observe a statistically significant negative AR and CAR around the event date. The results from both the single index model and the three factor model showed that in two of the three days prior to the breach event, we observed negative and statistically significant abnormal returns. Moreover, both models also indicated that there was a negative effect on the returns of these firms on the day of the event and a highly significant negative impact occurring on the day following the incident. This was fairly strong evidence that there was negative market impact on firm value surrounding announcements of security incidents.

The significant cumulative abnormal returns surrounding the event date documented in the tables revealed that the market anticipated the security breaches and had reacted negatively to the information (evidenced by an average decline in the stock price of the impacted firms). Such negative reaction is characteristic of bad news when investors are unsure or concerned about the extent of the financial damage that might result. Once the news of the breach is out, it is vital for firms to alleviate fears and uncertainty by clearly explaining the extent of the breach and their immediate and long-term response to it.

Figs. 1 and 2 depict the behavior of both the AR and the CAR for the single index model and the three factor models respectively. In both instances we see a clear and significant drop in the CAR immediately prior to the announcement date. The magnitude of this cumulative decline in the abnormal returns around the announcement of the security breach is in the order of 8% for the

**Table 2**
Average abnormal three factor (Fama–French) market model residuals and cumulative average residuals for 168 incidents of corporate security breach events during the period 2004–2008. One, two and three asterisks denote residuals are significant at the 10, 5 and 1% levels.

| Day | AR | CAR | Patell Z | Day | AR | CAR | Patell Z | Day | AR | CAR | Patell Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| −119 | −0.020 | −0.020 | 0.279 | −75 | −0.100 | 0.080 | 0.434 | −31 | 00.410 | 0.410 | −0.184 |
| −118 | −0.020 | −0.040 | −0.338 | −74 | −0.060 | 0.020 | 0.125 | −30 | 00.210 | 0.210 | −2.191** |
| −117 | 0.030 | −0.010 | 0.434 | −73 | −0.020 | 0.0200 | 1.051 | −29 | 0.330 | 0.330 | 0.897 |
| −116 | 0.090 | 0.080 | 0.279 | −72 | −0.040 | −0.040 | 1.823** | −28 | 0.090 | 0.420 | 1.515* |
| −115 | 0.060 | 0.140 | −0.647 | −71 | 0.050 | 0.010 | 0.434 | −27 | 0.540 | 0.540 | 0.588 |
| −114 | −0.230 | −0.090 | −0.956 | −70 | −0.170 | −0.160 | −1.265 | −26 | 0.560 | 0.560 | −0.184 |
| −113 | −0.070 | −0.160 | −0.184 | −69 | 0.080 | 90.080 | 1.669* | −25 | 0.050 | 0.610 | −1.265 |
| −112 | −0.030 | −0.190 | −0.493 | −68 | 0.270 | 0.190 | 3.213 | −24 | −0.060 | 0.550 | −1.110 |
| −111 | −0.090 | −0.280 | 0.125 | −67 | −0.170 | 0.020 | −0.810 | −23 | −0.010 | 0.540 | −0.184 |
| −110 | 0.150 | −0.130 | 0.897 | −66 | −0.040 | −0.020 | −0.493 | −22 | 0.190 | 0.730 | 1.36* |
| −109 | −0.140 | −0.270 | −0.956 | −65 | −0.070 | −0.090 | −1.419* | −21 | −0.030 | 0.070 | −0.810 |
| −108 | 0.120 | −0.150 | −0.338 | −64 | −0.080 | −0.170 | −0.647 | −20 | −0.090 | 0.610 | −0.493 |
| −107 | −0.030 | −0.180 | −1.419* | −63 | 0.050 | −0.120 | −0.184 | −19 | −0.110 | 0.500 | −0.493 |
| −106 | −0.130 | −0.310 | −0.338 | −62 | 0.110 | −0.010 | −0.493 | −18 | 0.050 | 0.550 | 0.434 |
| −105 | 0.020 | −0.290 | −0.493 | −61 | 0.080 | 0.070 | 0.743 | −17 | 0.580 | 0.580 | 0.279 |
| −104 | 0.090 | −0.200 | 1.669* | −60 | 0.000 | 0.070 | −0.184 | −16 | −0.150 | 0.430 | −1.419* |
| −103 | 0.040 | −0.160 | −0.184 | −59 | −0.030 | 0.040 | −1.419* | −15 | 0.540 | 0.540 | −0.493 |
| −102 | 0.120 | −0.040 | 0.897 | −58 | −0.060 | −0.020 | −0.956 | −14 | 00.330 | 0.330 | −2.191** |
| −101 | 0.140 | 0.100 | −0.338 | −57 | −0.040 | −0.060 | 0.279 | −13 | −0.130 | 0.200 | −0.647 |
| −100 | −0.020 | 0.080 | 0.434 | −56 | −0.140 | −0.200 | 0.125 | −12 | 0.060 | 0.260 | −0.184 |
| −99 | 0.040 | 0.120 | 0.434 | −55 | 0.050 | −0.150 | −0.493 | −11 | 00.100 | 0.100 | −0.493 |
| −98 | 0.100 | 0.220 | 0.743 | −54 | 0.070 | −0.080 | 0.279 | −10 | 40.070 | 0.030 | −0.029 |
| −97 | 0.040 | 0.260 | −0.338 | −53 | 0.020 | −0.0 | 0.897 | −9 | −0.0 | −0.0 | −0.029 |
| −96 | −0.230 | 0.030 | 0.125 | −52 | 0.000 | 00.060 | −0.647 | −8 | 0.120 | 0.060 | 1.515* |
| −95 | −0.040 | −0.010 | 0.279 | −51 | 0.020 | −0.040 | 0.588 | −7 | 0.130 | 0.130 | 0.279 |
| −94 | 0.170 | 0.160 | −1.265 | −50 | −0.040 | −0.080 | −0.029 | −6 | 00.100 | 0.100 | −0.647 |
| −93 | 0.020 | 0.180 | 0.897 | −49 | 0.060 | −0.020 | 0.279 | −5 | 0.120 | 0.120 | −0.493 |
| −92 | −0.020 | 0.160 | −0.493 | −48 | −0.020 | −0.040 | 0.279 | −4 | −0.020 | 0.100 | −1.265 |
| −91 | 0.020 | 0.180 | 1.260 | −47 | 0.050 | 0.010 | −0.338 | −3 | 00.0200 | 0.020 | 0.434 |
| −90 | −0.010 | 0.170 | −0.810 | −46 | −0.090 | −0.080 | −0.647 | −2 | −0.370 | −0.350 | −2.037** |
| −89 | 0.110 | 0.280 | 0.434 | −45 | −0.050 | −0.480 | −0.029 | −1 | −0.480 | −0.480 | −1.978** |
| −88 | 0.010 | 0.290 | 0.897 | −44 | 0.070 | −0.690 | 0.125 | 0 | −0.210 | −0.690 | −1.265 |
| −87 | 0.140 | 0.430 | −0.184 | −43 | −0.120 | −0.180 | −0.184 | 1 | −0.340 | −1.030 | −1.573* |
| −86 | −0.080 | 0.350 | −1.573* | −42 | 0.050 | −0.130 | −0.493 | 2 | 0.940 | −0.940 | 0.743 |
| −85 | 0.000 | 0.350 | 0.897 | −41 | −0.140 | −0.270 | −0.029 | 3 | 0.140 | −0.800 | 0.743 |
| −84 | 0.120 | 0.470 | 0.279 | −40 | 0.090 | −0.180 | 0.743 | 4 | −0.9400 | −0.940 | 0.125 |
| −83 | 0.060 | 0.530 | −0.184 | −39 | −0.060 | −0.240 | −0.830 | 5 | 0.110 | −0.830 | 0.279 |
| −82 | −0.190 | 0.340 | −1.573* | −38 | 0.020 | −0.220 | −0.184 | 6 | −0.840 | −0.840 | −0.184 |
| −81 | −0.090 | 0.250 | 0.279 | −37 | −0.060 | −0.280 | −2.037** | 7 | 0.130 | −0.710 | −0.029 |
| −80 | −0.270 | −0.020 | −1.573* | −36 | 0.080 | −0.200 | 0.125 | 8 | 0.080 | −0.630 | 0.434 |
| −79 | −0.050 | −0.070 | −0.338 | −35 | 0.320 | 0.120 | 1.669* | 9 | 0.380 | −0.250 | 1.051 |
| −78 | 0.230 | 0.160 | 0.897 | −34 | 0.170 | 0.290 | 1.36* | 170 | 0.070 | −0.180 | 1.594* |
| −77 | 0.020 | 0.180 | 0.125 | −33 | 0.120 | 0.410 | 1.823** | | | | |
| −76 | 0.000 | 0.180 | −1.882** | −32 | 0.17 | 0.58 | 2.132** | | | | |

single index model and 1% for the three factor model. This decline resulted from the significant negative average abnormal returns observed in the few days immediately prior to the incident. Both the average and the cumulative average residuals returned to normal immediately after the incident.

It is important to take a closer look at the behavior of the AR and CAR in the days immediately before and after an event date.

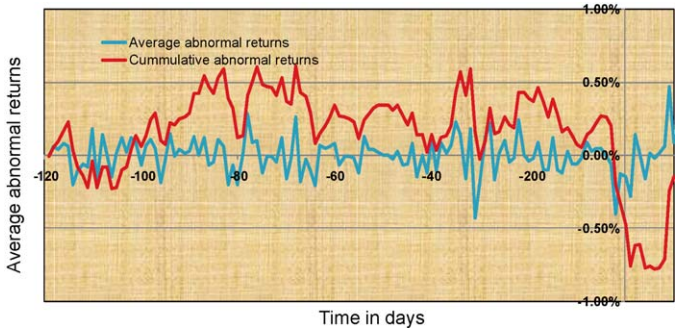


**Fig. 1.** Average abnormal returns and cumulative abnormal returns around the security Breach event using the single index market model (168 observations).

As the tables indicated, the only three statistically significant AR around the event were negative and they occurred two days (−2) and one day (−1) prior to the event and on the day (+1) following the announcement of the event. We further

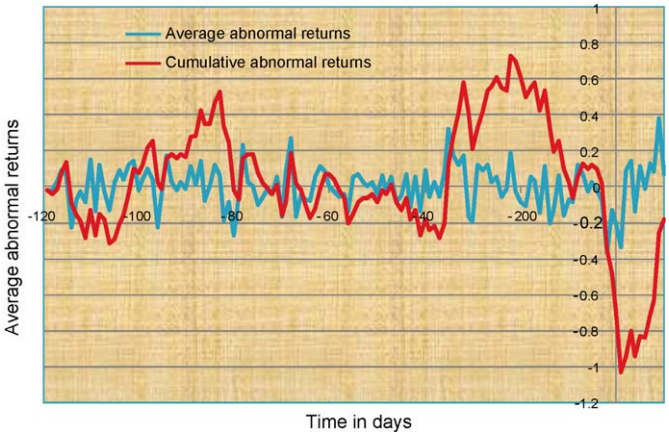


**Fig. 2.** Average abnormal returns and cumulative abnormal returns around the security Breach event using the three factor (FF) market model (168 observations).

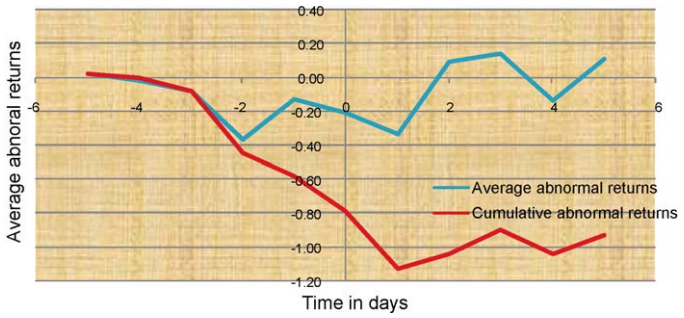


**Fig. 3.** Average abnormal returns and cumulative abnormal returns using three factor model five days prior and five days after security breach event date.

considered an event window of plus/minus five days around the event date. Fig. 3 graphs the pattern of both the AR and CAR that were estimated using the three factor Fama–French model results for five days prior and five days after the security breach event. There was a significant negative market reaction in the four days prior to the announcement that continued for two days after the event. The negative AR in the four days prior to the event date may indicate that the news of the security breach may have been leaking to the market before its official disclosure.

## 3. Summary and conclusions

Security breaches can have a significant impact on the financial performance of firms. With public disclosure laws in place, breaches of private information of clients can cause damage to the firms' reputation and lead to governmental sanctions. In our study, the impact of security breaches was measured by its impact on the firm's market value. The impact of security breach announcements on the market value of publicly traded firms was estimated using the standard event-study methodology. We found a statistically significant negative AR and CAR around the event date. The results from both the single index model and the three factor Fama–French model showed that in two of the three days prior to the security breach event; we observed negative and statistically significant abnormal returns. Moreover, both of the return-generating models used indicated that there was a negative effect on the returns of these firms on the day of the event with a highly significant negative impact occurring on the day following the incident. Our results indicated that, on average, the announcement of a security breach had a significant negative impact of about 1% of the market value of the firm. An important benefit of this research is to aid firms in balancing the costs of controls with the benefits of increased security. There are very few objective ways to compute the costs of security breaches. Using market valuations provides a credible and a quantifiable way of estimating the losses.

## Acknowledgements

We are grateful to Christopher Brown for assistance with data collection and analysis during the early stages of this research and to Laura Iwan, Anthony Saia, and Damira Pon for help with data collection efforts. We are also grateful to Edgar H. Sibley (editor) and three anonymous referees for valuable comments and insights. Finally, we would like to thank Uday Chandra for his help with WRDS and Eventus and the seminar participants at the International Forecasting Conference, New York City, NY, August 2007 for valuable comments and suggestions.

## Appendix A. Event-study methodology

There are three broad types of event studies; market efficiency (which evaluate how quickly and accurately financial markets react to information, such as earnings or merger announcements), information usefulness (which determines how security prices react to the information), and metric explanation (which uses cross-sectional regression to explain abnormal returns observed around the time of an event). Campbell et al. [3] suggest the following steps for event study analyses:

(1) Define a window of time around the event in which the stock price is monitored.
(2) Determine the selection criteria of firms in the study.
(3) Determine the model for computing the abnormal return.
(4) Design the testing framework for abnormal returns: define the null hypothesis, determine techniques for aggregating abnormal returns for individual firms, and select statistical tests for analyzing the data.
(5) Collect of data for analysis: Identify firms where event occurred and collect stock prices for the firms over the time period of analysis.

There are several essential procedures to be performed: first, its normal or expected return performance must be estimated. The market model used for estimating expected returns is a one-factor model that assumes a linear relationship between the return of the market portfolio and the individual security. Specifically, the estimated return for security $i$ is defined in Eq. (1) as:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \tag{1}$$

where $R_{it}$ is the return on security $i$ in period $t$ and $R_{mt}$ is the return on the market portfolio. $\varepsilon_{it}$ is the disturbance term with zero mean assumed to be independent and identically distributed, $\alpha_i$ is a measure of risk-adjusted performance, and $\beta_i$ is a measure of systematic risk.

In addition to estimating residuals from the single index market model, we also must estimate another set of residuals from the three factor Fama–French regression model:

$$R_t - R_t^{T\text{-}Bill} = \alpha + \beta_1 \cdot RMRF_t + \beta_2 \cdot SMB_t + \beta_3 \cdot HML_t + \varepsilon_t \tag{2}$$

where $R_t$ is the return on security $i$ in period $t$, $R_t^{T\text{-}Bill}$ is the return on the treasury-bill in month $t$, and $RMRF_t$, $SMB_t$, and $HML_t$ are the three-Fama–French factors that represent market return, small firm premium, and value firm premium, respectively.

Having estimated the expected return, abnormal returns can then be calculated by subtracting the normal return from the actual return as shown in Eq. (3):

$$AR_{it} = K_{it} - R_{it} \tag{3}$$

where $AR_{it}$ is the abnormal return on security $i$ in period $t$ and $K_{it}$ is the actual return on security $i$ in period $t$. We have chosen the length of the estimation window (119 days) to be sufficiently long so that, under the null hypothesis, the distribution of the sample abnormal returns of a given observation in the event window is:

$$AR_{it} \approx N(0, \sigma^2(AR_{it})) \tag{4}$$

The next step is to aggregate the abnormal returns through time. The cumulative abnormal return from period $t_1$ through $t_2$, is

defined as:

$$CAR_i(t_1, t_2) = \sum_{t=t_1}^{t=t_2} AR_{it} \quad (5)$$

The abnormal return observations must also be aggregated across observations of the event. If we assume that there is no clustering or overlap in the event window, the abnormal returns will be independent across securities, and can be aggregated for period t as:

$$\overline{AR_t} = \frac{1}{N}\sum_{i=1}^{N} AR_{it} \quad (6)$$

$$\mathrm{var}(\overline{AR_t}) = \frac{1}{N^2}\sum_{i=1}^{N} \sigma_{\tilde{\varepsilon}}^2 \quad (7)$$

Test statistic to test if the average abnormal return and the cumulative abnormal return are statistically different from zero is asymptotically normal with zero mean and unit variance.

Although the event study structure is relatively simple, some statistical issues need to be considered, especially when the event window is long more than a year. Long-horizon studies typically lack the ability to detect abnormal performance, and are sensitive with respect to the return generating process. However, short-horizon studies like tours, generally do not suffer from these serious limitations.

Other possible sources of bias that can impact event-study results include non-synchronous trading, thinly traded securities, and some liquidity aspects related to small capitalization stocks. Fortunately, our sample was mostly made up of large firms that are actively traded on major exchanges. The average market capitalization of the firms in our sample as of December 31, 2007 was $43.6 billion and the average Beta for firms in the sample was 1.18. Finally, the choice of the appropriate market index is critical. In our study we used both the standard market model as well as the Fama and French three factor model with the proxy for the market portfolio in both models being the CRSP market value weighted index provided by Kenneth French. Because our sample was composed of mostly large firms, it was important that a market wide and value weighted index be used to represent the market portfolio in the event study estimations.

## Appendix B. Sample of the firms/incidents used in the event study analysis

| SN. | Company name | CUSIP | Incident date[a] | Impact[b] | Incident details |
|---|---|---|---|---|---|
| 1 | H&R Block, Inc. | 093671105 | 1/2/2006 | 700 | 6 Stolen computers. Names, Social Security numbers, birthdates. |
| 2 | FedEx Corporation | 31428X106 | 2/4/2006 | 8500 | Inadvertently exposed W-2 forms that included tax information such as SSNs and salaries. |
| 3 | OfficeMax Inc. | 67622P101 | 2/9/2006 | ~200,000 | Hacking. Debit card accounts exposed involving bank and credit union accounts nationwide (including CitiBank, BofA, WaMu, Wells Fargo). |
| 4 | Honeywell International | 438516106 | 2/9/2006 | 19,000 | Exposed online. Personal information of current and former employees including Social Security numbers and bank account information posted on an Internet Web site. |
| 5 | MasterCard Inc. | 57636Q104 | 2/27/2006 | 2000 | Though MasterCard refused to say how the breach occurred, fraudsters stole the credit card details of holders in a major security breach. |
| 6 | Medco Health Solutions Inc. | 58405U102 | 3/1/2006 | 4,600 | Stolen laptop containing Social Security numbers for State of Ohio employees and their dependents, as well as their birth dates and, in some cases, prescription drug histories were exposed. |
| 7 | Verizon Communications Inc. | 92343V104 | 3/8/2006 | "Significant number" | 2 Stolen laptops containing employees' personal information including Social Security numbers were stolen/lost. |
| 8 | General Motors Corp. | 370442105 | 3/14/2006 | 100 | Dishonest insiders steal Social Security numbers of co-workers to perpetrate identity theft. |
| 9 | The Boeing Company | 097023105 | 3/21/2006 | 3,600 | A laptop was taken from a boeing human resources employee at Sea-Tac airport. It contained SSNs and other personal information, including personnel information from the 2000 acquisition of Hughes Space and Communications. |
| 10 | Aetna | 00817Y108 | 3/26/2006 | 38,000 | Laptop containing personal information including names, addresses and Social Security numbers of Department of Defense (35,253) and Omni Hotel employees (3000) was stolen from an Aetna employee's car. |
| 11 | Wells Fargo & Company | 949746101 | 5/5/2006 | Undisclosed | Computer containing names, addresses, Social Security numbers and mortgage loan deposit numbers of existing and prospective customers may have been stolen while being delivered from one bank facility to another. |
| 12 | M&T Bank | 55261F104 | 5/19/2006 | Undisclosed | Laptop computer, owned by PFPC, a third party company that provides record keeping services for M&T's Portfolio Architect accounts was stolen from a vehicle. The laptop contained clients' account numbers, Social Security numbers, last name and the first two letters of their first name. |

[a] Incident Date is when the incident was discovered and reported and may be different from when it actually occurred. In some cases the incident data and the report date are the same in other cases they are different but close. Incidents where reliable dates were not available were stricken from the data.

[b] Impact is defined in terms of the number of people impacted by the incident.

## Appendix C. List of companies used in analysis

(1) Abn Amro Holding NV—ADR
(2) Aetna Inc.
(3) Aflac Inc.
(4) Allstate Corp.
(5) Altria Group Inc.
(6) American Express Co.
(7) American Mortgage Acceptance
(8) Aramark Corp.
(9) AT&T Inc.
(10) Automatic Data Processing
(11) Avaya Inc.
(12) Bank of America Corp.
(13) Bear Stearns Companies Inc.
(14) Block H&R Inc.
(15) Blockbuster Inc.
(16) Boeing Co.
(17) Cablevision Sys Corp.—Cl A
(18) Chevron Corp.
(19) Choicepoint Inc.
(20) Circuit City Stores Inc.
(21) Citigroup Inc.
(22) Columbia Banking System Inc.
(23) Comcast Corp.
(24) Commerce Bancorp Inc./NJ
(25) Consolidated Edison Inc.
(26) CTS Corp.
(27) CVS Caremark Corp.
(28) Deb Shops Inc.
(29) Deutsche Bank AG
(30) Deutsche Telekom AG—ADR
(31) Diebold Inc.
(32) Disney (Walt) Company
(33) Disney (Walt) Internet Group
(34) Dnp Select Income Fund Inc.
(35) Eastman Kodak Company
(36) Electronic Data Systems Corp.
(37) Equifax Inc.
(38) Fedex Corp.
(39) First Horizon National Corp.
(40) Firstbank Corp.
(41) Forrester Research Inc.
(42) Franklin Templeton Ltd. Dur.
(43) Gap Inc.
(44) General Electric Co.
(45) General Motors Corp.
(46) Goldman Sachs Group Inc.
(47) Google Inc.
(48) Group 1 Automotive Inc.
(49) Gymboree Corp.
(50) Hartford Financial Services
(51) Hilb Rogal & Hobbs Co.
(52) Home Depot Inc.
(53) HSBC Finance Corp.
(54) HSBC Holdings Plc—ADR
(55) Humana Inc.
(56) ING Group NV—ADR
(57) Intl Business Machines Corp.
(58) JetBlue Airways Corp.
(59) JPMorgan Chase & Co.
(60) KB Home
(61) Kerzner International Ltd.
(62) Keycorp
(63) Koninklijke Ahold Nv—ADR
(64) Kraft Foods Inc.
(65) Laboratory Cp of Amer. Hldgs.
(66) M&T Bank Corp.
(67) Mckesson Corp.
(68) Medco Health Solutions Inc.
(69) Merrill Lynch & Co. Inc.
(70) Microsoft Corp.
(71) MoneyGram International Inc.
(72) Movie Gallery Inc.
(73) Nationwide Finl. Svcs.—CL A
(74) Nationwide Health Pptys Inc.
(75) Nelnet Inc.
(76) New York Times Co.—CL A
(77) Nissan Motor Co. Ltd.—ADR
(78) North Fork Bancorporation
(79) Paccar Inc.
(80) Papa Johns International Inc.
(81) Pfizer Inc.
(82) Piper Jaffray Cos. Inc.
(83) PNC Financial Svcs Group Inc
(84) Polo Ralph Lauren Cp—CL A
(85) Progressive Corp.—Ohio
(86) Prudential Financial Inc.
(87) Radioshack Corp.
(88) Rainbow Media Group
(89) Safeway Inc.
(90) Semtech Corp.
(91) SLM Corp.
(92) Sovereign Bancorp Inc.
(93) Starbucks Corp.
(94) Time Warner Inc.
(95) TJX Companies Inc.
(96) Toyota Motor Corp.—ADR
(97) Union Pacific Corp.
(98) Verisign Inc.
(99) Verizon Communications Inc.
(100) Verizon Inc./Nj
(101) Wachovia Corp.
(102) Wal-Mart Stores Inc.
(103) Wellpoint Inc.
(104) Wells Fargo & Co.
(105) Wesco Intl Inc.

## References

[1] A. Acquisti, A. Friedmann, R. Telang, Is there a cost to privacy breaches? An Event Study in: Proceedings of the Twenty Seventh International Conference on Information Systems and Workshop on the Economics of Information Security, Milwaukee, WI, December 10–13, 2006, pp. 1–23.
[2] K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security 11 (3), 2003, pp. 431–448.
[3] J. Campbell, A. Lo, A.C. MacKinlay, The Econometrics of Financial Markets, Princeton University Press, Princeton, NJ, 1997, pp. 1–632.
[4] H. Cavusoglu, B. Mishra, S. Raghunathan, 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), 2004, pp. 70–104.
[5] L.A. Gordon, M.P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security 5 (4), 2002, pp. 438–457.
[6] A. Hovav, J. D'Arcy, Capital Market Reaction to defective IT products: the case of computer viruses, Computers & Security 24 (5), 2005, pp. 409–424.
[7] A. Hovav, J. D'Arcy, The impact of virus attack announcements on the market value of firms, Information Systems Security 13 (3), 2004, pp. 32–40.
[8] A. Kotulic, J.G. Clark, Why there aren't more information security research studies, Information and Management 41, 2004, pp. 597–607.
[9] B. Suh, I. Han, The IS risk analysis based on a business model, Information and Management 41, 2003, pp. 149–158.
[10] R. Telang, S. Wattel, An empirical analysis of the impact of software vulnerability announcements on firm stock price, IEEE Transactions on Software Engineering 33 (8), 2007, pp. 544–557.
[11] Q. Yeh, A.J. Chang, Threats and countermeasures for information system security: a cross-industry study, Information and Management 44 (5), 2007, pp. 480–491.

**Sanjay Goel** is an associate professor in the School of Business and the director of research at the NYS Center for Information Forensics and Assurance at UAlbany. He represents UAlbany in the Capital Region Cyber Crime Partnership. Dr. Goel received his PhD in mechanical engineering from RPI. His research includes information security, risk analysis, security policies, information classification, and self-organization in complex systems. He and his team have worked with CSCIC in developing the information classification policy for New York. He won the promising Inventor's Award in 2005 from the SUNY Research Foundation. In 2006, he was awarded the SUNY Chancellor's Award for Excellence in Teaching, the UAlbany Excellence in Teaching Award, and the Graduate Student Organization Award for Faculty Mentoring. He was named one of the three AT&T Industrial Ecology Faculty Fellows for 2009–2010. He has received grants and funding from NIJ, NSF, UTRC, NYSERDA, US Department of Education, and CSCIC.

**Hany A. Shawky** is professor of finance and former director of the Center for Institutional Investment Management (CIIM) at the University at Albany School of Business. Widely published on asset pricing, stock market behavior, and international financial markets, he has served as a consultant to many private and public organizations. Shawky teaches corporate finance, investment analysis, and portfolio management. He received his doctorate in finance (1978) from Ohio State University.