December 2006

The Economic Impact of Information Security Breaches: Firm Value and Intra-industry Effects

Kregg Aytes  
*Idaho State University*

Steve Byers  
*Idaho State University*

Mukunthan Santhanakrishnan  
*Idaho State University*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2006](http://aisel.aisnet.org/amcis2006)

**Recommended Citation**  
[http://aisel.aisnet.org/amcis2006/399](http://aisel.aisnet.org/amcis2006/399)

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
The Economic Impact of Information Security Breaches: Firm Value and Intra-industry Effects

Kregg Aytes
Idaho State University
aytekreg@isu.edu

Steve Byers
Idaho State University
byerstev@isu.edu

Mukunthan Santhanakrishnan
Idaho State University
santmuku@isu.edu

ABSTRACT

IT managers often struggle to justify investments in information security. In addition to standard quantitative analyses such as Return on Security Investment (ROSI), executive management may also want to know what the effect of potential security breaches would be on the market value of a publicly-traded firm. This study attempts to shed light on the issue by examining the impact of information security breach announcements on shareholder value. This study also examines the effects of such announcements on a portfolio of the firm’s competitors in an effort to examine the contagion and competitive intra-industry effects. We find that the market value of an affected firm’s competitors increases following the announcement of a security breach, consistent with the competitive model of intra-industry effects. The magnitude of the competitive effect appears to depend on the nature of the security breach. The increase in competitor value is higher when the security breach involves non-confidential firm and customer information. When the security breach involves confidential data, the announcement return is negative and significant (both economically and statistically), providing IT management with additional support for seeking funds to avoid such security events.

Keywords: Security, event analysis, investment

INTRODUCTION

On October 9, 2005, Bank of America announced that they had notified users of the Visa Buxx prepaid debit card, a product targeted to teenagers, that their personal information may have been compromised as a result of the theft of an unencrypted laptop computer. In a letter sent to card users, the bank warned customers that their bank accounts, routing transit numbers, names, and credit card numbers were all subject to the security breach caused by the theft. In the two trading days following this announcement the stock price of Bank of America fell by almost 1 percent. This type of information security breach announcement is not unusual, nor is the market’s reaction to the announcement. Previous researchers have found evidence that the announcement of information security breaches have an impact on the market value of a firm. In this paper we confirm these results using enhanced data, and we add to the literature by examining the impact of a company’s security breach on its competitors.

Information security personnel continually face the need to justify security expenditures to management. Typically, information security best practices include a recommendation to conduct a cost-benefit analysis. Such an analysis often requires one to determine the annualized loss expectancy (ALE) or Return on Security Investment (ROSI) of various security events by determining or estimating various components of assets, vulnerabilities, threats, and the costs of countermeasures. While these are valid, quantitative techniques, they are based on estimated costs and probabilities. It may be difficult to convince management to spend significant amounts of money based on such estimates, particularly when even the best information security, by itself, does not result in increased revenues or profits. Standard quantitative tools, such as Return on Investment, are somewhat lacking when applied to investments in security (Gordon and Loeb, 2002; Ramachandran and White, 2004).
On the other hand, management of publicly held firms is generally sensitive to events that affect a firm’s market value or the value of its competitors. Telang and Wattal (2005) find that announcements of vulnerabilities in vendor-provided software adversely affect the stock price of the vendor companies. There is some evidence that certain types of information security events affect a firm’s stock price. One way to categorize security breaches is by separating those events that result in a loss of confidential data, such as intellectual property or customer data (e.g., credit card information) from non-confidential events, such as denial-of-service attacks. Campbell et. al. (2003) examine the stock price reaction to announcements of information security breaches. They find that, on average, firms announcing breaches involving confidential firm and customer information experience a significantly negative stock market return.

Interestingly, they do not find a significant market reaction when the security breaches do not involve confidential information (e.g., denial-of-service attacks), suggesting that the stock market discriminates based on the type of security breach. We have undertaken a study to extend that study to include more recent events and to investigate how publicly reported security events affect the market value of competitors of the affected firm.

We expand on the existing literature on the shareholder effects of security breaches in two ways. Starting with the sample of 43 events from 1995 – 2000 in the study by Campbell et. al., we add more recent security announcements for the subsequent 5-year period (2001-2005). In addition to adding more recent events to the sample, the larger sample size increases the power of the significance tests. However, the major contribution of this paper is the examination of intra-industry effects of a security breach announcement.

There are three possible scenarios for the market reaction of an affected firm’s competitors. One is that there is no effect on competitors’ stock prices, i.e. the market assigns neither a benefit nor a cost to the firms based on the security breach by a firm in the industry. The second possible effect is that when a firm announces an information security breach the firm’s competitors are positively affected. We will call this a “competitive” effect because the competitors benefit from the affected firm’s misfortune. The third possibility is that the competitors are harmed by a firm’s announcement of a security breach in what we call a “contagion” effect. In this scenario investors believe that a reported breach may affect other firms in the industry. Our treatment of these scenarios for intra-industry effects is similar to the examination of such effects for bankruptcy announcements by Lang & Stulz (1992).

Based on our sample of 67 information security breaches for the period 1995-2005, we find that, on average, a firm’s competitors benefit when the firm announces a security breach. The evidence is consistent with the competitive model of intra-industry effects. The magnitude of the benefit is both economically and statistically significant. On average, the market value of competitors increases by 0.8% over the five-day event window. The stock price increase for competitors is larger (0.88%) when the event involves non-confidential information than for confidential events (0.70%). For the affected firms themselves, our study confirms the evidence from prior research. We find that, on average, the announcement of an information security breach results in a negative (but statistically insignificant) shareholder return for the overall sample and for a subsample of events involving non-confidential firm and customer data. When the security breach involves confidential data, the announcement return is negative and significant (both economically and statistically).

**HYPOTHESIS DEVELOPMENT**

Campbell et al (2003) discuss three possibilities for the stock market reaction to a security breach. The first prediction is that such an announcement is bad news, negatively affect the firm’s cash flows and therefore lowering the market value. The negative effects derive from the explicit costs of dealing with the security breach as well as the implicit costs of potential lost business and legal liability. A competing argument is that security breaches are to be expected and are simply a cost of doing business. In this case the there would be no abnormal stock return when the breach is announced. Finally, there is the possibility that the net economic effect is positive as a result of expected investments in information security resulting from the breach. The first hypothesis tested is the market reaction to an information security breach on the market value of the firm itself without a prediction about direction.

**H1**: There is no stock market reaction to public reports of an information security breach

Following Campbell et al we break the sample into security breaches involving confidential information and non-confidential information. Confidential information would include things like customer information, account numbers, etc. Non-confidential events include denial-of-service and virus attacks.

**H2**: There is no stock market reaction to public reports of an information security breach involving access to confidential information

**H3**: There is no stock market reaction to public reports of an information security breach that does not involve access to confidential information
The primary thrust of the paper involves examining the market value effects on the affected firm’s competitors. The null hypothesis is that there is no market reaction by competitors in response to an information security breach by a firm in their industry. Empirically, this would be demonstrated by the lack of an abnormal return for a portfolio of competitors during the event window.

Alternatively, a firm’s security breach could be bad news or good news for the industry. If the market views a security breach announcement by one firm in an industry as a signal about the vulnerability of other firms to a similar breach, we would expect the stock returns to fall for the industry. This would be the contagion effect. Empirically, this would be reflected by negative abnormal returns for the industry portfolio. On the other hand, competitors could benefit from the misfortunes of an affected firm. Customers may be expected to view the affected firm as too risky and shift their business to the competitors. The present value of such competitive effects would be reflected in positive abnormal returns to the industry portfolio, reflecting the dominance of the competitive effect.

**H3a:** there is no market reaction by competitors in response to an information security breach by a firm in their industry

Once again, we divide the sample into events involving confidential and non-confidential information, examining the effects on competitors for these subsamples.

**H4a:** there is no market reaction by competitors in response to an information security breach by a firm in their industry involving access to confidential information

**H4b:** there is no market reaction by competitors in response to an information security breach by a firm in their industry that does not involve access to confidential information

**METHODOLOGY**

**Research Design**

We use event study methodology to measure the effects of security breach announcements on the value of firms. This technique has a long history in the economics, accounting, and finance literatures (MacKinlay (1997)). It is also frequently used in other disciplines such as IT (e.g. Dos Santos et al (1993) and Chaterjee et al (2001)). Event studies measure the impact of a specific event, in this case an information security breach, on the market value of a firm. The basic technique is to examine the reaction of a firm’s stock price during the trading days surrounding an event (the ‘event window’) and compare the return to the expected return during the window. The difference between the actual return and the expected return is the abnormal return attributable to the event. The details of determining the expected return are described in a later section.

We examine two distinct economic effects of information security breach announcements: the effect on the firm with the security breach, and the effect on a portfolio of the firm’s competitors. The effect on the firm has been examined before (Campbell et al (2003)). We reexamine these effects using a more robust set of data that was unavailable to prior researchers simply because these types of security breaches are relatively recent phenomena and so every year that passes provides significantly more data.

The major contribution of this paper is the examination of the effects on competitors. We structure the possible industry reaction to a security breach similar to the way Lang & Stulz (1992) looked at competitive reactions to bankruptcy announcements: i.e. we observe whether the industry responds in a way consistent with contagion or competition.

**Sample Selection**

We expand the sample of security breaches examined in Campbell et al (2003), by following their approach of searching for specific terms (such as “information security breach”, computer system security” etc) in Lexis Nexis Academic Search. Lexis Nexis covers news sources such as leading newspapers (including the New York Times, Washington Post, USA Today etc.), business magazines (such as Business Week, Economist etc) and News Wires (including Business Wire, PR Newswire). The Lexis Nexis’s vast and broad range of news sources enables us to identify any reported security breach event that is likely to have any measurable impact on the value of the company.

Campbell et al (2003) search for information security breaches covers the period from January 1995 to December 000. We expand on their sample period till 2005, resulting in identification of a total of 67 security breaches from 1995 to 2005. Table 1 provides a yearly distribution of the sample. The increase in reporting of security breaches in 2005 may be a result of a recent regulatory change in California, which requires reporting of events that may involve loss of confidential consumer
data. We also find that all but three events in the new period are events where security of confidential data may have been compromised. The distribution of the sample in Table 2 suggests that security breaches happen more often in business services industry (two digit SIC code: 73) and banking/financial services industries (SIC code: 60-67). This is possibly due to the fact that operations of companies in these industries are more information oriented than other industries. The sample also consists of companies in the manufacturing sector (SIC code 30-38), transportation (SIC code 40-48) and retail (SIC code 53-59). The sample is fairly evenly distributed between events resulting in loss of confidential data (31) and events that did not result in data loss (36).

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>2</td>
</tr>
<tr>
<td>1998</td>
<td>4</td>
</tr>
<tr>
<td>1999</td>
<td>13</td>
</tr>
<tr>
<td>2000</td>
<td>26</td>
</tr>
<tr>
<td>2003</td>
<td>3</td>
</tr>
<tr>
<td>2004</td>
<td>5</td>
</tr>
<tr>
<td>2005</td>
<td>14</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>67</strong></td>
</tr>
</tbody>
</table>

Table 1: Distribution of events by year

<table>
<thead>
<tr>
<th>2 digit SIC Code</th>
<th>Industry description</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>Apparel and other textile products</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>Printing and publishing</td>
<td>2</td>
</tr>
<tr>
<td>28</td>
<td>Chemicals and allied products</td>
<td>2</td>
</tr>
<tr>
<td>30</td>
<td>Rubber and miscellaneous plastics products</td>
<td>1</td>
</tr>
<tr>
<td>35</td>
<td>Industrial machinery and equipment</td>
<td>3</td>
</tr>
<tr>
<td>36</td>
<td>Electrical and electronic equipment</td>
<td>1</td>
</tr>
<tr>
<td>37</td>
<td>Transportation equipment</td>
<td>4</td>
</tr>
<tr>
<td>38</td>
<td>Instruments and related products</td>
<td>1</td>
</tr>
<tr>
<td>45</td>
<td>Transportation by air</td>
<td>2</td>
</tr>
<tr>
<td>48</td>
<td>Communications</td>
<td>2</td>
</tr>
<tr>
<td>53</td>
<td>General merchandise stores</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>Apparel and accessory stores</td>
<td>1</td>
</tr>
<tr>
<td>59</td>
<td>Miscellaneous retail</td>
<td>3</td>
</tr>
<tr>
<td>60</td>
<td>Depository institutions</td>
<td>9</td>
</tr>
<tr>
<td>61</td>
<td>Nondepository credit institutions</td>
<td>1</td>
</tr>
<tr>
<td>62</td>
<td>Security, commodity brokers, and services</td>
<td>5</td>
</tr>
<tr>
<td>63</td>
<td>Insurance carriers</td>
<td>1</td>
</tr>
<tr>
<td>64</td>
<td>Insurance agents, brokers, and service</td>
<td>1</td>
</tr>
<tr>
<td>67</td>
<td>Holding and other investment offices</td>
<td>2</td>
</tr>
<tr>
<td>73</td>
<td>Business services</td>
<td>18</td>
</tr>
<tr>
<td>78</td>
<td>Motion pictures</td>
<td>5</td>
</tr>
<tr>
<td>99</td>
<td>Diversified conglomerates</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>67</strong></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Distribution by industry

Identification of Competitors

The competitors of sample firms is defined as all other companies with the same four digit Compustat Standard Industry classification (SIC) code with daily stock returns available in the Center of Research in Security Prices (CRSP) database. This results in 9499 industry peers. Since the industry-matched rival firms have a common event date, the returns are
potentially correlated, which may result in biased statistical significance tests. To overcome this problem and compute the
effect of the sample companies’ security breach on the value of the common equity of their industry peers, we form 67
contemporaneous equally weighted portfolios consisting of all firms with daily stock returns and the same Compustat
primary four-digit SIC code as the sample firms\(^1\).

\[
\text{Variable} & \quad \text{Mean} & \text{Median} & \text{Minimum} & \text{Maximum} & \text{Std. Dev} \\
\hline
\text{Total Assets} & 163878 & 5248 & 10 & 1484101 & 362593 \\
\text{Net Sales} & 20817 & 5520 & 1 & 162558 & 31861 \\
\text{Net Income} & 2578 & 332 & -2743 & 17046 & 4528 \\
\text{Market Value of Equity} & 69655 & 12061 & 13 & 596476 & 119844 \\
\text{Market/Book Value of Equity} & 16 & 5 & -57 & 219 & 40 \\
\hline
\end{array}
\]

**Table 3: Sample Firm Characteristics**

\[
\text{Variable} & \quad \text{Mean} & \text{Median} & \text{Minimum} & \text{Maximum} & \text{Std. Dev} \\
\hline
\text{Total Assets} & 11772 & 340 & 0 & 1276778 & 81732 \\
\text{Net Sales} & 1190 & 57 & 0 & 174694 & 6480 \\
\text{Net Income} & 125 & 4 & -2743 & 14143 & 766 \\
\text{Market Value of Equity} & 3069 & 204 & 0 & 596476 & 15969 \\
\text{Market/Book Value of Equity} & 9 & 3 & -1503 & 19224 & 290 \\
\hline
\end{array}
\]

**Table 4: Industry Portfolio Characteristics**

**Event Study Methodology**

Event Study methodology has been used by social scientists studying the impact of a particular event on the value of
companies\(^2\). The usefulness of this methodology rests in the rationality in the financial markets and hence the expectation that
the effects of any significant event will be reflected immediately in security prices. Appraisal of the security breach’s impact
requires a measure of abnormal return. The abnormal return is the actual stock return (observed after the event) minus the
normal stock return over the event window. The normal return in our study is estimated in a time period when the security
breach would not have impacted the return (day -31 to -151 relative the event date)\(^3\). To estimate a firm’s ‘normal’ return we
use a statistical model which relates the return of any stock’s return to the market portfolio. The model we use is the market
model, the most common model used in estimating the expected return (MacKinlay (1997)). Therefore, the normal return on
any stock is estimated using the following model in the estimation period.

\[
R_{it} = \alpha_i + \beta_i R_{mt} + \epsilon_{it}
\]

where \(R_{it}\) and \(R_{mt}\) are return on stock \(i\) and the market portfolio at time period \(t\).

We use the NYSE/AMEX/NASDAQ value weighted index as the proxy for the market portfolio and estimate \(\alpha_i, \beta_i\) and \(\epsilon_{it}\), the parameters of the market model during the estimation period (day -166 to day -46). Based on the estimates of the market
model, we are able to compute the abnormal returns for the event period as follows:

\[
AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt})
\]

\(^1\) This procedure to control for contemporaneous cross-sectional correlation is described in detail by Jaffe (1974). This
technique has also been used by Herzel (1991) and Lang and Stulz (1992) in their respective studies examining the intra-
industry effects of self-tender offers and bankruptcy announcements respectively.

\(^2\) For a more detailed review of this technique, refer Mackinlay (1997).

\(^3\) We chose this period in order to have a long enough estimation period that will be untainted by the security breach event.
The results are robust to varying the estimation period.
The abnormal return AR represents how the return on the sample firms is different from the expected return around the security breach event. Since the security breach event is seldom reported immediately after the actual occurrence of the security breach, it is possible that some market participants become aware of the event ahead of the reporting in major news sources. Hence, we use a window of two days before to two days after the report (signified as (-2, +2)) of the event. The cumulative abnormal return is the sum of the abnormal return during the five day event window. We compute the mean cumulative abnormal return as the average of cumulative abnormal returns of sample companies during the event window.

Following a similar procedure, we estimate the cumulative abnormal return for the industry portfolio. Specifically, for each sample company, we estimate the cumulative abnormal return for each of the industry peers and compute the average return for the industry portfolio during the event window. This represents the return on the portfolio of industry peers, which deviates from its normal return right around the security breach event and hence is expected to capture the impact of the event on the industry portfolio. Finally, we compute the mean portfolio return as the average of cumulative abnormal returns of industry portfolios during the event window. To protect against possible confounding events that would contribute to abnormal returns for the selected firms, Lexis Nexis was again searched for significant events during the event window time period. No confounding events were found.

RESULTS

Based on our sample of 67 information security breaches for the period 1995-2005, we find that, on average, the announcement of an information security breach results in a negative (but statistically insignificant) shareholder return for the overall sample (See Table 5) and for a sub-sample of events involving non-confidential firm and customer data. We are not able to reject the H1 and H2B null hypotheses of no stock market reaction. However, when the security breach involves confidential data (H2A), the announcement return is negative and significant (both economically and statistically). These results are consistent with the results of Campbell et al (2003).

<table>
<thead>
<tr>
<th></th>
<th>N</th>
<th>Mean CAR</th>
<th>Z-stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Sample</td>
<td>67</td>
<td>-0.20%</td>
<td>-0.632</td>
</tr>
<tr>
<td>Panel B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non Confidential Events</td>
<td>36</td>
<td>1.22%</td>
<td>0.981</td>
</tr>
<tr>
<td>Confidential Events</td>
<td>31</td>
<td>-1.85%*</td>
<td>-1.986</td>
</tr>
</tbody>
</table>

Table 5: Cumulative Abnormal Returns for Sample events

* significant at the .05 level  
** significant at the .01 level  
*** significant at the .001 level

The cumulative abnormal returns for the 67 sample events are obtained using a market model for the event window (-2, +2). The value weighted index is used as the proxy for the market portfolio and normal return is estimated during the period (-46, -165) relative to each event.

The significant contribution of this paper is to address the question: How do these events impact the competitors of companies that are directly affected. On the one hand, these results may cast a shadow on all companies in the industry and negatively impact their results (contagion effect). At the same time, it is plausible that these security breaches drive customers towards other companies in the industry and improve the stock performance. On average, we find that the market value of competitors increases by 0.79% over the five-day event window (See Table 6). We are therefore able to reject the H3 null hypothesis for no stock market reaction. Further, results also indicate that the market distinguishes between security breaches based on whether confidential firm and customer information is involved. The stock price increase for competitors is larger (0.88%) when the event involves non-confidential information (H4B) than for confidential events (0.70%) (Hypothesis H4A). The magnitude of the benefit is both economically and statistically significant (at the 1% and 5% level respectively).

---

4 We find similar results for other choices for the event window such as (-1,1) and (-1,5).
The cumulative abnormal returns for the 67 sample events are obtained using a market model for the event window (-2, +2). The value weighted index is used as the proxy for the market portfolio and normal return is estimated during the period (-46, -165) relative to each event.

These results imply that security breaches are associated with the competitive model of intra-industry effects. In other words, the evidence suggests that security breaches influence the competitive positions of companies within industries by potentially making the competitor appear as a better option to their customers.

DISCUSSION

In the competitive environment of publicly-held companies, any event that results in either a reduction in a firm’s market value or an increase in the value of the firm’s competitors will be viewed negatively by management. To avoid these negative effects, firms would probably choose not to announce security breaches. However, California enacted a new law in July of 2003 that requires a company to disclose publicly any computer security breaches that involve the personal information of a California resident. Because of the large population of California and the subsequent actions in other states, this requirement has become a de facto national law in the United States. The result is that “confidential events,” as we have called them, will have to be announced to the public. Our research indicates that these types of events have a negative effect on firm market value and a positive effect on the value of a firm’s competitors.

For IT and information security managers, this provides added leverage when seeking funding for information security. On average, firms that announced a confidential security breach saw their market value drop by 1.85% in the five days surrounding the announcement relative to what was expected (based on overall market returns). For a large firm such as the Bank of America, this is a loss of $3.38 billion in market capitalization at its current valuation. At the same time, the market capitalization of an announcing firm’s competitors increased by 0.7%, relative to their normal expected return. An economic impact of such magnitude is likely to garner attention by executive management.

CONCLUSION, LIMITATIONS, AND FURTHER RESEARCH

This research attempts to extend, both in time and perspective, earlier investigation into the market effects of publicly announced security events. When firms experience the loss or exposure of confidential data, they suffer market value losses compared to their competitors. While this result is applicable only to publicly-traded firms, it indicates that there is value in avoiding security breaches.

Studying security events in this fashion is complex due to the nature in which security breaches become known. Unlike many event studies that investigate such things as the announcements of mergers, changes in executive management, etc., firms often do not want security events to be publicized. Even after the California law requiring notification of customers when their data was compromised came into effect, firms do not always issue press releases after such events. Instead, the breach becomes widely known after the company sends letters to its customers, and then the media begins to report that such letters were sent. This introduces several lags in the timeline of the event. First, it may take the firm a period of weeks or even months before it discovers a breach has occurred. Second, it takes time to determine which customers need to be notified and then to send out the official letters of notification. Third, a delay occurs before the media finds out that the letters are being received by customers. Each of these delays “muddies” the event window and reduces the statistical power of the analysis.

Future research should include a finer-grained perspective on security breach announcements. We utilized two broad categories: events resulting in the loss of confidential data and those that did not result in confidential data loss. However,
there are many types of occurrences that may have different effects on the market, such as internal versus external perpetrators, intentional theft versus accidental loss, and the magnitude (number of records/individuals effected) of the event. It is possible that the market would view each type of event somewhat differently. As the number of announced events increases over time, such finer-grained analysis will become possible.

REFERENCES


