The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers

Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan
huseyin@utdallas.edu, bmishra@utdallas.edu, sraghu@utdallas.edu
The University of Texas at Dallas
School of Management

February 2002

Abstract

Assessing the value of information technology (IT) security investments by firms is a challenging task because of difficulties in the measurement of tangible and intangible benefits. Event study methodology that uses market valuations is a widely used in these cases. We employ the event study methodology to assess the impact of Internet security breaches on the market value of the breached firms. We also study the information transfer effect of security breaches, namely the effect of security breaches of other firms on market values of firms that develop security technology. The results of our study show that the announcement of Internet security breach is negatively associated with the market value of the announcing firm. Compromised firms, on average, lose approximately 2.1% of their market values within two days surrounding the events. This translates into $ 1.65 billion average loss in market capitalization per incident. We find that firm type, firm size, and time are important factors that explain the cross-sectional variations in abnormal returns. Our results also show that the effects of security breaches are not restricted to breached firms. The market values of security developers are positively associated with the disclosure of security breaches by other firms. Each security developer, on average, gains 1.36 % more than normal gain expected by market model. This translates into, on average, a total gain of $ 1.06 billion per security firm over a two-day period.

1. Introduction

The number of companies conducting business over the Internet has been rapidly increasing. However, this massive growth of e-business has not been an unmitigated boon. Open access nature of the Internet that facilitates easy exchange of information, goods, and services also presents the biggest impediment in the form of security. The interconnectivity in a network is extremely susceptible to security breaches. A recent survey by CSI/FBI (2002) found that the Internet was the point of attack in 74% of hacking incidents in 2002, up from 38% in 1996 (Power 2002).

Public attention about security breaches increased dramatically when high profile companies like Amazon.com, Ebay, and Yahoo were hit by Denial-Of-Service (DOS) attacks in February 2000. A number of high-profile computer worms and viruses, such as Code Red, Nimda, and I Love You, also heightened the awareness. Firms have also increased their emphasis on security as illustrated by the following quote from a recent memo issued by Bill Gates to Microsoft's employees: *"(the new emphasis is) more important than any other part of our work. If we don't do this, people simply won't be willing -- or able -- to take advantage of all the other great work we do. When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box.*"

While more firms have realized the importance of security, the assessment of the value of security has proved to be challenging. Information security should be viewed as a value creator that supports and enables e-business, rather than simply as a cost of doing business. A secure environment for information and transaction flow can create value for the organization as well as its partners and customers. In the same token, security breaches can lead to breach of consumer confidence and trust in addition to lost business and third party liability. In a recent survey by Media Metrix only 12.1 percent of U.S companies with a web presence cite direct financial loss as a concern in a security breach while more than 40 cite consumer trust and confidence (Pastore 2001). The true cost of security breaches is multifaceted. A direct way of measuring these costs seems quite difficult though an indirect estimate is possible by analyzing the effects of security breaches on market values of firms.

To the best of our knowledge ours is the first large-scale study on security breaches on capital markets. Our study differs from the two earlier studies; Ettredge and Richardson (2001) and Bharadwaj and Keil (2001) in the following respects. First, we consider all types of security incidents and do not restrict only to DOS attacks. This allows us to study the differential effects of DOS versus other types of attacks. Second, our focus is only on security breaches whereas Bharadwaj and Keil (2001) included security breach as one of several types of IT failures. Consequently, we provide more specific insights on the impact of IT security failures. Third, contrary to Ettredge and Richardson (2001), we analyze the impact of security breaches using data over the period 1995-2001 rather than just the February 2000 incident. We use this incident to study the differential effects of security breach announcements on the capital markets in pre and post February 2000 periods. Futhermore, the two earlier studies analyzed the impact on only firms that deploy security technology. We analyze the effect of security breaches both on the firms attacked as well as on firms that develop the technology.

We found that the announcements of Internet security breaches were negatively associated with the market value of announcing firms. Compromised firms, on average, had a ***negative*** abnormal return of approximately 2.1% within two days surrounding the events. The effects of security breaches were not restricted to breached firms. The market values of security technology firms were positively associated with the disclosure of security breaches by other firms. Each security developer, on average, had a ***positive*** abnormal return of 1.36 %. Our study shows that breached firms pay a heavy price for the lack of adequate security but security developers benefit immensely from breaches on other firms.

2. Development of Hypotheses

2.1. Impact of Security Breaches on Market Value of the Breached Firm

The relationship between IT security and market valuations can be traced to the trust placed by customers and partners who do business with the firm through the Internet. Customer and partner's trust assumes more significance in e-business because of concerns related to data privacy. They may be unwilling to transact business with sites that are perceived to be insecure. A security breach can irrevocably damage the trust and confidence required to build a long-term relationship with the customer and partners. In the Internet era characterized by high competition and low loyalty, dissatisfied customers can switch to competitors that are just a click away. Thus, a perception of low security can have a profound financial impact on the firm. Security problems may also signal to the market a lack of concern for customer privacy and/or poor security practices within the firm. These signals in turn lead investors to question the long-term performance of the firm. In efficient capital markets investors are believed to revise their expectations based on new information in announcements. Investor expectations are reflected in stock prices. If security breaches are expected to reduce future cash flows, capital markets would respond unfavorably to announcements of security breaches by driving stock prices down (Fama 1991). These arguments lead to our first hypothesis as follows.

HYPOTHESIS 1 **(H1): Announcement of Internet security breach in a firm is negatively associated with its abnormal stock market return.**

2.2. The Determinants of Abnormal Stock Returns

2.2.1. Firm Type

Firms on the Internet are typically grouped into two categories: *conventional* firms and *net* firms. The conventional firms, both *brick-and-mortar* and *click-and-mortar* firms, conduct business in traditional channel. Brick-and-mortar firms, such as Coca-Cola, use Internet as a marketing channel to communicate with their customers if not to sell products. Click-and-mortar firms, like Barnes and Noble, use the Internet as a new channel to sell their products. The second group of firms on the Internet is called *pure-play* or *internet-only* companies. This group includes firms like Amazon.com and eBay.com that rely purely on Internet channel to sell their products and services.

Although a security breach can damage the reputation of a firm of any type, the damage can be much more severe for net firms. These firms depend solely on the Internet for their survival. Information security is not just insurance, rather an essential ingredient for their success. Outages due to denial-of-service attacks mean lost revenues and lost opportunities because customers cannot make their intended purchases. Confidentiality and integrity of data are also more critical for the net firms.

In comparison to net firms, conventional firms are relatively less affected by security breaches on the Internet. If they are using the Internet simply to provide information to public, the security breach on their web sites will be less damaging. Even if they conduct business over the Internet a DOS attack will not stop them completely from doing business. For example, if Barnes and Noble site is down due to a security problem, it can continue to sell books through its physical stores. However that is not true for Amazon. Based on the above arguments we expect to see more severe reactions to security breaches for net firms. We state our second hypothesis in alternate form as follows.

HYPOTHESIS 2 (H2): Other things being equal, the abnormal (negative) stock market return due to Internet security breaches is larger for net firms.

2.2.2. Firm Size

Large firms are likely to better absorb negative economic and financial shocks than small firms due to greater access to capital markets, lower cost of capital, multiple sources of income, diversified product markets, and trusted brand names. Large firms are likely to better deal with security breaches than small firms. Large organizations may have more capital to work with. They may have more slack resource to be used in case of a security breach than small firms, such as backup web servers. Also, they may have more skillful IT personnel than small firms. We believe that these differences result in asymmetries in impact of security breaches. We hypothesize that (negative) abnormal return around the security breach is negatively related to firm size.

HYPOTHESIS 3 (H3): Other things being equal, the abnormal (negative) stock market return due to Internet security breach is larger for smaller firms.

2.2.3 Nature of Attack

One can argue that availability is the most critical security issue on the Internet, especially for e-commerce services[1]. As mentioned earlier, if the site is not available, revenue is lost resulting in a direct hit to the bottom line. However DOS attacks have relatively brief durations and they do not destroy data. While obviously disruptive, attacks against availability only affect site accessibility--making them less damaging than other forms of attacks, such as a virus that destroys, manipulates, or exposes programs and sensitive information on a wide scale. Therefore in a DOS attack firms are not exposed to huge third party

[1] CloudNine Communications, one of Britain's oldest Internet Service Providers (ISPs) went out of business because the network was down for a too long time after the DOS attack (Warner 2002).

liability associated with breach of privacy and unauthorized leak of customer or partner information. Hence, it is difficult to say if the capital markets consider the availability breaches more seriously than other type of breaches. Thus we do not hypothesize a directional result in our next hypothesis.

***HYPOTHESIS* 4 (H4): Other things being equal, the abnormal (negative) stock market returns due to Internet security breaches are different between availability and other type of breaches.**

2.2.4. Time

The attention paid by firms and investors to security on the Internet has increased over time. In the early days of the Internet there were few incidents related to security. Security used to be seen as a burden on firms' shoulders. This view of security has changed dramatically in recent years as more and more firms experienced security breaches first hand. The pattern of increase can easily be seen in the number of security incidents reported to CERT in figure below.

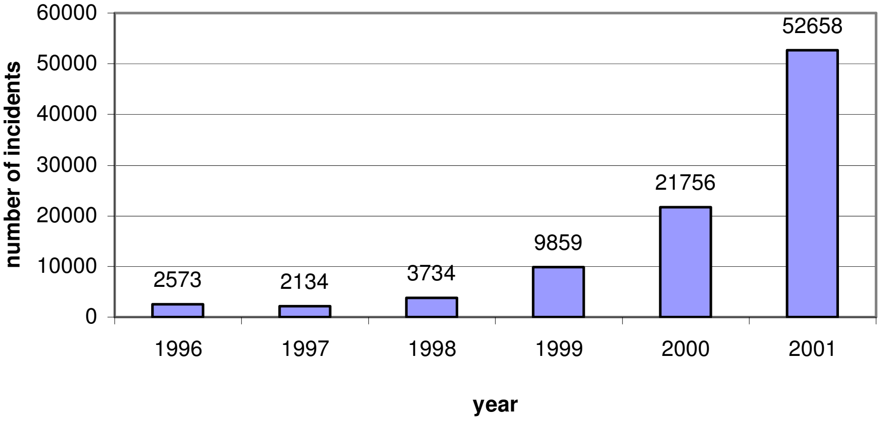

Figure 1: The number of security incidents (Source: CERT)

Recent attacks on several high profile web sites such as Amazon, eBay, Yahoo, and Etrade have also contributed to the heightened awareness of security on the Internet. The increasing number and the increasing severity of attacks over the years have brought the issue to the forefront of investors. Thus if the investors had a learning curve to fully understand the implications of security breaches, one would expect that response to security breaches will be more severe over time. Therefore, our next hypothesis is:

***HYPOTHESIS 5* (H5): Other things being equal, the abnormal (negative) stock market returns due to Internet security breaches is positively associated with time.**

2.3. The Relationship Between Internet Security Breaches and Market Value of Internet Security Firms (The Information Transfer)

The announcements of security breaches also convey information to investors about Internet security developers. Anecdotal evidence suggests the link between security breaches and the market value of Internet security firms. Following the news of February 2000 DOS attacks, five different Internet security stocks climbed more than 20%. A series of attacks against web firms over the last few years proves that this is not a temporary issue. As firms invest more on security, demand for security products goes up. Gartner predicts that U.S companies' investments in information security will increase from the current 0.4% of revenue to 4% of revenue by 2011, a 1000% increase (Rombel 2001).

Information transfers are said to occur if announcements made by one group of firms contemporaneously affect the returns of another group of non-announcing firms (Schipper 1990). Previous studies have documented information transfers in various settings, such as earnings announcements (Asthana and Mishra 2001) and management forecasts (Baginski 1987). Following both empirical and anecdotal evidence, we expect that the announcement of security breaches will impact the valuation of security firms in a positive way. Therefore our last hypothesis is as follows:

***HYPOTHESIS 6* (H6): Announcement of Internet security breach is positively associated with abnormal stock market returns of Internet security firms.**

3. Sample Selection and Coding

3.1. Dataset

To analyze the effects of announcements of security breaches on capital markets we defined the event as the first public disclosure in the media of a security breach of a firm. Our study covered security breaches that occurred between January 1, 1996 and December 31, 2001. Announcements of security breaches for our study came from two different news sources: Lexis/Nexis and technology portals CNET and ZDNET. We used the online search features of these sources to search for announcements using the words *attack*, *breach*, *break-in*, within the same search string as the words *hacker*, *internet*, and *security*. This search resulted in 2563 articles for potential events. We identified 225 events corresponding to various security breaches from these articles. Of those, 159 events were dropped for the following reasons: (i) they were attacks on government agencies, non-profit organizations, and privately-held companies, (ii) historical stock data were not available (iii) there were confounding effects, such earnings announcements.

3.2. Sample Coding

Similar to other event studies we used the natural logarithm of market value of the firm at the end of the year immediately preceding the event date as a measure of the firm size to test hypothesis H2 (Im et al. 2001). To code the firms in each announcement as *conventional* or *net* firm we used Internet.com's Internet Stock List^{TM} and Morgan Stanley Dean Writer's Internet Companies List. These are the most comprehensive lists of firms that conduct business solely over the Internet and have been used in prior studies (Ettredge and Richardson 2001). We classified the firm as a net firm if it was listed under both lists. If it was not listed in either list, it was coded as a conventional firm. To code the nature of the breach in each announcement as *availability breach* or *other breach*, each announcement was carefully examined to determine whether the security breach resulted in the loss of availability of the service, application, or information. To code the time of security breaches as *new breach* or *old breach*, a cut-off date was used. The breaches were classified as old if the announcement date of the breach was on or before February 2000, otherwise it was classified as new. We chose February 2000 as a cut off point because we believe that February 2000 is the *turning point* in terms of the rise in the awareness about the risk of the Internet security among investors and in terms of rise in the frequency of attacks.

3.3. Selection of Internet Security Product Firms

We compiled Internet security firms from two sources. These are *INFOSYSSEC*, the security portal for information system security and *Information Security Magazine*, the leading magazine for security industry. *INFOSYSSEC* provides a section about top security companies and their stock quotes. To this we added the list of security firms nominated for 2002 Information Security Excellence Awards by Information Security Magazine.

A total of 128 security firms were identified after combining the firms in these two sources. After the checks similar to those in section 3.1, our final list included 40 security firms that are traded in U.S capital markets. In the next step we compiled a security firm sample for each announcement of security breach. We included a security firm in the security firm sample for an event only if it had been a publicly traded company for at least 160 days before the event occurred. The exact composition of security firm sample for each event was different because the number of security firms that qualified for inclusion varied over time. The mean number of security firms per event was 31.12, the median was 36, the minimum was 17, and the maximum was 38. Similar to the breached firms, these firms were then matched with their return data in CRSP.

4. Statistical Analysis

An event study seeks to determine the effect of an announcement on stock prices of firms. This method has been employed extensively in accounting and finance literature to study the effects of an assortment of events. The first application of this methodology in the IS literature was the study by Dos Santos et al. (1993) who examined the effect of IT investment announcements on the market value of the firm. More recently the effects of various types of IS-related announcements on capital markets have been examined including e-commerce initiatives (Subramani and Walden 2001a), IT failures (Bharadwaj and Keil 2001), IT investments (Im et al. 2001), Dotcom name changes (Cooper et al. 2001), and newly created CIO positions (Chatterjee et al.2001).

The event of interest in our study is the announcement of an Internet security breach for a firm. We computed the event window abnormal return using the market model. The market model is specified

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \tag{1}$$

where

$R_{i,t}$ = return of stock *i* on day *t*;

$R_{m,t}$ = return on the market portfolio on day *t*;

α_i, β_i = intercept and slope parameter for firm *i*;

$\varepsilon_{i,t}$ = disturbance term for stock *i* on day *t* with the usual OLS properties.

Since most of the firms in our sample were technology firms, we use NASDAQ composite index, which is characterized as technology index, as the market index. Previous event studies on the Internet firms also used NASDAQ index as the market index (e.g. Rajgopal et al. 2001)[2].

Using market model we estimated the intercept and slope parameters for each firm in the sample. We chose an estimation window of 160 days that started before the announcement day and ended 1 day before the announcement day. To capture the price effect of announcements that occurred after the stock market's close on announcement days, we used two-day event window. Some studies included the period prior to the announcement day in the event window in order to capture possibility of information leakage to markets before the announcement day (Subramani and Walden 2001a). Since security breaches are generally unanticipated, our event window did not incorporate any period before the announcement.

We used the coefficient estimates, $\hat{\alpha}_i, \hat{\beta}_i$, from market model regression (1) to predict the expected return over the event window. Then we computed the abnormal return for the firm *i* on the day *t* of the event window as

$$AR_{i,t} = R_{i,t} - (\hat{\alpha}_i + \hat{\beta}_i R_{m,t}) \qquad (2)$$

The abnormal returns are unbiased estimates of changes in market value of the firm during the event period, which are attributed to investors' reactions to information contained in the announcement. The standard errors were calculated as (Subramani and Walden 2001a)

$$\operatorname{var}(AR_{i,t}) = \left(s_i^2 \left[1 + \frac{1}{160} + \frac{(R_{m,t} - \overline{R}_m)^2}{\sum_{t=-160}^{-1} (R_{m,t} - \overline{R}_m)^2} \right] \right) \qquad (3)$$

where s_i^2 is the residual return variance from the estimation of market model over 160 days before the event window, $\overline{R}_m$ is the mean market return on the market index over the estimation window, and $R_{m,t}$ is the return on the market index on day *t* in the estimation window.

The cumulative abnormal return and variance of cumulative abnormal return assuming independence are

[2] Use of other indexes does not change our results qualitatively.

$$CAR_i = \sum_{t=0}^{1} AR_i \qquad \text{var}(CAR_i) = \sum_{t=0}^{1} \text{var}(AR_i) \qquad \text{(4) and (5)}$$

These are aggregated across all firms to draw overall inference as

$$\overline{CAR} = \frac{1}{N}\sum_{i=1}^{N} CAR_i \qquad \text{var}(\overline{CAR}) = \frac{1}{N^2}\sum_{t=0}^{1} \text{var}(CAR_i) \qquad \text{(6) and (7)}$$

To test the hypothesis that mean CAR over the event period was significantly different from zero, we used a student's *t* test, which is of the form

$$t = \frac{\overline{CAR}}{\sqrt{\text{var}(\overline{CAR})}} \sim t_{(\alpha, df=N-1)} \qquad (8)$$

5. Results

5.1. The Effect of Security Breach Announcements on Announcing Firms

On the announcement day (t=0) we observed an average abnormal return of -0.8638 %. The stocks realized, on the average, an abnormal return of -1.2282 % in the day following the announcement (t=1). This gave rise to a -2.092 % cumulative abnormal return over the event window. This translated into $ 1.65 billion average loss in market capitalization per incident based on the mean market value of the firms in the data set. Our CAR values were comparable to CAR values found in other event studies (see Subramani and Walden 2001a).

Table 1 presents the results related to H1. Mean abnormal returns are negative and statistically significant in each day in the event period. Over the event window, t-statistic for the mean CAR is almost 3, with a p-value of 0.00192, indicating that mean CAR is significantly different than zero. Thus we reject the null hypothesis of zero mean CAR in favor of the alternative hypothesis in H1. In order to check robustness of our results we also employed a nonparametric test, namely Wilcoxon signed-rank test. The result in Table 1 indicates that test statistics (z-value= -1.8238) is negative and significant (p-value=0.0341), confirming the result of the parametric test.

5.2. Determinants of Cross-Sectional Variance in CARs

To study the relationship between CARs and characteristics of events, we set up a multiple linear regression model, given in equation 9. This allowed us to test hypotheses H2 -H5.

$$CAR_i = \beta_0 + \beta_1(FirmSize)_i + \beta_2(FirmType)_i + \beta_3(Time)_i + \beta_4(AttackType)_i \tag{9}$$

A value of "1" was assigned if the firm type is net and "0" otherwise. The size of the firm was coded as the log of market value of the firm (in millions) immediately preceding the event. The nature of the attack was labeled as "1" if the security breach was an availability attack and "0" otherwise. Finally time was captured using an indicator variable, "1" for new attacks and "0" for old attacks. Descriptive statistics and correlation matrix for variables are shown in table 2.

Table 3 presents the results of the regression analysis. The overall model is significant (F=4.58, p=0.0027) with an R^2 of 0.2311 and adjusted R^2 of 0.1807. Based on the results in table 3, H2 is supported. The coefficient for firm type is negative and significant (t=-1.59; p=0.0583), indicating that abnormal (negative) stock market returns due to Internet security breaches were larger for net firms than conventional firms. The results show that, all other things being equal, compared to conventional firms, net firms' stocks experienced, on the average, 2.615 % more negative abnormal return. H3 that relates firm size to abnormal return was strongly supported by the data. Parameter estimate for the firm size is positive and significant (t=3.54; p=0.0004), as expected. The result confirms that smaller firms lose more than larger firms in case of a security breach.

In contrast to our expectations, we couldn't find any support for H4. Our supposition that DOS attacks have a different impact than other types of attacks was not supported by the data. The parameter estimate is negative but not significant (t=-0.51; p=0.3055). This implies that markets do not distinguish between different types of security breaches. In other words, market participants apply a similar negative premium across all attacks regardless of their types. Finally, H5 is supported by the data. The estimate of time coefficient is negative and significant (t=-1.63; p=0.0537), indicating recent attacks received harsher reaction from investors. Security breaches occurred after February 2000 resulted in more than 2.8 % drop in firms' returns compared to breaches occurred before February 2000.

5.3. The Effect of Security Breach Announcements on Internet Security Firms

Since all security firms experience the same signal for possible information transfer, i.e. an announcement of a security breach, on the same day, the event windows for security firms overlap perfectly. Thus we cannot aggregate, as we did before, the estimated variances of CARs of individual Internet security firms for a given event to estimate the variance of mean CAR for that event. Hence it is crucial to consider cross-sectional dependencies to avoid incorrect inferences.

Because of above concerns, we chose not to estimate the variance of mean CAR from the estimated variances of sample CARs for each information transfer event. Instead we only calculated the mean CAR for each event. Although the OLS based CARs give biased estimate of the variance, they provide unbiased estimates of coefficients in that context (Bernard 1987). Then we estimate mean and variance of average CAR over all events as (see Subramani and Walden (2001b) for a detailed discussion).

$$\overline{\overline{CAR}} = \frac{1}{N}\sum_{i=1}^{N}\overline{CAR_i} \qquad \text{var}(\overline{\overline{CAR}}) = \frac{1}{N-1}\sum_{i=1}^{N}(\overline{CAR_i} - \overline{\overline{CAR}})^2 \qquad \text{(10) and (11)}$$

where $\overline{CAR_i}$ is the mean CAR of security firms for security breach *i*, and $\overline{\overline{CAR}}$ is average over all $\overline{CAR_i}$ s. Then the test statistic is

$$t = \frac{\overline{\overline{CAR}}}{\sqrt{\text{var}(\overline{\overline{CAR}})}} \sim t_{(\alpha, df=N-1)} \qquad (12)$$

We observed an average abnormal return of 0.7061 % on the announcement day (*t*=0). The stocks realized, on the average, an abnormal return of 0.654 % in the day following the announcement (*t*=1) giving rise to a 1.1356 % cumulative abnormal return over the event window. Thus, over two-day period, on average, a total gain of \$ 1.06 billion of market values of security developers could be attributed to information transfer effect of security breach announcements.

The information transfer effects of security breach announcements are disclosed in table 4. When we consider all security breach announcements, the mean cumulative abnormal return is 0.01356. This positive abnormal return is significant (t-value= 2.712). Nonparametric test is also significant (z-value= 2.028). These results support the hypothesis that security breach announcements increase the market values of security firms.

6. Implications and Conclusions

Our study shows that the announcements of Internet security breaches are negatively associated with the market value of announcing firms. In addition our results show that the market values of security developers increase when security breaches are announced. Overall, our study shows that investors pay close attention to news concerning Internet security breaches.

The finding that average (negative) CAR associated with announcements decreases with the size of the firm suggests that smaller firms are penalized more than larger firms. This result has several implications. For the managers of small firms, this result serves as a reminder of the importance of security for survivability of these firms. They should start to see the security not only as a risk-reducer but also as an enabler in this internetworked world.

Although, market penalizes all firms for security breaches, net firms are penalized more compared to conventional firms. A possible explanation for this effect is the differential degree of dependency by the firms on Internet to generate revenues. Firms that solely depend on the Internet as a revenue generating mechanism pay higher prices in case of a security breach than firms that have multiple sales channels. Security of IT systems for net firms is extremely important for a net firm's success.

Further the results indicate that negative effects of security problem have risen over time. The consequences of security breaches are much higher for incidents that occurred after the famous February 2000 DOS attacks. This result along with an increase in vulnerabilities of systems as a result of greater dependency on technology should caution firms to periodically reassess their security risks and take necessary steps to mitigate the risk.

The finding that the firms experience similar CARs irrespective of the nature of attack is unexpected. One possible explanation is that investors regard any kind of security breach as a failure of IT security and penalize firms for not having taken adequate steps to prevent security problems. This shows that availability, although very important in e-commerce, is not the only criterion that determines the market's response to a security breach. We couldn't classify the attacks into more than two categories because we didn’t have enough observations. Future research should focus on more general classification of attack types on a larger data set.

The finding that security firms realize significant positive returns as a reaction to announcements on security breaches shows that security and e-commerce are tightly interlinked. E-commerce without security can be harmful to firms. The rise in stock prices of Internet security firms further justifies this argument because security can be improved only with security technology.

Our results have a number of other implications. In contrast to the anecdotal evidence on the effect of Internet security problems on the market value of firm, we provide a more objective and statistically valid assessment of the value loss in capital markets. Weak security practices do lead to huge loss in capitalization in case of a security breach. Our results should be reassuring to firms that have invested in information security. For the firms that haven’t adopted sound security practices yet because of doubts about their value, our results should be a source of encouragement to implement it.

Our results show that the true cost of security is not restricted to cost of replacing the breached systems. The cost due to loss of market capitalization may be more devastating than the direct cost of breach. There is no single security technology that can solve the security problem by itself. Firms are increasingly realizing that appropriate security management requires an IT security architecture that consists of multiple layers of controls with different capabilities and characteristics. The problem of how to implement an optimal IT security architecture is unexplored and deserves attention.

References

Asthana S. C. and Mishra B. K., "The Differential Information Hypothesis, Firm Size, and Earnings Information Transfer An Empirical Investigation," *Journal of Business Research*, 53, 2001, pp. 37-47.

Atomic Tangerine, "NPV: Information Security," *White Paper*, Atomic Tangerine Inc., 2000.

Baginski, S. P., "Information Transfer Associated with Management Forecasts of Earnings," *Journal of Accounting Research*, 25, 1987, pp.196-216.

Chatterjee, D., Richardson, V. J. and Zmud, R. W., "Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO Positions," *MIS Quarterly*, 25, 1, 2001, pp. 43-70.

Cooper, M.J., Dimitrov, O. and Rau, P. R., "A Rose.com by Any Other Name," *The Journal of Finance*, 56, 6, December 2001.

Dos Santos, B. L., Peffers, D. C. and Mauer D. C., "The Impact of Information Technology Investment Announcements on the Market Value of the Firm," *Information Systems Research*, 4, 1, 1993, pp. 1-23.

Ettredge, M. and Richardson, V. J., "Assessing the Risk in E-Commerce," *Working Paper*, University of Kansas, May, 2001

Fama, E., "Efficient Capital Markets II," *Journal of Finance*, 46, 5, 1991, pp. 1575-1617.

Hendricks, K. B.and Singhal, V. K., "The Effect of Supply Chain Glitches on Shareholder Wealth," *Working Paper*, December 2000.

Im, K. S., Dow, K. E. and Grover, V., "Research Report: A Reexamination of IT Investment and the Market Value of the Firm-An Event Study Methodology," *ISR.*, 12, 1, March 2001, pp.103-117.

Pastore, M., *Companies Lack Understanding of Information Security*, Internet.com, October 10, 2001.

Power, R., "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, 8,1, 2002.

Rajgopal, S., Venkatachalam M. and Kotha, S., "Managerial Actions, Stock Returns, and Earnings: The Case of Business-to-Business Internet Firms," *Journal of Accounting Research (forthcoming)*, 2001.

Rombel, A., *Internet Security in an Insecure World*, Global Finance, 15, 13, December, 2001, pp. 28-32.

Schipper, K., "Information Transfers," *Accounting Horizons*, 4, 1990, pp. 94-107.

Subramani, M and Walden, E., "The Impact of E-Commerce Announcements on the Market Value of Firms," *Information Systems Research*, 12, 2, 2001a, pp. 135-154.

Subramani M and Walden, E., "The Game of the Name: A Comparison of Capital Market Reactions to Dotcom vs. Traditional Name Changes," *Working Paper*, University of Minnesota, July 18, 2001b.

Warner, B., *Internet Firm Hacked Out of Business*, Yahoo News, February 18, 2002.

Table 1: Event Study Results for Breached Firms (N=66)

Event Window	Mean	t-value	p-value[a]	Frequency of Negative Returns	z-value[b]	p-value[a]
0	0.008638	-1.74985	0.04243	36	-0.948630	0.171404
1	0.012282	-2.49133	0.0076442	39	-1.894067	0.029108
0,1	-0.02092	-2.99862	0.00192	41	-1.823797	0.034091

[a] p-values with one-tailed significance.

[b] If T^+ is the sum of the ranks assigned to positive CARs, and N is the sample size, the statistics is given by $(T^+-a)/b$ which is distributed as N(0,1) for large samples, where a= N*(N+1)/4 and b= N*(N+1)*(2N+1)/24

Table 2: Descriptive Statistics and Pearson Product-Moment Correlations

Variable		Mean	Std. Dev.	Minumum	Maximum	(1)	(2)	(3)	(4)
(1)	Firm Size	9.87763	2.0879	5.0668	13.04	1.000			
(2)	Firm Type	0.46987	0.5029	0	1	-0.249[b]	1.000		
(3)	Time	0.68182	0.4693	0	1	0.283[b]	-0.139	1.000	
(4)	Nature of Attack	0.51515	0.5036	0	1	0.211[c]	-0.180	0.053	1.000

[a] significant at $p \leq 0.01$ [b] significant at $p \leq 0.05$ [c] significant at $p \leq 0.10$.

Table 3: Results of Cross-Sectional Regression to Predict Variability in CARs

	Predicted Sign	Parameter Estimate	Standard Error	t-statistic	p-value[a]
Intercept	-/+	-0.12856	0.04205	-3.06	0.0033
Firm Type (H2)	-	-0.02615	0.01643	-1.59	0.0583
Firm Size (H3)	+	0.01456	0.00411	3.54	0.0004
Nature of Attack (H4)	-/+	-0.00829	0.01621	-0.51	0.6110
Time (H5)	-	-0.02879	0.01762	-1.63	0.0537
Model R^2	0.2311				
Adjusted R^2	0.1807				
F-value	4.58	(0.0027)[b]			

[a] P-values represent one (two) tailed significance when a sign is (is not) hypothesized.

[b] Number in parenthesis specifies the significance of F-value.

Table 4: Information Transfer Effect on Security Firms (N=66)

Event Window	Mean	t-value	p-value[a]	Frequency of Positive Returns	z-value[b]	p-value[a]
0	0.007061	2.3671	0.010458	36	1.440512	0.07486
1	0.006540	2.0011	0.024780	35	1.357467	0.08732
0,1	0.013560	2.7123	0.004271	37	2.028216	0.02127

[a] p-values with one-tailed significance.

[b] If T^+ is the sum of the ranks assigned to positive CARs, and N is the sample size, the statistics is given by $(T^+-a)/b$ which is distributed as N(0,1) for large samples, where a= N*(N+1)/4 and b=N*(N+1)*(2N+1)/24