Measuring the Impact of Security Breaches on Stock Valuations of Firms

Sanjay Goel, Christopher Brown, Hany Shawky

School of Business, University at Albany

Abstract

Security breaches can have a significant impact on the financial performance of firms. Information has become the most valuable asset of an organization and security breaches can lead to loss of confidentiality, availability, and integrity of information as well as to disruption of critical services. With public disclosure laws in place, security breaches of personal private information of clients can cause damage to the firms' reputation and also lead to legislative sanctions. The evidence on the impact of security breaches is clear. However, the impact is typically difficult to estimate. In this research, the impact of security breaches on an organization is gauged via the reaction of the market. The impact of public disclosure of security breaches on market valuations is estimated using the event study methodology. To conduct this study, incidents of security breaches were collected over the last three years. In addition, reports and news articles corresponding to these breaches were collected from public sources to accurately determine when the event was disclosed publicly. The study considers both severity and type of breach to more precisely calibrate market reaction. Data on stock returns of firms obtained from the CRSP database is used for the event study. This paper describes our research approach, data collection, and the work that will be conducted.

1.0 Introduction

Security breaches can lead to the compromise of organizational information, potentially revealing company secrets or confidential client information. Leakage of sensitive information can have a harmful effect on the company leading to litigation, government sanctions, and loss of competitive edge. Organizations are reluctant to publicly reveal information concerning security breaches for fear of providing information to other hackers. An even greater concern is the erosion of market value that follows a public revelation of security breaches (Gordon and Loeb, 2002). The severity of damage caused to organizations due to the disclosure can vary significantly based on the amount as well as the value of information. However, we believe that in the past there was a disproportionate reaction of the market and the erosion of market value exceeded the actual damage to the organization. The disproportionate erosion of market value can be attributed to psychological factors.

Firms typically institute managerial, technical, and operational controls in an attempt to minimize exposure of their valuable assets. Selection of controls is an optimization problem that requires balancing the potential damage against the cost of controls. The potential damage is estimated by the value of each asset and probability of it being damaged. The impact of controls on reducing the potential damage is then balanced against the cost of controls. The fundamental problem in this approach is that data collection is cumbersome and estimates rely heavily on

subjective judgment of the analysts. Consequently, there can be a high level of uncertainty in the analysis rendering the entire process fruitless. In addition, since technology and threats change continually, the analysis can become obsolete quickly.
Determining the impact of breaches to organizations by utilizing the fluctuations in the market value of publicly traded companies in response to security breaches provides an efficient means of computing security risks. The efficient market hypothesis asserts that "financial markets are informationally efficient, and that prices on traded assets, e.g., stocks, bonds, or property, already reflect all known information and therefore are unbiased in the sense that they reflect the collective beliefs of all investors about future prospects." Thus, the impact of security breaches can be measured by observing fluctuations of the market in response to security breaches. The impact of different kinds of breaches should be reflected in differential changes to market valuations. In this study, mandatory data disclosures made by organizations, that include the type of breach (e.g. malicious code, stolen hardware, and insider attacks) and the severity (in terms of the number of people impact) are identified. By classifying the breaches based on severity and type, the market reaction can be calibrated precisely for different types of breaches for use in risk analysis.

The potential benefit of this research will be to assist organizations in making sound business cases for information security investments, as well as providing better guidance on managing public disclosure of security breaches. Several high profile cases have been mishandled where organizations were not forthcoming with information and released it only under public and legal pressure. This study has two main objectives 1) to determine the market reaction to security breaches in publicly traded organizations, and 2) quantify the impact of security breaches for risk analysis.

An event study methodology is employed for this investigation. We hypothesize that investors would react rationally to breaches and their response would be measured based on breach impact. Research will also examine the impact of repeated breaches on the market value of firms. Campell et al. (2003) have examined the impact of security breaches on market performance; however, their study does not discriminate between the different types of attacks or the severity of attacks. Hovav and D'Arcy (2004, 2005) have examined this effect for a limited subset of attacks (viruses, worms, and denial-of-service) but the relative impact of the different types of breaches is not clear. Of the utmost importance today is the impact of identity theft, which 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 could potentially jeopardize the victims' credit ratings, there is much larger publicity associated with these types of incidents. The impact of identity theft on the market value of publicly traded companies will be empirically examined using stock market data.

The rest of the paper is organized as follows: Section 2.0 describes the approach of Event Study analysis that we are planning to use and Section 3.0 describes the data collection methodology and Section 4.0 presents a brief summary of our work and future plans.

2.0 Methodology

In an event study, prices around the time of an event are examined to analyze the impact of the event on firm valuation. The basic premise in such studies is that if the market is rational, the true economic effects (detrimental or benign) will be reflected in the security price of the affected firm. Three broad types of event studies are: market efficiency studies, information usefulness studies, and metric explanation studies (Henderson, 1990). Market efficiency studies evaluate how quickly and accurately financial markets react to information, such as earnings or merger announcements, while information usefulness studies determine how security prices react to those pieces of information (Henderson, 1990). Conversely, metric explanation studies use cross-sectional regression in an attempt to explain abnormal returns experienced around the time of an event (Henderson, 1990). Examining security price behavior for organizations that experienced an information security related incident would shed light on the impact, if any, of security breaches on security prices, as well as determine how quickly the market reacts to such news. This study is a hybrid between market efficiency and information usefulness.

In the late 1960s, two influential event studies were conducted; Ball and Brown (1968) investigated the impact of earnings announcements, while Fama, Fisher, Jensen, and Roll (1969) measured market efficiency with regards to stock splits. These studies introduced the event study methodology that is still predominantly employed today. MacKinlay (1997) presents a comprehensive review for this type of research and clearly defines the required steps:

1) Define a window of time around the event in which the stock price is monitored: A window of one day around the event is typically used, however longer windows would be useful in case information is trickling in slowly prior to the event or if repercussions of an event become gradually clear after the occurrence of the event. Since the public fathoms the impact of security breaches slowly, a larger window might be more appropriate.
2) Determine the selection criteria of firms in the study: Several criteria, such as market capitalization or business industry can be used to narrow down the firms in the corpus to reduce potential biases in the study.
3) Determine the model for computing the abnormal return: Abnormal returns can be defined as the difference between the actual and the normal return of the firm over the event window. The normal return can be defined as the expected return when no incidents occur. It can be computed using two different models 1) constant mean return model 2) market model. The constant mean return model assumes that the mean return of a given security is constant through time and the market model assumes a stable linear relation between the market return and the security return.
4) Design of the testing framework for the abnormal returns: Defining the null hypothesis and determining techniques for aggregating abnormal returns for individual firms. Statistical tests will be identified for analyzing the data.
5) Collection of Data for Analysis: Firms need to be identified for which event information is available and stock prices for those firms over that period of time need to be extracted from databases.

There are three essential calculations to be performed in an event study. First, normal performance for the organization must be estimated. The market model of estimating normal returns is a one-factor model that assumes a linear relationship between the return of the market portfolio and the individual security (MacKinlay, 1997). Specifically, the estimated normal return for security *i* is defined in Equation 1.

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

Where, R_{it} is the return on security *i* in period *t* and R_{mt} is the return on the market portfolio. ε_{it} is the zero mean disturbance term, α_i is a measure of risk-adjusted performance, and β_i is a measure of risk (MacKinlay, 1997). Having estimated the normal return, abnormal returns can then be calculated by subtracting the normal return from the actual return as shown in Equation 2.

$$AR_{it} = K_{it} - R_{it} \quad (2)$$

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.* The final step is to aggregate the abnormal returns for each security in the sample. The cumulative abnormal return from period t_1 through t_2, is defined in Equation 3.

$$CAR_i(t_1, t_2) = \sum AR_{it} \quad (3)$$

Although the event study structure is relatively simple, some statistical issues need to be considered especially when the event window is long (typically greater than 12 months). Long-horizon studies typically lack the ability to detect abnormal performance, and are sensitive about the return generating process (Kothari & Warner, 2006). Short-horizon studies, on the other hand, generally do not suffer from these limitations (Kothari & Warner, 2006).

3.0 Data Collection and Analysis

The research entails collection of data on security breaches, classification of data, and correlation of data with stock valuations for firms where security breaches have occurred in the past. The data required for this research includes security breach disclosures, reports in media, and stock market returns. The reports are available from public sources, such as Lexis Nexis, Wall Street Journal, PC Week, Register, etc. Several states have enacted laws to force corporations to inform people possibly affected by the compromise of personal information through breaches. This information is open to pubic and has been obtained for this research. The data also contains the severity of each incident in terms of the number of people impacted. Eventus (CITE) is used for the event study analysis, which employs the CRSP (Center for Research in Stock Prices) stock database.

For each security breach that was identified, media reports covering the security breach were collected and stored in a database. As many media reports as possible were collected for each security breach. Using the approximate date of the security breach as a starting point, public

databases like Lexis Nexis were queried for media reports. Media reports that covered more than one individual security breach were associated with each security breach reported on (i.e. a media report detailing security breaches at Wachovia and Bank of America would be associated with both security breaches). In the event that a single report was published in numerous media outlets (e.g. an Associated Press story printed in various newspapers), all reports were logged in the database and associated with a single report ID. Such redundancy was warranted in order to capture the sheer exposure of a media report.

The database contains six main tables: *Incident*, *IncidentTypes*, *Report*, *ReportOutlet*, *Company,* and *Incident-NonIncident-Companies* as shown in Figure 1. The *Incident* table contains data pertaining to actual security breaches and has attributes like company ID (ticker symbol), incident type (e.g. stolen hardware, lost backup, fraud, etc), date (either date of internal discovery or first media reporting), cost associated with breach, number of people affected, and whether or not legal action has occurred as a result of the incident.

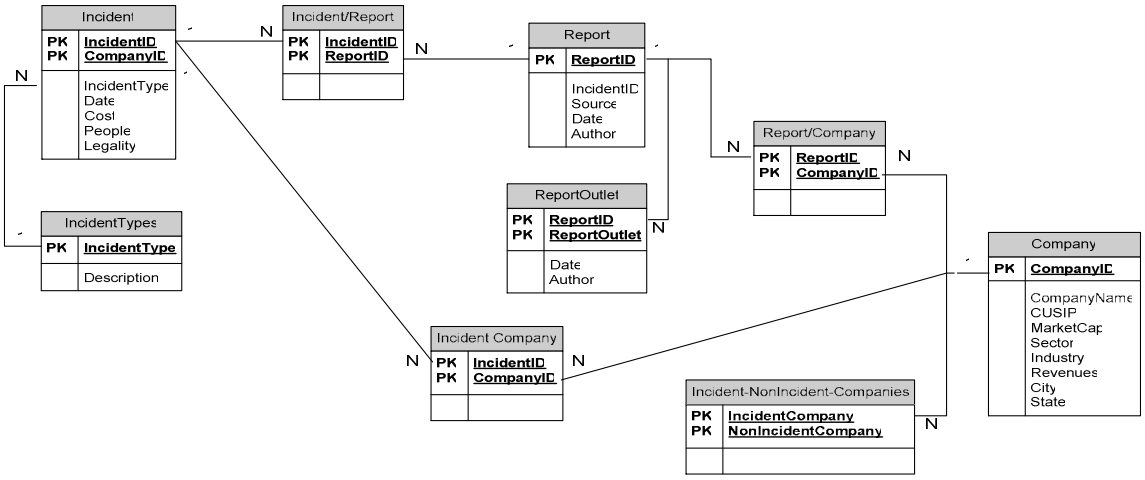

Figure 1: Database Schema for the Security Breach Database

The *IncidentTypes* table consists of only two attributes: type of security breach and a two-letter code associated with that type of security breach. Types of security breaches included exposed information (EI), fraud (FR), hackers (HA), insiders (IN), lost backup tape (LB), malicious code – Trojan (MCT), malicious code – virus (MCV), malicious code – worm (MCW), and stolen hardware (SH).

The *Report* table houses media report data. Each report has an original source (i.e. publication), author, and date, and could be associated with many security breaches. As alluded to earlier, some reports reference numerous security breaches, and it is critically important to ensure that each incident mentioned is associated with the report. Related to the *Report* table is the *ReportOutlet* table. This table was used to account for the fact that some reports would be printed in numerous publications

The *Company* table contains data for all companies. There are two types of companies: those that have experienced a security breach and those that have not experienced a security breach.

Regardless of the type of company, there are critical elements collected for every company. A company's ticker symbol is used as the company ID, and in order to ensure compatibility with the CRSP database, CUSIP (Committee on Uniform Securities Identification Procedures) identifiers were also obtained. Market capitalizations and revenues were also retrieved to determine if the size of a company has any bearing on the market's response to news of a security breach. Finally, industry and sector information were collected to determine if the type of business affects the market's response. For every company that experienced a security breach, information for one or two similar companies that did not experience a security breach was also logged in the database. "Similarity" is determined on the basis of market capitalization and business area. The *Incident-NonIncident-Companies* table is used to correlate companies that have experienced a security breach with those similar comparison companies that have not experienced a security breach.

4.0 Summary

We attempt to address the fundamental issue that the stock market valuations are impacted by security breaches in an organization. Using the date of the first news release as the event date, we examine a window of 5 days before this date to test for leakage of information prior to the press release. Furthermore, a window of 5 days beyond the incident is also examined as information may percolate slowly to investors and delayed information may be released. We also consider a long window to observe the long-term impact of the change in the returns; for instance, short-term losses may be corrected over the longer term in case of an irrational short-term reaction. While initial results demonstrate a correlation between stock market valuations and security breaches, due diligence is still required to confirm the results of the event study and the results will be presented in the full version of the paper.

References

[1] Campbell, K., L.A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Journal of Computer Security, Vol. 11, No. 3, 2003.

[2] Gordon, L. A. and M. P. Loeb, "The Economics Information Security Investment," *ACM Transactions on Information and System Security*, November 2002.

[3] Hovav, A. and D'Arcy, J. (2005). Capital Market Reaction to Defective IT Products: The Case of Computer Viruses, *Computers & Security*, Vol. 24(5) pp. 409-424.

[4] Hovav, A. and D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms, *Information Systems Security*, Vol. 13(3) pp. 32-40.

[5] Dolley, J. C., "Characteristics and Procedure of Common Stock Split-Ups," *Harvard Bus. Rev.*, Apr. 1933, *11*, pp. 316–26.

[6] MacKinlay, A.C., (1997) "Event Studies in Economics and Finance", *Journal of Economic Literature, Vol. XXXV* (*March 1997*)*, pp. 13–39.*