An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price

Rahul Telang and Sunil Wattal

Abstract—Security defects in software cost millions of dollars to firms in terms of downtime, disruptions, and confidentiality breaches. However, the economic implications of these defects for software vendors are not well understood. Lack of legal liability and the presence of switching costs and network externalities may protect software vendors from incurring significant costs in the event of a vulnerability announcement, unlike such industries as auto and pharmaceuticals, which have been known to suffer significant loss in market value in the event of a defect announcement. Although research in software economics has studied firms' incentives to improve overall quality, there have not been any studies which show that software vendors have an incentive to invest in building more secure software. The objectives of this paper are twofold. 1) We examine how a software vendor's market value changes when a vulnerability is announced. 2) We examine how firm and vulnerability characteristics mediate the change in the market value of a vendor. We collect data from leading national newspapers and industry sources, such as the Computer Emergency Response Team (CERT), by searching for reports on published software vulnerabilities. We show that vulnerability announcements lead to a negative and significant change in a software vendor's market value. In our sample, on average, a vendor loses around 0.6 percent value in stock price when a vulnerability is reported. We find that a software vendor loses more market share if the market is competitive or if the vendor is small. To provide further insight, we use the information content of the disclosure announcement to classify vulnerabilities into various types. We find that the change in stock price is more negative if the vendor fails to provide a patch at the time of disclosure. Also, more severe flaws have a significantly greater impact. Our analysis provides many interesting implications for software vendors as well as policy makers. In particular, our study provides some evidence of the value of secure software.

Index Terms—Information security, software vulnerability, quality, event-study, patching, software vendors.

1 Introduction

A security vulnerability is a flaw within a software product that can cause it to work contrary to its documented design and can be exploited to cause the system to violate its documented security policy.[1,2] Anecdotal evidence shows that software vulnerabilities have widespread impact and cause significant economic and noneconomic damage to firms (in this paper, "firms" refers to companies that use software products, and "vendors" refers to companies that develop software products). A National Institute of Standards and Technology study [39] estimates the cost of faulty software at $60 billion per year. Incidents such as the Code Red virus (2001) and the Melissa virus (1999) occurred when hackers exploited flaws in software. The damage due to Code Red was estimated at $2.1 billion and that due to Melissa at $1.1 billion.[3] The Gartner Group estimates that the system downtime caused by security vulnerabilities would triple from 5 percent of the total downtime in 2004 to 15 percent of the total downtime in 2008.[4] In 2003, the Computer Emergency Response Team (CERT) at Carnegie Mellon University reported about 250,000 attacks on the Internet, most of which exploit vulnerabilities in software code (Applewhite 2004). Instances exist where software vendors also seem to suffer due to flaws in their products. The *Wall Street Journal* (9 November 2004) reported that Microsoft's Internet Explorer (IE) is losing market share in the Web browser market to competitors, such as Mozilla's Firefox, due to numerous flaws discovered in IE. For example, nearly 8 million people downloaded the Firefox browser between September and November 2004. Moreover, vulnerability disclosure is finding its way into firms' strategy toolkits, as is evident from a *Wall Street Journal* report (February 2004) that software vendors are spending time and effort in discovering flaws in their rivals' products in order to influence the

[1] As defined by the Organization of Internet Safety (OIS, www.oisafety.org).

[2] In this paper, we use the terms "software vulnerability," "security vulnerability," "bug," and "flaw" interchangeably. Any other type of vulnerability, such as a non-security-related vulnerability, is explicitly mentioned by name.

[3] Source: www.cisco.com/warp/public/cc/so/neso/sqso/roi1_wp.pdf.

[4] "Building a Sound Security Infrastructure: New Defenses for a New World of Threat," Gartner Security Report (ISBN 1-932876-01-04), http://www.tekrati.com/research/NewsArchives.asp?q=gartner+security&id=3564.

- *R. Telang is with the H.J. Heinz III School of Public Policy and Management, Carnegie Mellon University, 2107D Hamburg Hall, 4800 Forbes Ave., Pittsburgh, PA 15237. E-mail: rtelang@andrew.cmu.edu.*
- *S. Wattal is with the Fox School of Business, Temple University, 209D Speakman Hall, 1810 N. 13th Street, Philadelphia, PA 19122. E-mail: swattal@temple.edu.*

Manuscript received 1 June 2006; revised 26 Jan. 2007; accepted 8 May 2007; published online 22 May 2007.
Recommended for acceptance by A. Wolf.
For information on obtaining reprints of this article, please send e-mail to: tse@computer.org, and reference IEEECS Log Number TSE-0123-0606.
Digital Object Identifier no. 10.1109/TSE.2007.1015.

0098-5589/07/$25.00 © 2007 IEEE Published by the IEEE Computer Society

rivals' stock prices. For example, security software vendor IDS released a vulnerability alert on rival Checkpoint's firewall software on the day Checkpoint usually holds its annual US investor conference.

In spite of all these concerns about software vulnerabilities, there is a widespread belief that software vendors do not have enough incentives to improve the quality of their software. Many believe that software vendors typically follow the policy of "sell today and fix later" or "I'd rather have it wrong than have it late" [4], [40] when launching software products in the market. One reason for such an attitude is that software errors which escape detection during prelaunch testing have a good chance of escaping detection later. However, in the Internet age hundreds (if not thousands) of people are looking for flaws in software products, drastically increasing the chances that a flaw will be exposed. Not only are security software products such as firewalls at risk, but software such as operating systems, enterprise software, and database software also contain numerous flaws that can be exploited to create security-related attacks. Many users believe that the market does not adequately punish software vendors for these defects and are pushing for legislation to hold software vendors legally responsible for flaws in their software. Bruce Schneier, a leading security expert, summarizes this popular sentiment as follows: "There are no real consequences to the vendors for having bad security or low-quality software. Even worse, the marketplace often rewards low quality. More precisely, it rewards additional features and timely release dates, even if they come at the expense of quality" (*Computerworld*, October 2004).[5] Hovav and D'Arcy [31] find no evidence of negative stock returns for software vendors if a virus attack is announced in their products. They conclude that software vendors do not have any incentive to develop defect-free software.

So far, software economics literature has mentioned very little regarding the incentive of vendors to invest in producing software that is free of security-related defects. Prior research on software risks [46], [5] fails to include any measure for security-related risks. The closest literature to the topic of security vulnerabilities is that on software quality [6], [26]. However, quality is traditionally measured in terms of reliability and integrity of the source code, which essentially tests software against specified streams of input from users. Since the cost of testing typically follows an S-shaped curve [29], vendors may be tempted to stop the testing once the product passes the desired functionality tests rather than determining whether intentionally improper action can cause the software to fail. In today's Internet age, software designers must think not only of users, but also of malicious adversaries [18]. Some quality models, such as ISO9126, fail to include computer security [42]. Therefore, software which has been certified as high quality, based on existing definitions of software quality, can have many security flaws. Researchers are working on better integration of software quality and software security while designing software [47], [38].

Since security vulnerabilities relate to defects in software, we look at prior literature on product defects in other industries. Jarrell and Peltzman [33] empirically show that product recall announcements in drug and automotive industries are associated with a loss in a firm's market value. Davidson and Worrell [17] confirm the negative impact of product defects on stock prices in nonautomotive industries as well. But any direct comparison between software defects and defects in other products is not appropriate because of some unique characteristics of software products: 1) software products generally come with a click-wrap agreement (or End User License Agreement (*EULA*)), which limits the vendors' liability. 2) The general philosophy held by software vendors, software customers, and the US courts is that software is a uniquely complex product that will probably have some defects [16]. Over the long run, markets will anticipate the effect of vulnerability announcements on cash flows of software vendors, so the impact of a specific announcement might not be significant. Finally, vulnerability announcements are directly related to the installed base of a software product. Popular software products, like those from Microsoft, are constantly subject to malicious and nonmalicious attacks and, as such, have a greater proportion of flaws reported in them as compared to the software installed by fewer users (e.g., Mac OS, of which the user base is smaller). Therefore, the presence of vulnerabilities may not always signal a lower product quality. John Thomson, CEO of Symantec, predicts the flaws in Linux will likely increase as the installed base increases.

In view of these arguments, understanding whether and how the market responds to vulnerability disclosures in software products is interesting. Motivated by these observations, we try to quantify software vendors' losses when a vulnerability is disclosed in their product. The main questions we seek to answer are:

1. Do software vendors suffer a loss in market value if a vulnerability in their products is disclosed?
2. How do the vulnerability, vendor, and market characteristics condition this impact?

Our research has important implications for understanding vendors' incentive to improve prelaunch and postlaunch quality of their software products. Although security flaws receive a lot of attention in popular press, the incentives of software vendors to provide more secure software is still unclear. If we indeed find that the stock market is willing to punish software vendors over vulnerability announcements because it perceives these announcements as a signal of poor quality software that will either increase vendor costs to fix them or erode market share in the long run, then our research provides direct evidence of incentives to provide more secure software. Vulnerabilities are disclosed by vendors or by third parties/competitors with or without a patch. Since we measure whether significant differences in market reaction to such disclosures exist, our paper provides policy guidelines to vendors about whether and how they may disclose the information themselves. Moreover, our study also provides an estimate of the value of patches. Finally, we also examine how vulnerability characteristics and firm characteristics affect the market reaction.

[5] http://computerworld.com/securitytopics/story/0..96948.00.html.

Using an event-study approach, we collect data on 147 vulnerability disclosure announcements from popular press and industry sources over a period of more than five years. Our results confirm that vulnerability disclosure adversely and significantly affects the stock performance of a software vendor. We show that, on average, a software vendor loses around 0.63 percent of market value on the day of the vulnerability announcement. This translates to an average $0.86 billion loss in market value. We also find that vulnerabilities disclosed without a patch yield more negative returns than those disclosed with a patch. This provides evidence as to why vendors are trying to push for legalizing the "limited disclosure norms."[6] Finally, we find that product-specific and firm-specific characteristics also play roles in determining how much product defect announcements affect a vendor.

This paper's main contribution is that it is one of the first comprehensive studies that measure the impact of security vulnerabilities on software vendors. Thus, we extend prior literature on product defects and confirm that software vendors also suffer a loss in market value when a flaw is discovered in their product. This is in spite of the fact that software vulnerabilities are prevalent among software of almost all major vendors and that vendors face no legal liability if clients suffer losses due to these vulnerabilities and that the customers usually incur switching costs when changing their software vendor.

The rest of the paper is organized as follows: In Section 2, we provide a literature review. We develop our hypotheses in Section 3. In Section 4, we discuss the methodology of data collection and also describe the event-study methodology. In Section 5, we present our results using regression analysis and test hypotheses related to how various vulnerability and firm characteristics affect the change in stock prices. Finally, we present the concluding remarks in Section 6.

2 Literature Review

Most prior research on information security [2] discusses the economics of such investments from a customer perspective rather than from a software vendor perspective. Prior event study analyses on information security have focused on the change in market value of firms whose systems are breached [12], [35]. These studies show that announcements of a security breach negatively impact the CAR (Cumulative Abnormal Return) of firms whose information systems have been breached. Campbell et al. [11] conduct a similar event study and find that only the impact of confidentiality-related security breaches is negative and significant; the impact of non-confidentiality-related security breaches is not significantly different from zero. Hovav and D'Arcy [30] show similar results by finding that Denial of Service (DoS) type attacks are not associated with any significant loss in value for firms.[7]

Generally, vulnerability announcements and disclosure have been contentious. Typically, benign independent security analysts (ISA) report a major portion of the vulnerabilities. Since no legal guidelines exist which dictate how vulnerabilities should be handled by the discoverer, some ISAs report the vulnerability to the vendor and give it sufficient time to come up with a patch.[8] This policy is known as "limited disclosure." However, some other ISAs follow the policy of "full disclosure." That is, they immediately post the vulnerability to a public listing such as Bugtraq. One major goal of full disclosure is to eventually force vendors to come up with more secure software. Arora et al. [4] study the optimal timing of vulnerability disclosures and suggest that full disclosure can force vendors to release patches quickly. Kannan and Telang [34] explore the welfare implications of a market mechanism for software vulnerabilities and report that a market-based mechanism for software vulnerabilities always underperforms a CERT-type mechanism. However, none of these studies measures the impact of disclosure on a vendor's market value or profitability. Although one major goal of full disclosure is to eventually force vendors to develop secure software, no empirical evidence exists to suggest that disclosure indeed creates such incentives. Our paper provides an understanding of whether such disclosures create incentives for the vendors to produce secure software in the first place.

Our methodology follows closely from prior-event-study analysis. Campbell et al. [10] present a useful summary of the event-study analysis highlighting the history as well as the commonly followed methodologies. Event-study methodologies are well accepted for studying the implications of public announcements on stock prices. Hendricks and Singhal [27] study the impact of quality-award winning announcements on the market value of firms and document positive abnormal returns for firms winning a quality award. In Information Systems literature, Subramani and Walden [43] show that e-commerce announcements lead to significant increases in the stock price of firms. Im et al. [32] examine the changes in a firm's market value in response to IT investment announcements.

3 Theory and Hypotheses

The costs of software defects to a vendor can be broadly classified into two categories: 1) The cost of producing and distributing a patch for the defect and 2) the cost of lost sales due to dissatisfied customers and negative publicity.

1. **Cost of patching defective systems.** The cost of fixing a system after release can be substantial in comparison to prerelease fixing. For example, the security fixes cost more than four to eight more times when fixed after the application has been shipped. Slaughter et al. [44] and Westland [48] suggest that software defects are harder and costlier to fix if discovered later in the software development cycle (e.g., when the product has been shipped to the customer). According to [14], Microsoft spends about $100,000 on average for each security-related

[6] Disclosure norms are the practices that firms (vendors, users, or third parties) follow about how to report software vulnerabilities. More details on the disclosure norms are mentioned in Section 2 and Section 6.

[7] DoS attacks are classifed as nonconfidential in [11].

[8] The OIS recommends a time period of 30 days to be given to vendors to come up with a patch.

patch. However, the cost of releasing each patch may still not be as significant compared to a firm's market value (typically hundreds of millions of dollars). Patches for faulty software can be generally distributed online with minimal costs to the vendor. Therefore, prima facie, the cost of patching does not seem to be the main reason the market will punish a software vendor.

2. **Cost of lost sales.** Software vulnerabilities can lead to customer dissatisfaction, reputation loss, and, ultimately, to lost sales. Defective software imposes costs on the users (customers) in various ways:

   a. Security breaches caused due to vulnerable software may lead to downtime, disruptions, and compromised confidential information. For example, Cavusoglu et al. [12] show that the market capitalization values of firms decreases, on average, by $2.1 billion within two days of experiencing a security breach.

   b. Using defective software can impose other costs on users as well. For example, cyber insurance firm J.S. Wurzler charges an additional premium to firms for using Windows NT due to the number of security breaches in the software [24].

Summarizing points 1 and 2, we can say the actual cost the vendor bears is

$$\begin{gathered}\textit{Cost of patching the vulnerability}\\ +\ \textit{cost of lost sales in future.}\end{gathered}$$

The magnitude of the second term ($cost\ of\ lost\ sales\ in\ future$) depends on the amount of loss the customers suffer due to the vulnerability, and, potentially, how easily the customers can punish the vendors (by switching vendors, or some large buyers may contractually force vendors to compensate them). Moreover, vendors may also lose future sales because potential customers might avoid buying a product, or existing customers may delay purchasing upgrades due to insecure products. However, software products exhibit network externalities and have large switching costs making it difficult for users to switch vendors ([20], [21], [9]). Therefore, the cost of lost sales depends on the market structure as well. In more competitive markets, buyers have more choices and hence vendors may suffer more. Similarly, in markets with large and influential buyers, vendors would be forced to internalize a higher proportion of customer losses (e.g., due to contractual obligations).

Thus, we would expect that loss due to vulnerability announcements directly depends on how much the patch costs, how much customer loss (and, in turn, loss of profits for the vendor) the vulnerability can cause, and how competitive the market is. Based on our discussion so far, we hypothesize that

H1. *A software vendor suffers a loss in market value when a security-related vulnerability is announced in its products.*

We test this hypothesis against the null hypothesis that vulnerability announcements do not have a significant impact on the market value of a software vendor. Hypothesis testing allows a researcher to test whether a parameter is truly different from a baseline measure.

We next examine how this loss is conditioned by various firm, market, and vulnerability characteristics.

3.1 Firm and Industry Characteristics

3.1.1 Competitiveness

As noted earlier, we would expect the loss in market value due to a software vulnerability to be greater in a more competitive market. Therefore,

H2. *A software vendor suffers a greater loss in the market value when its product operates in a competitive market.*

We define how we measure competitiveness in the later section.

3.1.2 Firm Size and Diversification

The impact of a vulnerability announcement may also depend on the size of the firm. Large firms have a larger customer base and will, therefore, suffer greater damage if a vulnerability is announced. However, large firms are also diversified. Diversified firms have many product lines and the potential loss in revenues due to a flaw in one product may not impact the market value appreciably. For example, firms such as IBM are well diversified and operate in many segments, whereas firms such as RedHat primarily depend on one major product (Linux-based software) for most of their revenues. Thus, we test how the firm size and level of diversification affects market value.

3.2 Vulnerability Characteristics

3.2.1 Patch versus No Patch

Software vendors can quickly release a patch to mitigate the impact of such disclosures. In many instances, vendors release a patch at the time of the vulnerability announcement. The presence of the patch is likely to reduce customers' loss. Since the presence of the patch also reflects the vendor's commitment to its customers, we expect vulnerabilities disclosed with the patch to compensate, to an extent, the negative signal due to vulnerability disclosure. We thus hypothesize:

H3. *The presence of a patch mitigates the negative impact of the vulnerability announcement.*

3.2.2 Type of Attack Facilitated

Customer damage suffered due to a vulnerability in the vendor's software depends on the type of security breach the vulnerability facilitates. Campbell et al. [11] classify the security breaches as confidentiality-related and non-confidentiality-related. Confidentiality-related breaches involve attacks where an intruder can gain access into a system and steal sensitive information. Nonconfidentiality-related breaches include attacks such as denial of service (DoS) where the most likely scenario is a disruption and/or a downtime. Typically, confidentiality breaches are considered more serious, causing significantly more losses than non-confidentiality-related breaches. Hovav and D'Arcy [30]) show that DoS attacks are not associated with any significant loss in market value for a firm. Therefore, we hypothesize that

H4. *A software vendor suffers a greater loss in market value when the vulnerability facilitates confidentiality-related breaches.*

3.2.3 Severity of the Vulnerability

The impact of a software flaw on a vendor also depends on how severe the vulnerability is. More severe vulnerabilities tend to cause higher customer loss. Davidson and Worrell [17] conduct an event study with product defect announcements in the tire industry and show that the impact of severe flaws (which involve a recall) is more than that of less severe flaws (which involve repairs but not a recall).

H5. *A software vendor suffers more losses in market value when the vulnerability is severe.*

3.2.4 Source of Vulnerability

A recent article in the *Wall Street Journal* hints that firms are using vulnerability disclosure as a strategic weapon against competitors. For example, ISS disclosed a vulnerability in rival Checkpoint's flagship firewall product just ahead of Checkpoint's investor summit. Vendors themselves disclose vulnerability information in their products routinely. In fact, many users believe vendors would prefer not to disclose information at all but fear that someone else will disclose it. Generally vendors, as opposed to a third party, are likely to be more careful about the disclosure. Moreover, disclosure by vendors would signal their commitment to providing secure software. Therefore,

H6. *The loss in market value for a software vendor is lower when the security vulnerability is discovered by the vendor itself rather than by rivals or third-party security firms.*

4 Data Description and Methodology

4.1 Data

Our data comes from the vulnerability disclosures in the popular press as well as the advisory reports from CERT/CC.[9] We include articles published by news networks such as Businesswire and Newswire and daily articles in popular press outlets such as the *Wall Street Journal*, the *New York Times*, the *Washington Post* and the *Los Angeles Times*. We search for these news articles in Proquest and Lexis-Nexis Academic databases which, between them, maintain news articles from major newspapers and news networks all over the country. We also include articles from News.com, which is a CNET-owned site and is a premier source for up-to-date technology news coverage. We used the following terms in our search: "vulnerability AND disclosure," "software AND vulnerability," "software AND flaw," "virus AND vulnerability," and "vulnerability AND patch." Some examples of vulnerability announcements reported in the popular press are:

1. *News.com* (25 April 2000). "A computer security firm has discovered a serious vulnerability in RedHat's newest version of Linux that could let attackers destroy or deface a Web site—or possibly even take over the machine itself..."
2. *Wall Street Journal* (11 February 2004). "Microsoft Corp. warned customers about serious security problems with its Windows software that let hackers quietly break into their computers to steal files, delete data..."

We searched the vulnerability announcements for information on the type of vulnerabilities. Based on this information, we classify vulnerabilities into various categories:

- If the announcements contain words such as "serious," "severe," or "dangerous" to describe the vulnerability, we characterize the vulnerability as "Severe." If the announcement characterizes the vulnerability as "moderately severe" or "with low severity," we characterize it as "Nonsevere."
- The vulnerability announcements also have references to what kind to security breach could be facilitated if attackers exploited the vulnerability. If the vulnerability contains terms such as "cause denial of service" or "disrupt operations," we classify the vulnerability as type "DoS"; otherwise, if the vulnerability contains terms such as "gain access," "steal information," or "take control," we classify the vulnerability as "Confidentiality Related."
- Further, the announcements also describe whether the vendor released a patch at the time of the vulnerability announcement. If the vendor announces a patch at the time of vulnerability disclosure, we classify the vulnerability as "Patch Available."
- Finally, we also classify vulnerabilities on whether an "exploit" exists for the vulnerability in the public domain. If the vulnerability announcement contains terms such as "an exploit for the vulnerability is circulating," we classify the vulnerability as type "Exploit Available."

As per convention in prior event-study literature [27], we exclude the following type of announcements from our sample:

- Vulnerability announcements in nondaily periodicals, such as magazines, because of the difficulty in determining the exact date of the announcement.
- Repeat announcements of the same event in a different publication at a later date. In a case of such repeat announcements, the earliest announcement date is chosen as the event day.
- Announcements associated with other confounding events, like stock splits and mergers, on the event date.
- Announcements related to firms not traded on any public exchange in the United States.
- Announcements that point to a fundamental protocol flaw rather than a particular software. For example, a flaw in the FTP protocol affects multiple vendors. The reason behind dropping this category is that the flaw exists in the software only because it follows a flawed protocol and not due to the vendor.
- Software flaws that are not security related.

Our data set contains 147 vulnerability announcements pertaining to 18 firms between January 1999 and May 2004. A list of software vendors, their market capitalization

[9] The Center for Emergency Response/Coordination Center is a federally funded organization whose key job is to disseminate vulnerability related information to the user population.

values, and the number of vulnerabilities announced during this period for each vendor is provided in the Appendix. The vulnerabilities affect different types of software, such as firewalls, operating systems, e-mail-servers, Web servers, browsers, media players, and network management software, to name a few. For each such event, we also capture the date of the event, the affected firm and product, who discovered the flaw, the news source, whether a patch is available, whether an exploit is circulating, and severity of the flaw.

4.2 Methodology

We use the standard event-study methodology for this analysis. An event study assumes that an event of interest (in our case, the vulnerability disclosure announcement) significantly impacts returns on a stock. The period of interest for which we observe the event is known as the event window. The smallest event window is one day (day of the announcement, or "day 0").[10] In practice, the event window is often expanded to include two days (day 0 and day 1) to capture the effect of price announcements made after the close of the markets on a particular day.[11] Sometimes, researchers include a day before the announcements to incorporate any information leaks about the event. In our study, we define a one-day event window (day 0).[12] Hendricks and Singhal [27] cite two reasons to use a one-day event period. 1) A shorter event period permits a better estimation of the effects of information on stock prices since it reduces the possibility of other confounding factors not related to the announcement. 2) It also increases the power of the statistical tests.

Abnormal returns are defined as the difference between the actual return of the stock over the event window minus the expected return of the stock over the event window. The expected return on the stock is calculated in several ways, but in our analysis, we use the market model, which assumes a stable linear relation between the market return and the return on the stock. We also verify our results using other methods, such as the market-adjusted method and the mean-adjusted method ([10], [27]).

4.2.1 The Market Model

In the market model, the abnormal returns for a stock are estimated as follows:[13]

$$AR_{it} = R_{it} - \alpha - \beta_{it} R_{mt}, \tag{1}$$

where i denotes the event $(i = 1, 2 \ldots \mathrm{N})$, m denotes the market, and t denotes the day of the event ($t = 0$ denotes the day of the vulnerability announcement). AR_{it} is the abnormal return of event i at time t, which is the difference between the actual return and the expected normal return. R_{it} denotes the actual return and R_{mt} denotes the market return at time t.[14] $\alpha + \beta_{it} R_{mt}$ is the expected normal return of the firm due to the marketwide movement. Thus, abnormal return is the part of the actual return that market movements cannot explain and, hence, captures the effect of the event. Since most of the technology stocks are listed on NASDAQ, we use NASDAQ as our indicator for market returns. We use ordinary least squares regression (OLS) to estimate the coefficients α and β for the above regression by choosing a portion of the data as the estimation window. (OLS is a popular technique used to analyze how some independent variables (in this case, market return R_{mt}) affect a dependent variable (in this case, actual return R_{it}). See http://dss.princeton.edu/online_help/analysis/regression_ intro.htm for an excellent introduction to regression analysis. Goldberger [22] and and Greene [25] provide a detailed overview of regression analysis. The estimation window, generally between the 120 days and 200 days used in most studies, is the period immediately before the event window. In our case, we use an estimation window of 160 days, from $\mathrm{day}\ -175$ to $\mathrm{day}\ -16$.

4.2.2 The Market-Adjusted Model

In this case, the abnormal returns are given as

$$AR_{it} = R_{it} - R_{mt}, \tag{2}$$

where the terms have similar meanings as in the Market Model.

4.2.3 The Mean-Adjusted Model

$$AR_{it} = R_{it} - \bar{R}_i, \tag{3}$$

where $\bar{R}_i = \sum_{s=1}^{T} R_{is}$ is the mean return for the stock. The mean is calculated by averaging the return over the estimation window (from -175 to -16 days). Thus, T is the number of days in the estimation period (in our study, $T = 160$).

Since we have N observations (or $N = 147\ \mathrm{events}$), the mean abnormal return across all observations on day t of the event is given as $\bar{A}_t = \sum_{i=1}^{N} AR_{it}$ The Cumulative Abnormal Return $CAR = \sum_{event} \bar{A}_t$ for the event is defined as the sum of the abnormal returns over the event window. To be able to do hypothesis testing (to determine if CAR is significantly different from 0), we also need to calculate the standard error for the calculated CAR. Brown and Warner [7], [8] present a comprehensive analysis of suitable test statistics for the abnormal mean return. Since multiple vulnerabilities may be disclosed on a given day, our statistic should allow for event-day clustering. Based on [8] (also used by [27]), the standard error $S_{\bar{A}}$ is given by $-S_{\bar{A}}^2 = \frac{1}{T-1}(\sum_{s=1}^{T}(\bar{A}_s - \bar{\bar{A}}))$, where T is the number of days in the estimation period and $\bar{\bar{A}} = \frac{1}{T}(\sum_{s=1}^{T} \bar{A}_s)$. Given this standard error we can calculate the following t-statistic, which can be used to test whether the abnormal return is different from zero:

$$t = \frac{CAR}{\sqrt{S_{\bar{A}}^2}}. \tag{4}$$

The null hypothesis is that the abnormal returns are not significantly different from zero. We also perform a regression analysis and test our hypotheses of how CAR varies with vendor characteristics and vulnerability characteristics. But,

[10] If an announcement is made on a day when the markets are closed, we consider the next day the markes open as day 0.

[11] Day 1 is the day after the announcement.

[12] We also explore different values of the event window.

[13] R_{it} for a stock is the percent change in the stock price at time t, $(= P_{it} - P_{it1})/P_{it_1}$.

[14] We obtain the data on the stock and market returns from Yahoo Finance (http://finance.yahoo.com).

TABLE 1
Cumulative Abnormal Return

Day 0 **CAR**	**Market Model**	**Market-Adjusted Model**	**Mean Model**
Mean Abnormal Return	-0.63 (*0.01*)	-0.67 (*0.01*)	-0.5 (*0.09*)
Median Abnormal Return	-0.44 (*0.00*)	-0.5 (*0.00*)	-0.55 (*0.01*)
Percent Less than Zero	64 percent (*0.00*)	63.5 percent (*0.001*)	58.7 percent (*0.03*)

TABLE 2
CAR for Various Time Periods

Day	**-1**	**0**	**0 to 1**	**0 to 2**	**0 to 5**	**0 to 10**
CAR **(p-value)**	0.25 (0.4)	-0.63 (0.01)	-0.65 (0.07)	-0.47 (0.35)	-0.25 (0.7)	-0.8 (0.36)

before we present the details on our regression analysis, we present the results of the event study.

4.3 Event-Study Results

Table 1 summarizes the results of our event study and quantifies the effect of vulnerability disclosures on the stock prices of software vendors for our entire sample of 147 announcements (p-$values$ are in parentheses—mapping between p-values and t-statistics is readily available through t-tables).

We calculate CARs under three different models (Market Model, Market-Adjusted Model, and Mean-Adjusted Model). For each of the three models, we use three different test statistics (Mean Abnormal Return, Median Abnormal Return, and Percent Less than Zero). The Mean Abnormal Return Test ((1)-(4)) is parametric in nature and makes assumptions about the distribution of abnormal returns. We also use two nonparametric tests to strengthen our results. We use the Wilcoxon Signed Rank Test to calculate the p-value for the median abnormal return, and we use the Sign Test to calculate the p-value for the percent negative returns. The Sign Test is based on the sign rather than the magnitude of the abnormal returns and requires that, under the null hypothesis, the proportion of abnormal returns greater than (or less than) zero is 50 percent.

From Table 1, we note that the CAR for day 0 is negative across all three different models and the Mean Abnormal Return varies between 0.5 percent and 0.67 percent depending on the model used. Further, the Market Model and the Market-Adjusted Model are statistically significant at $p < 0.01$, whereas the Mean-Adjusted Model is statistically significant at $p < 0.1$ level. The Median Abnormal Returns range between 0.44 percent and 0.55 percent and are significant at the $p < 0.01$ level. Finally, the percentages of observations less than zero range between 57.8 percent and 64 percent and are significant at the $p < 0.05$ level. CAR is clearly negative and statistically significant for all three models and all three tests. We also calculate the abnormal returns using different event windows (beyond 0 days) using the market model (the results do not change substantially for other models). The results are given in Table 2.

From the table, CAR on day 0 is clearly negative and significant at the 0.01 level. The CAR for day 0 and day 1 combined is negative and significant at the 0.1 level. The p-value for $\text{day} - 1$ is neither negative nor statistically significant, suggesting little or no impact of news leakage. The CARs in columns 3, 4, 5, and 6 are negative but not statistically significant. Interestingly, the CARs are negative and large for even a 10-day window.

Overall, our results suggest that software vendors lose market value when a vulnerability is announced in their product. This result is robust across various models and across various statistical tests. The result provides support for hypothesis *H1* that vulnerability announcements are associated with a loss in the market value of software vendors. This result also corroborates prior work on defective products [33], [17] by showing that product defects lead to a significant loss in a firm's market value. The extent of losses a vendor suffers, on average, is about 0.63 percent of its market capitalization value on the day the vulnerability is announced.

4.3.1 Market Capitalization

Next, we calculate the abnormal change in market capitalization values of the software vendor due to the vulnerability announcement.[15] For each firm, the day 0 change in market capitalization value is calculated by multiplying the $\text{day} - 1$ market capitalization value by the abnormal returns on day 0. On average, we find that the software vendors in our sample lost $0.86 billion in market capitalization value on the day of the vulnerability disclosure. Since Microsoft accounts for more than 40 percent of our sample, we subdivide our sample into Microsoft and non-Microsoft samples. For the Microsoft sample, the average change in market capitalization is around $0.92 billion. For the non-Microsoft sample, the average change in market value is $0.81 billion.

[15] We obtain the market capitalization values from the CSRP database by multiplying the share price by the number of shares outstanding.

4.3.2 Robustness Checks

We also perform the following robustness checks on our results, as specified in the event study by Cooper et al. [15].

1. **Robustness to Outliers.** To check the robustness of our results to exclude the effect of outliers, we compute the CAR for our sample after excluding the top 10 percentile and the bottom 10 percentile of observations (ranked according to the day 0 mean abnormal returns). We find that our results remain qualitatively the same. For example, mean abnormal returns for this sample are 0.53 percent (against 0.63 percent for the entire sample) and these are significant at the 5 percent level, suggesting that our results are robust to outliers in the data.
2. **Momentum Effect.** One can argue that the day 0 abnormal returns are caused simply by market momentum rather than by the underlying event. For example, the movement of stock returns on days prior to the event influences the stock returns during and after the event in some way. To check whether this correlation between stock returns prior to the event, during the event, and after the event is significant, we perform a simple check proposed by Cooper et al. [15]. We compute the correlation between the abnormal returns before the event and those during/after the event. Specifically, we check the pairwise correlation (along with the level of significance) for three pairs of values: 1) $\mathrm{day}\ -10$ to $\mathrm{day}\ -1$ CAR and $\mathrm{day}\,0$ to $\mathrm{day}\,10$ CAR, 2) $\mathrm{day}\ -10$ to $\mathrm{day}\ -1$ CAR and $\mathrm{day}\,0$ CAR, and 3) $\mathrm{day}\ -1$ CAR and $\mathrm{day}\,0$ CAR. The pairwise correlations are as follows:

   - $\mathrm{day}\ -10$ to $\mathrm{day}\ -1$ CAR and $\mathrm{day}\,0$ to $\mathrm{day}\,10$ CAR ($correlation\ 0.13$, $p\text{-}value\ 0.12$),
   - $\mathrm{day}\ -10$ to $\mathrm{day}\ -1$ CAR and $\mathrm{day}\,0$ CAR ($correlation - 0.05$, $p\text{-}value 0.5$), and
   - $\mathrm{day}\ -1$ CAR and $day\,0$ CAR ($correlation\ 0.03$, $p\text{-}value\ 0.67$).

Thus, we find that none of the correlations is strong or significant at the 10 percent level and, hence, we rule out the possibility that momentum in the stock prices drives our results.

5 Regression Analysis

To test other hypotheses, we now develop a regression model to explain the effect of various firm-specific and vulnerability-specific characteristics on abnormal returns. Regression analysis is a common econometric tool to model relationships between variables and used by prior event studies such as [28] and [13]. The regression model can be specified as

$$AR_{it} = \beta X_i + \gamma Z_i + \varepsilon_i, \tag{5}$$

where $i = 1 \ldots N$ (N is the total number of events). The Abnormal Return (AR_{it}) for event i is calculated according to the market model in (1).[16] X_j and Z_j are the independent variables that capture the firm-specific and vulnerability-specific characteristics, respectively, corresponding to the $i\mathrm{th}$ event (vulnerability announcement). The description of the independent variables is as follows.

5.1 Firm-Specific Characteristics

Firm size is measured as the variable $LASSETS$, which is the natural logarithm of the total assets of the firm (measured in millions of dollars).

We measure diversification ($DIV\}$) in terms of the Herfindahl index, which is a common measure of diversification [40]. The Herfindahl index of a firm is measured as $DIV = \sum_{i=1}^{N} P_i \cdot Log(\frac{1}{P_i})$, where N is the number of segments in which the firm operates and P_i is the ratio of segment is revenue to total firm revenue (segment revenues and other details are reported in the SEC (Security and Exchange Commission) filings that every publicly traded firm has to file). For a firm that is nondiversified (i.e., operates in only one segment, $P_i = 1$), $DIV = 0$. The more diversified a firm is, the higher the value of DIV.

To measure market competition, we define a binary variable (commonly referred to as a dummy variable), $COMP$, where $COMP = 1$ if the product operates in a competitive market and $COMP = 0$ if the product has a monopoly. A dummy variable is a variable that can only take discrete values of 0 and 1.[17] We define the firm as a monopolist if its product has more than 50 percent market share and the nearest competitor has at least 20 percent less market share than the leader. For example, Internet Explorer has a market share of more than 75 percent, which is far more than that of competitors, such as Firefox. Therefore, $COMP = 0$ for Internet Explorer and $COMP = 1$ for Firefox. On the other hand, the Windows server operating system has a market share of 40 percent, which is similar to competitors such as Linux; therefore, $COMP = 1$ for the Windows server operating system (market share information collected from industry sources such as News.com).

A firm's growth rate also determines how the market will react to a vulnerability in its products. As Hendricks and Singhal [29] suggest, many new customers enter the market during times of high growth. These customers may experience lower switching costs as compared to the "older" customers and therefore may be more willing to avoid defective software. Therefore, the potential for more lost sales is greater during periods of high growth. We represent firm growth by the variable $FGROWTH$, which measures the rate of growth of the firm (measured as the percent change in total firm revenues compared to the previous year).

We also measure the number of times vulnerability, n, was reported in a product within the last 12 months prior to the announcement date. We use a transformed variable $FREQ = 1/(1 + e^n)$ in our regression (a log transformation gives similar results).

[16] Since the market model is the most common model event studies use, we proceed with the remaining analysis with this model.

[17] Dummy variables are variables that can take only two values: 0 or 1. These variables are used to represent categorical data (e.g., gender) in regression analysis. See http://dss.princeton.edu/online_ help/analysis/dummy_variables.htm for a brief overview of dummy variables.

TABLE 3
Descriptive Statistics on Firm Specific Variables

Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

We collect information on the firm financials, such as firm revenues, segment revenues, and total assets, from the Compustat database. Table 3 gives the descriptive statistics of the firm-specific variables in our data. The terms in brackets give the standard deviation on the nonbinary variables.

5.2 Vulnerability Characteristics

We measure patch availability, confidentiality breaches, severity, exploit code availability, and whether the vulnerability was first identified by the vendor or by a third party or competitor.

- $PATCH$—where $PATCH = 1$ if a patch is available at the time of the vulnerability announcement.
- $TYPEC$—where $TYPEC = 1$ if the vulnerability can allow potential intruders to steal confidential information ($TYPEC = 0$ signifies that the vulnerability can be exploited to cause a nonconfidentiality-type attack, such as a DoS attack).
- $SEVERE$—where $SEVERE = 1$ if the vulnerability is categorized as severe or serious.
- $EXPLOIT$—where $EXPLOIT = 1$ if an exploit is publicly circulating when a vulnerability is discovered.
- $DISC$—where $DISC = 1$ if the firm itself discovers the vulnerability and $DISC = 0$ if third parties, such as competitors or independent researchers, discover the vulnerability.

5.3 Control Variables

We use a variable $PRESS$ to control for the source of the vulnerability announcement. $PRESS = 1$ if the vulnerability is announced in the popular press and $PRESS = 0$ if the vulnerability is announced in industry sources such as CERT. To control for abnormal returns due to overall market sentiments, we introduce a set of dummy variables based on the time the vulnerability was announced. We use the events surrounding 9/11 as the basis for segmenting our sample into various time periods. The stock market crash in late 2000 could also have played a role in the negative abnormal returns. We introduce the following dummy variables in our model:

- $POST\_911$—It is 1 if the vulnerability was announced between 11 September 2001 and 11 September 2002, and 0 otherwise.
- PRE_911—It is 1 if the vulnerability was announced between 11 September 2000 and 11 September 2001. This was also the time after the stock market crashed in mid-2000 and lasted until the first three quarters of 2001 (*Wall Street Journal*, 2000;[18] [35]; *Wall Street Journal*, 2003[19]).
- $Y00$—It is 1 if the vulnerability announcement is between 1 January 1999 and 11 September 2000.
- $Y0203$—It is 1 if the vulnerability announcement is between 11 September 2002 and 11 September 2003.
- $Y0304$—It is 1 if the vulnerability announcement is between September 11, 2003 and 1 June 2004. This is the baseline category for our regression.

TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	Mean
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

The descriptive statistics on the vulnerability characteristics variables and control variable are (as fractions of total vulnerability announcements) as shown in Table 4.

5.4 Results

The results of the regression model outlined in (5) are presented in Table 5. We present the parameter estimates as well as their associated p-values. We do not find major correlation (> 0.4) between any two independent variables.

The R^2 for this regression is 23.7 percent and the adjusted R^2 for the model is 16.2 percent, which are quite large for models that attempt to explain abnormal stock returns. The F-test (p-value 0.0006) for the overall model suggests that our model is highly significant. We also run diagnostic tests on our model to check whether the assumptions of least squares regression hold. The White test rules out heteroskedasticity in our model. We also calculate the variance inflation factors (VIF) for our model and estimate that all our VIFs are below the recommended level of 10. Our regression provides several interesting observations regarding the effect of firm and vulnerability-specific characteristics on the vendor's stock price. We find that the coefficient of the $COMP$ variable is negative and significant, suggesting that vendors lose more market value if the product operates in a competitive market. Specifically, the vendor loses 0.6 percent more market value if the market for the product is competitive than if it is a monopoly. Finally, we also find that larger firms lose less market value than smaller firms since the coefficient of $LASSETS$ is positive and significant; on average, the loss in market value increases by 0.56 percent if the total assets

[18] Article titled "The Internet Bubble Broke Records, Rules and Bank Accounts," 14 July 2000.

[19] Article titled "Thinking Things Over: On Repairing Economic Damage," 10 March 2003.

TABLE 5
Regression Estimates

	Proxy for	Variable	Coefficient
Firm Characteristics	**Competitiveness**	**COMP**	***-0.006**** (0.07)
	Growth	**FGROWTH**	- 0.007 (0.43)
	Diversification	**DIV**	-0.007 (0.55)
	Size	**LASSETS**	***0.0056***** (0.04)
Vulnerability Characteristics	**Available Exploit**	**EXPLOIT**	-0.0047 (0.22)
	Fix Availability	**PATCH**	***0.0082***** (0.03)
	Source of Discovery	**DISC**	-0.055 (0.11)
	Type of Attack	**TYPEC**	-0.005 (0.14)
	Severity	**SEVERE**	***-0.0067***** (0.08)
Control Variables	**Disclosure Source**	**PRESS**	-0.004 (0.28)
	Frequency of Vulnerability	**FREQ**	-0.002 (0.8)
	Year	**Y00**	0.002 (0.7)
		PRE_911	-0.006 (0.26)
		POST_911	***-0.018****** (0.00)
		Y0203	-0.007 (0.11)
		CONSTANT	-0.003 (0.8)
R- Square			23.7 percent
F-value (significance)			***2.7****** (0.00)

**** denotes significance at the 1 percent level, ** denotes significance at the 5 percent level, and * denotes significance at the 10 percent level.*

of the firm decrease by 1 percent. The rest of the firm-specific variables—$FGROWTH$ and DIV—are not significant, suggesting that the growth rate of the firm and the degree of diversification do not play a significant role.

Vulnerability-specific variables also determine how much the market punishes a software vendor due to a vulnerability announcement. The coefficient of the $SEVERE$ variable is negative and significant. More severe vulnerabilities have a higher potential to cause damage and, hence, have a larger adverse impact on CAR. On average, a severe vulnerability can cost a software vendor 0.67 percent more than a nonsevere vulnerability. The coefficient of $PATCH$ suggests that the nonavailability of a patch is positive and significantly correlated with the market value. On average, firms that do not provide a patch at the time of the vulnerability disclosure suffer a loss of 0.82 percent more than firms that provide a patch. None of the other vulnerability-specific coefficients are significant. Our result that the coefficient of the $DISC$ variable is not significant is especially interesting because it suggests the markets do not penalize a vendor any more if a third party discovers the vulnerability than if the vendor itself discovers it.

We also find that the coefficient of the $POST\_911$ variable is negative and significant, suggesting that the loss suffered by software vendors due to security flaws was the greatest during the one year period following 9/11; for example, on average, vendors lost 1.8 percent more in market value for each vulnerability announcement in the year following 9/11 than they did in the baseline period (2003-2004). This suggests that security concerns among investors were highest during this period, as an aftermath of 9/11. The other coefficients of the time specific variables are not significant, suggesting that there is no significant difference in abnormal returns across different time periods.

6 Conclusions and Discussion

This research addresses an interesting and contemporary issue of whether software vendors are adversely affected by security-related vulnerability announcements in their products. Prior studies in other industries mostly suggest vendors suffer a loss in market value when defects are announced in their products. However, the unique characteristics of the software industry suggest that the potential damage to software vendors' future profitability may be minimal. This is the first study to analyze the impact of all security-related product defects on software vendors. Our analysis of 147 different security-related vulnerability incidents related to 18 vendors and announced in popular press and industry sources, such as CERT, suggests that the loss in market value for software vendors is negative and significant. We find that, on average, vendors lose 0.63 percent in market value on the day the vulnerability is announced. This translates to an average loss of \$0.86 billion and indicates that the stock markets react negatively to the news of a vulnerability disclosure because the discovery of a vulnerability could suggest a loss in future cash flow of the software vendors.

We also show that the average loss of 0.63 percent is conditioned by various factors. Actual loss depends on many vulnerability and vendor/market characteristics. We find that vendors lose more value in competitive markets. One possible reason is that in a competitive market, customers have many options from which to choose. Our results also suggest that larger software vendors are less affected by vulnerability disclosures than smaller vendors. We also show that the loss in market value differs across types of vulnerabilities. Releasing a patch with the announcement greatly reduces the loss in market share. This result is interesting for the managers because a corrective action can somewhat mitigate the impact of a bad event (vulnerability disclosure). We further find that more severe vulnerabilities and confidentiality-related vulnerabilities cause more stock price losses. A possible reason is that such vulnerabilities also have a large potential to cause more customer losses.

6.1 Significance of Our Results and Business Implications

Given our findings, an interesting question arises: Should firms care about such movement in stock price?[20] Firms lose and gain market value over the normal course. The event-study methodology used in our analysis, which is also extensively used in finance and accounting literature, assumes any event that produces an impact over and above the normal ups and downs in the price of a stock is of interest to managers. In fact, if the markets are efficient and rational, then event studies should correctly measure the long-term economic impact of an event [37]. In other words, in the absence of the event, the stock price of the firm at any time would have been higher. As [36] suggests, "In a corporate context, the usefulness of event studies arises from the fact that the magnitude of abnormal performance at the time of an event provides a measure of the (unanticipated) impact of this type of event on the wealth of the firms' claimholders. Thus, event studies focusing on announcement effects for a short horizon around an event provide evidence relevant for understanding corporate policy decisions." Like any economic model, the event-study literature assumes capital markets are efficient and people have full information, and, hence, any loss in market capitalization is due to reduction in future cash flows (which, in the case of software vendors, could be due to loss of revenues as customers shift to competitors or due to the cost of spending resources in developing a patch for the flaw). In short, event studies indeed measure the overall economic impact of vulnerability disclosures (even if the stock prices eventually increase because of other, positive events). However, whether or not the event studies correctly measure the long-term impact, a key finding of our paper is that investors pay attention to the news of software vulnerabilities. This finding in itself is interesting and runs counter to the notion that security is not worth the investment and customers would rather have more product features than security.

Our paper also points to the fact that having a vulnerable product (and associated bad press) does generate negative outcomes for the firm. In fact, the recent uproar over AOL mishandling search query data (two employees were fired and the chief technology officer resigned) indicates that managers need to pay attention to these issues carefully. From the press material, it seems that managers do seem to care about security (e.g., Microsoft's special focus on security).

In summary, our study points to the fact that product defects hurt software vendors and that the managers need to pay attention to associated bad press as well as stock price slide. In particular, our paper provides some evidence that a more secure product can generate positive value for a firm. Thus, although vendors would like to launch software products as soon as possible, our study shows they need to focus testing in areas that can potentially contain a greater number of security vulnerabilities. Our study also provides preliminary evidence that firms should integrate security into software quality practices.

We should stress that event studies are just one of the methodologies for understanding this phenomenon and market value is only one of the metrics for quantifying the impact of a defective product on the firm's value. A more interesting and comprehensive work would be to measure the impact on profit or market share of these firms and what the economic value of security is. Our paper paves the way for such future research and provides a starting point for why we should analyze this issue in more detail.

6.2 Implications for Software Quality and Disclosure Policy

As we noted in the Introduction, one major argument the full disclosure group gives is that disclosure will eventually force the vendors to improve the quality of their product. Our analysis finds some support for this argument. Disclosure, in general (with or without a patch), adversely affects the market valuation of the vendors. It is more severe in cases without patches (which is what generally happens during full disclosure). Thus, disclosure clearly creates some incentives for vendors to produce better-quality software.

Our discussion clarifies why vendors are pushing for a limited disclosure policy. Recently, the Organization for Internet Safety (OIS), which is a consortia of 11 large software vendors, announced a limited disclosure policy that requires the discoverer to notify the vendors and give them some time before making the information public. We find that such a policy benefits vendors because limited disclosure gives them the time to release a patch for the vulnerability, and the availability of a patch mitigates some adverse effects of disclosure. Generally, an argument could be made that vendors should release the information themselves; otherwise, someone else will, thereby leading to worse consequences. However, we do not find any evidence for such an argument. However, our results do suggest that vulnerability news is bad news for vendors and they are probably better off keeping quiet and integrating their fixes as either service packs (which do not give microdetails on what it fixes) or newer versions and announce the patch only if someone else has disclosed it.

Another issue raised in discussing software flaws is whether laws should hold software vendors responsible for vulnerabilities discovered in their products. Industry experts generally believe software vendors do not have enough incentive to invest in defect-free software and that legal liability is required to compensate users for losses due to security flaws and to encourage vendors to invest more

[20] The authors thank an anonymous reviewer for raising this issue.

TABLE 6
Summary of Previous Event Studies

Classification of Event Study	Authors	Time Period	CAR
Impact of Vulnerability Disclosures on Software Vendors	This research	1999-2004	-0.63%
Impact of Security Breaches on Firms	Campbell K, Gordon LA, Loeb MP and L Zhou (2003)	1995-2000	-2.0%*
	Cavusoglu H, Mishra B and S Raghunathan (2004)	1998-2000	-2.0%
	Hovav A and J D"Arcy (2003)	1998-2002	Not Significant
	Kannan K, Rees J and S Sridhar (2004)	1997-2003	-0.73%
Impact of Product Recall Announcements	Jarrell G and S Peltzman (1985)	1967-1981	-0.81% (for auto)
	Davidson WL III and DL Worrell (1992)	]1968-1987	-0.36% (day -1)
Impact of IT Investment Announcements	Chatterjee D, Richardson VJ and RW Zmud (2001)	1987-1998	1.16%
	Im KS, Dow KE and V Grover (2001)	1981-1996	Not Significant
	Subramani M and E Walden (2001)	Oct 1998-Dec 1998	7.5%
	Dos Santos BL, Peffers K and DC Mauer (1993)	1981-1988	1%
Impact of Winning a Quality Award	Hendricks KB and Singhal VR (1996)	1985-1991	0.59%

** Not significant at the 10 percent level.*

in creating defect free software. Our results show that liability laws (which are quite controversial in the United States [43]) are not the only way to "punish" software vendors for flaws discovered in their products and that the stock market does penalize the vendors for software flaws. We show that the investors do act on disclosure announcements and that vendors, on average, lose around 0.63 percent of market value on the day a vulnerability is reported. Software liability could certainly cause the market value of the vendors to decline further in case of a vulnerability announcement.

6.3 Comparison with Prior-Event Studies

Finally, we compare our results with the prior event-studies in related fields. Specifically, we highlight the quantitative results in the following categories: security-breach-related announcements, IT-investment-related announcements, and product-defect-related announcements.

Hovav and D'Arcy [31] show that virus-related announcements do not have a detrimental impact on the stock price of software vendors. Our results show proof to the contrary. Two reasons for this exist: 1) The focus of [31] is virus-related announcements. During our data collection process, we noticed that virus attacks usually exploit some known software vulnerability. Therefore, virus attacks are not a new announcement about a product defect but are rather a manifestation of some previously known vulnerability. 2) Our study includes a broader range of software product defects than [31].

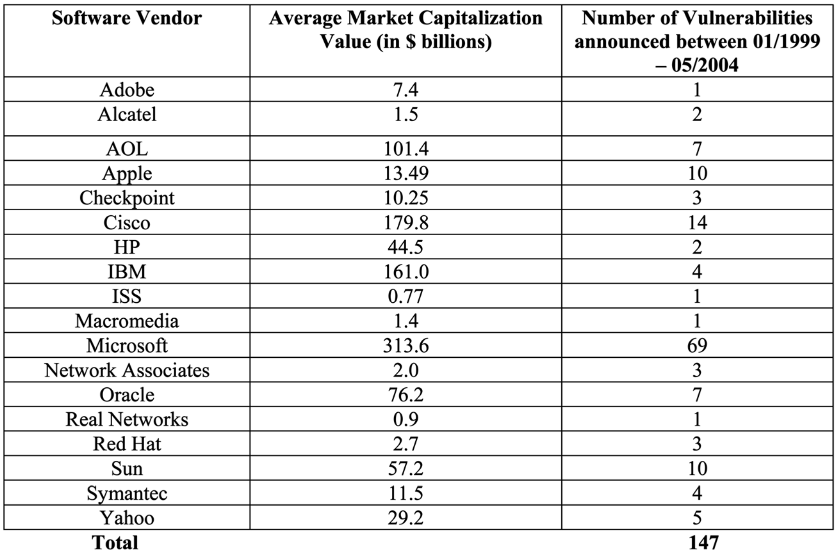
Table 6 shows that our results are comparable to prior studies on product defects and product recall announcements. Although making a direct comparison between the quantitative results of these studies may not be fair due to the different settings involved, we would like to make the observation that the loss in market value vendors suffer due to a security vulnerability is much less than that suffered by firms during a security breach (across all three studies on this topic). A possible reason could be that software vendors are protected by click-wrap agreements and have only limited liability for any flaw in their products. Another reason is that firms usually supply a patch with the vulnerability disclosure (almost 76 percent of the observations in our sample have a patch available at the time of disclosure) and all security vulnerabilities may not result in an actual breach. Sometimes, security breaches are not so much caused by unprotected vulnerabilities as by the lack of adequate patching. For example, the SQL Slammer virus, which affected millions of servers worldwide, was created when hackers exploited a 6-month-old vulnerability in SQL. Microsoft had already released a patch for the same, but, as the Slammer demonstrated, many firms had not adequately protected their servers by applying the patch.

In summary, we find a robust and consistent negative effect of vulnerability announcements on software vendors' market value. However, our study is not without limitations. We have focused on publicly traded firms and, therefore, some large firms such as Microsoft are over-represented in our sample. Future work should try to include smaller private firms as well.

APPENDIX

In this Appendix, we provide details of the data set used in our analysis. Table 7 provides a list of software vendors whose products had a reported flaw between January 1999 and May 2004. Of the 147 unique data points in our sample, 69 were related to Microsoft (~ 47 percent). The market capitalization values in the table below are an average of a

TABLE 7
Description of Software Vendors in the Sample



Software Vendor	Average Market Capitalization Value (in $ billions)	Number of Vulnerabilities announced between 01/1999 – 05/2004
Adobe	7.4	1
Alcatel	1.5	2
AOL	101.4	7
Apple	13.49	10
Checkpoint	10.25	3
Cisco	179.8	14
HP	44.5	2
IBM	161.0	4
ISS	0.77	1
Macromedia	1.4	1
Microsoft	313.6	69
Network Associates	2.0	3
Oracle	76.2	7
Real Networks	0.9	1
Red Hat	2.7	3
Sun	57.2	10
Symantec	11.5	4
Yahoo	29.2	5
Total		**147**

firm's market capitalization values on the day of each event. For example, if firm *A* announced a vulnerability on August 10, 2001 when its market capitalization was $10 billion, and announced another vulnerability on September 21, 2002 when its market capitalization was $9 billion, then the market capitalization value for firm *A* in Table 7 is $9.5 billion.

ACKNOWLEDGMENTS

The authors would like to thank Ashish Arora, Ramayya Krishnan, Sandra Slaughter, participants at the Security Working Group Meeting at the Heinz School of Public Policy, the Workshop on Information Systems and Economics (WISE '04), and the Workshop on Economics of Information Security (WEIS '05) for many helpful comments and suggestions. The authors also thank the associate editor and three anonymous reviewers for many helpful comments. Rahul Telang acknowledges the generous support of the US National Science Foundation (NSF) through the CAREER award CNS-0546009.

REFERENCES

[1] A. Applewhite, "Whose Bug Is It Anyway? The Battle over Handling Software Flaws," *IEEE Software*, vol. 21, no. 2, pp. 94-97, Mar.-Apr. 2004.

[2] R. Anderson, "Why Information Security Is Hard—An Economic Perspective," *Proc. 17th Ann. Computer Security Applications Conf.*, 2001.

[3] A. Arora, J. Caulkins, and R. Telang, "Sell First, Fix Later: Impact of Patching on Software Quality," research note, *Management Science*, vol. 52, no. 3, pp. 465-471, 2006.

[4] A. Arora, R. Telang, and H. Xu, "Optimal Policy for Software Vulnerability Disclosure," *Proc. Workshop Economics of Information Security (WEIS '04)*, 2004.

[5] H. Barki, H. Rivard, S.J. Talbot, "Toward an Assessment of Software Development Risk," *J. Management Information Systems*, vol. 10, no. 2, pp. 203-225, 1993.

[6] V.R. Basiliand and J.D. Musa, "The Future Engineering of Software: A Management Perspective," *Computer*, vol. 20, no. 4, pp. 90-96, Apr. 1991.

[7] S.J. Brown and J.B. Warner, "Measuring Security Price Performance," *J. Financial Economics*, vol. 8, pp. 205-258, 1980.

[8] S.J. Brown and J.B. Warner, "Using Daily Stock Returns: The Case of Event Studies," *J. Financial Economics*, vol 14, pp. 3-31, 1985.

[9] E. Brynjolfsson and C.F. Kemerer, "Network Externalities in Microcomputer Software: An Econometric Analysis of the Spreadsheet Market," *Management Science*, vol. 42, no. 12, pp. 1627-1647, 1996.

[10] J.Y. Campbell, W.L. Andrew, and A.C. MacKinlay, *The Econometrics of Financial Markets*. Princeton Univ. Press, 1997.

[11] K. Campbell, L.A. Gordon, M.P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *J. Computer Security*, vol 11, no. 3, pp. 431-448, 2003.

[12] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *Int'l J. Electronic Commerce*, vol. 9, no. 1, p. 69, 2004.

[13] D. Chatterjee, V.J. Richardson, and R.W. Zmud, "Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO Positions," *MIS Quarterly*, vol. 25, no. 1, pp. 43-70, 2001.

[14] J. Clayman, "Microsoft Security Response Center (A), Case 9B01E019," Richard Ivey School of Business, 2001.

[15] M.J. Cooper, O. Dimitrov, and P.R. Rau, "A Rose.com by Any Other Name" *J. Finance,"* vol. 6, pp. 2371-2387, 2001.

[16] M.A. Cusumano, "Who Is Liable for Bugs and Security Flaws in Software?" *Comm. ACM*, vol. 47, no. 3, pp. 25-27, 2004.

[17] W.L. Davidson III and D.L. Worrell, "The Effect of Product Recall Announcements on Shareholder Wealth," *Strategic Management J.*, vol. 13, no. 6, pp. 467-473, 1992.

[18] P. Devanbu and S. Stubblebine, "Software Engineering for Security: A Roadmap," *Future of Software Eng.*, pp. 225-239, 2000.

[19] B.L. Dos Santos, K. Peffers, and D. Mauer, "The Impact of Information Technology on the Market Value of the Firm," *Information Systems Research*, vol. 4, pp. 1-23, Mar. 1993.

[20] J.M. Gallaugher and Y.M. Yang, "Understanding Network Effects in Software Markets: Evidence from Webserver Pricing," *MIS Quarterly*, vol 26, no. 4, pp. 303-327, 2002.

[21] N. Gandal, "Hedonic Price Indexes for Spreadsheets and an Empirical Test for Network Externalities," *Rand J. Economics*, vol. 25, no. 1, pp. 160-170, 1994.

[22] A.S. Goldberger, *Introductory Econometrics*. Harvard Univ. Press, 1998.

[23] L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investments," *ACM Trans. Information and Systems Security*, vol. 5, no. 4, pp. 438-457, 2002.

[24] L.A. Gordon, M.P. Loeb, and T. Sohail, "A Framework for Using Insurance for Cyber Risk Management," *Comm. ACM*, vol. 46, no. 3, pp. 81-85, 2003.

[25] W.H. Greene, *Econometric Analysis.* Prentice Hall, 2002.

[26] D.E. Harter, M.S. Krishnan, and S.A. Slaughter, "Effects of Process Maturity on Quality, Cycle Time, and Effort in Software Product Development," *Management Science,* vol. 46, no. 4, pp. 451-466, 2000.

[27] K.B. Hendricks and V.R. Singhal, "Quality Awards and the Market Value of the Firm: An Empirical Investigation," *Management Science,* vol 42, no. 2, pp. 415-436, 1996.

[28] K.B. Hendricks and V.R. Singhal, "Delays in New Product Introductions and the Market Value of the Firm: The Consequences of Being Late to the Market," *Management Science,* vol 43, no. 4, pp. 422-436, 1997.

[29] G.J. Holzmann, "Economics of Software Verification," *Proc. Workshop Program Analysis of Software Tools and Eng.,* 2001.

[30] A. Hovav and J. D'Arcy, "The Impact of Denial-of-Service Attack Announcements of the Market Value of Firms," *Risk Management and Insurance Rev.,* vol. 6, no. 2, pp. 97-121, 2003.

[31] A. Hovav and J. D'Arcy, "Capital Market Reaction to Defective IT Products: The Case of Computer Viruses," *Computers and Security,* vol. 24, pp. 409-424, 2005.

[32] K.S. Im, K.E. Dow, and V. Grover, "Research Report: A Reexamination of IT Investment and the Market Value of the Firm—An Event Study Methodology," *Information Systems Research,* vol. 12, no. 1, pp. 103-117, 2001.

[33] G. Jarrell and S. Peltzman, "The Impact of Product Recalls on the Wealth of Sellers," *J. Political Economy,* vol. 93, no. 1, pp. 512-536, 1985.

[34] K. Kannan, R. Telang, "Market for Software Vulnerabilities? Think Again," *Management Science,* vol. 51, no. 5, pp. 726-740, 2005.

[35] K. Kannan, J. Rees, and S. Sridhar, "Reexamining the Impact of Information Security Breach Announcements on Firm Performance," working paper, 2004.

[36] S.P. Kothari and J.P. Warner, "Econometrics of Event Studies," *Handbook of Empirical Corporate Finance,* Espin Eckbo, ed. pp. 33-36, Elsevier-North-Holland, 2007.

[37] A.C. MacKinlay, "Event Studies in Economics and Finance," *J. Economic Literature,* vol. 35, no. 1, pp. 13-39, 1997.

[38] G. McGraw, "Software Security" *IEEE Security and Privacy,* vol. 2, no. 2, pp. 80-83, 2004.

[39] "The Economic Impacts of Inadequate Infrastructure for Software Testing," US Nat'l Inst. of Standards and Technology, http://www.nist.gov/director/prog-ofc/report02-3.pdf, 2002.

[40] K. Palepu, "Diversification Strategy, Profit Performance and the Entropy Measure," *Strategic Management J.,* vol. 6, pp. 239-255, 1985.

[41] M. Paulk, C. Weber, W. Curtis, and M. Chrissis, "The Capability Maturity Model: Guidelines for Improving the Software Process," Software Eng. Inst., Carnegie Mellon Univ., 1994.

[42] C.P. Pfleeger, "The Fundamentals of Information Security," *IEEE Software,* vol. 14, no. 1, pp. 15-17, Jan.-Feb. 1997.

[43] D. Ryan, "Two Views of Security Software Liability," *IEEE Security and Privacy,* pp. 70-73, Jan.-Feb. 2003.

[44] S.A. Slaughter, D.E. Harter, and M.S. Krishnan, "Evaluating the Cost of Software Quality," *Comm. ACM,* vol. 41, no. 8, pp. 67-73, 1998.

[45] M. Subramani and E. Walden, "The Impact of E-Commerce Announcements on the Market Value of Firms," *Information Systems Research,* vol 12, no. 2, pp. 135-154, 2001.

[46] L. Wallace, M. Keil, and A. Rai, "How Software Project Risk Affects Project Performance: An Investigation of the Dimensions of Risk and An Exploratory Model," *Decision Sciences,* vol. 35, no. 2, pp. 289-321, 2004.

[47] H. Wang and C. Wang, "Taxonomy of Security Considerations and Software Quality," *Comm. ACM,* vol. 46, no. 6, pp. 75-78, 2003.

[48] J.C. Westland, "The Cost Behavior of Software Defects," *Decision Sciences,* vol. 37, pp. 229-238, 2003.

Rahul Telang received the PhD in information systems from the Tepper School of Business at Carnegie Mellon University in 2002. He is an assistant professor of information systems and management at the Heinz School, Carnegie Mellon University. Dr. Telang's key research field is in the economics of Information security. He has done extensive empirical as well as analytical work on disclosure issues surrounding software vulnerabilities, software vendors' incentives to provide quality, mechanism designs for optimal security investments in multiunit firms, etc. His work on the impact of vulnerability announcements on vendors' stock price has received wide media coverage. Dr. Telang has received the prestigious US National Science Foundation CAREER award for his research in economics of information security. He has also done extensive work on consumer usage of new technologies (like P2P networks) and the impact of these technologies on market structure. His work on the used book market has been reported in the *New York Times* among other media outlets. His dissertation won the William W. Cooper Doctoral Dissertation Award. His research has been published in leading journals, including *Management Science*, *Information Systems Research*, the *Journal of MIS*, and the *Journal of Marketing Research*. He is on the editorial board of *Management Science and Information Systems Research.*

Sunil Wattal received the bachelor's degree in engineering from BITS Pilani, India, the MBA degree from IIM Calcutta, India, the MS degree from Carnegie Mellon University, and the PhD degree from the Tepper School of Business at Carnegie Mellon University. He joined the MIS Department at the Fox School of Business, Temple University, as an assistant professor in Spring 2007. His research interests include economics of information systems, technology adoption, privacy, software security, and internet marketing.