

**Effect of Vulnerability Disclosures on Market Value of Software Vendors**  
**– An Event Study Analysis**

**Sunil Wattal<sup>\*</sup>, Rahul Telang<sup>\*\*</sup>**

**Carnegie Mellon University**

**September 2004**

---

<sup>\*</sup> [swattal@andrew.cmu.edu](mailto:swattal@andrew.cmu.edu)

<sup>\*\*</sup> [rtelang@andrew.cmu.edu](mailto:rtelang@andrew.cmu.edu)

## **1. Introduction & Literature Review**

The objective of this paper is to estimate the losses that software vendors bear when a vulnerability is disclosed in their product. Software vulnerabilities are increasing grabbing media attention because incidents like SQL Slammer, Code Red and Nimda virus, which cost firms millions of dollars in downtime and damages, were caused as a result of hackers exploiting flaws in various software. In 2003, Computer Emergency Response Team (CERT) reported around 250,000 attacks on the internet (Applewhite 2004). A recent study by NIST in 2002 estimates the cost of faulty software at \$60 bn per year. While the damage that users suffer as a result of security breaches can be measured in terms of downtime and maintenance activity, the cost implication of vulnerability disclosures on the software vendors is not clear. Prior literature on product defects (Jarrell et al 1985) predicts that product recall announcements are associated with loss in market value of a firm. However these results cannot be directly applied to the software industry because of the following characteristics of software products: One, software products generally come with a click-wrap agreement which limits the vendors' liability. Two, vulnerabilities are prevalent in the most software products; so it is not clear if the market will 'punish' each vendor individually when a vulnerability is reported. Three, software vulnerability announcements are generally accompanied with a remedial patch which potentially protects customers from malicious exploits. Hence, the market should not behave adversely towards a vendor if it releases a patch along-with the vulnerability announcement. Motivated by these observations, we try to answer the following research questions: One how does the market value of a software vendor change if a vulnerability is reported for its product? Two, are the negative abnormal returns different for different types of vulnerabilities? Our research has important policy implications in terms of understanding vendors' incentive to improve pre- and post-launch quality of their software products.

Our research follows closely from prior event study analysis (Dolley et al 1933, Campbell et al 1997). We also draw from past empirical research on product defects announcements on shareholder value. Jarrell et al (1985) show that drug and auto recalls have a significantly negative impact on the market value of firms. Davidson et al (1992) confirm the results of prior studies in non-auto industries and also analyze the impact of different types of recall (e.g. total product recall versus a recall for repair; government ordered recall versus voluntary recall). Hendricks et al (1996) study the impact of quality award winning announcements on the market value of firms and observe positive abnormal returns generated by winning a quality award. In the field of Information Systems, Subramani et al (2001) used event study analyses to show that e-commerce announcements lead to positive and significant cumulative abnormal returns (CAR) for firms. Prior event study analyses on information security have focused on the change in market value of firms whose systems are breached (Cavusoglu et al 2002). Prior research on software vulnerabilities mainly comprises of analytical models which study the optimal timing of vulnerability disclosure (Arora et al 2004) or welfare implications of a market mechanism for software vulnerabilities (Telang et al 2004).

## **2. Hypotheses**

Our first hypothesis pertains to the change of market value of software vendors after a security related vulnerability becomes known in their product. Security related announcements have been known to have a negative impact on the share value for firms which report a breach. Cavusoglu et al (2003) show that the net market value of information security vendors, as a group, increases after a firm suffers a security related breach. However, the impact on the individual vendor, whose software vulnerability facilitated the breach, is

not known. Do stock markets penalize a firm if a bug<sup>1</sup> becomes known in its product or do markets by and large ignore these announcements? So the first hypothesis that we test is:

*H1: Cumulative Abnormal Returns (CAR) of a software stock are negatively related to security related vulnerability announcements.*

Our second hypothesis relates to the source of the vulnerabilities. Some vulnerabilities are reported in popular press. Others find mention only in industry sources like CERT. The question which arises is whether both sources are equally influential in affecting a stock's CAR? One would suspect the popular press of being more influential than industry sources because it reaches a broader audience. So our next hypothesis is:

*H2: The magnitude of CAR<sup>2</sup> is more when the vulnerability is reported in popular press than in industry sources.*

Our third hypothesis pertains to whether the software vendor releases a patch for the product at the time of the vulnerability announcement. As per accepted guidelines, vendors are given some lead time to develop a patch for a vulnerability before it is made public. A lack of a patch conveys that the vendor is not able to develop a patch in time. It may also convey a greater loss for the vendors' customers since their systems are open to attacks by possible hackers in the absence of a patch. The third hypothesis is:

*H3: CAR of a stock is greater for vulnerabilities where the software vendor does not release a patch at the time of the vulnerability disclosure.*

Software vulnerabilities can have a strategic implication as well. A recent Wall Street Journal article reports that firms are actively investing in finding flaws in their rivals' software. For example, in Feb 2004, security firm IDS released a vulnerability alert on rival firm Checkpoint's firewall software on the day Checkpoint usually holds its annual US investor conference. The question that we ask is whether firms should spend effort in discovering vulnerabilities in their own product or should they let rivals and independent researchers do the job for them. Therefore our fourth hypothesis is:

*H4: CAR is lower in case the security vulnerability is discovered by the vendor rather than rivals or third party security firms.*

### **3. Data Description & Methodology**

Our data comes from the vulnerability disclosures in popular press as well as from the advisory reports in CERT. We include articles published by news networks like Businesswire, Newswire and daily articles in popular press like WSJ, NY Times, Washington Post, LA Times and Houston Chronicle<sup>3</sup>. We also include articles from news.com which is a CNET owned site and is a premier source for round-the-clock, breaking technology news coverage. We used various search such as: 'vulnerability AND disclosure', 'software AND vulnerability', 'software AND flaw', & 'vulnerability AND patch'. We exclude articles published in non-daily publications like monthly or weekly magazines, since it would be difficult to pin-point the exact date of the vulnerability. We also exclude duplications from our sample. If the same vulnerability is reported on different dates by different papers, we consider on the earliest available report and drop the rest. We further exclude announcements that point to a fundamental protocol flaw rather than a particular software. E.g. 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. Lastly, we also

---

<sup>1</sup> We shall use the terms 'bug', 'flaw' and 'vulnerability' interchangeably in this study.

<sup>2</sup> We use the term CAR to refer to negative cumulative abnormal returns.

<sup>3</sup> We search for 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. For news.com articles, we searched the news.com site directly.

drop articles pertaining to firms which are not publicly traded in any major exchange or in case the stock market data is not available for that firm. We further limit our observations only to those software flaws which could potentially result in a security breach<sup>4</sup>. Our dataset contains 114 vulnerability announcements pertaining to around 15 firms in the time period January 1999 – June 2004. We capture information on the following details about the vulnerability announcement: date, firm name, product, who discovered the flaw, news source, and whether a patch is available.

We use the standard event study methodology for this analysis. Since the analysis uses a fairly well known procedure, we skip the details in our analysis. An event study assumes that returns on a stock are significantly impacted by an event of interest (in our case, the event of interest is the vulnerability disclosure announcement). 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’**<sup>5</sup>). In practice, the event window is often expanded to include two days (day 0 and day 1<sup>6</sup>) to capture the effect of price announcements made after the close of the markets on a particular day. 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)<sup>7</sup>, since we can exactly determine the date of the event. Hendricks et al (1996) cite two reasons to use a one day event period; one, a shorter event period permits a better estimation of the effects of information of stock prices since it reduces the possibility of other factors not related to the announcement. Two, it also increases the power of the statistical tests.

#### 4. Results

Table 1 summarizes the effect of vulnerability disclosures on the stock prices of software vendors for our entire sample of 114 announcements.

**Table 1**

<b>Event Window</b>	<b>CAR(n=114)</b>	<b>t-value</b>
1 day (day 0)	-0.75%	-2.68
3 day(day 0 to day 2)	-0.78%	-1.61
5 day(day -2 to day 2)	-0.6%	-0.96

Our results indicate that for our sample, the CAR is negative and statistically significant at the 1% level for day zero. For day ‘0’ CAR, the Wilcoxon Signed Rank Test gives a Z-value of -4.31; implying that the median % age change in market value is also significantly different from zero at the 1% level. Similarly the 3 day event window also gives a significantly negative CAR value at the 10% level. However, the 5 day CAR, taking into account the days prior to the event does not give any significant CAR, possibly suggesting that the effect of news leakage of the vulnerability disclosure is not significant. Thus our results show that a vulnerability announcement leads to significantly negative cumulative abnormal returns for software vendors. While prior research (Cavusoglu et al 2002) shows that the security market as a whole benefits in the event of a security breach, our results show that the individual software vendor, whose product was compromised, actually suffers a loss in market value. Our result corroborates prior work on defective products (Jarrell et al 1985) by showing that in case of software products too, a defect which compromises the security of customers’ information systems leads to a negative impact on the vendor’s market value.

<sup>4</sup> A security breach is an incident where an intruder could potentially gain unauthorized access to a firms’ network.

<sup>5</sup> If an announcement is made on a day when the markets are closed, we consider the next day when the markets open as day 0.

<sup>6</sup> Day 1 is the day after the announcement.

<sup>7</sup> We also include a five day event window ( from day -2 to day 2) and a 3 day event window (from day 0 to day 2) separately in our analysis for comparison sake. For a five day event window, we use the estimation window from day -163 to day -3.

#### 4.1 Effect of Patch Availability, Disclosure Source and Discovery Source<sup>8</sup>

In this section, we test our remaining hypothesis, **H2-H4**, regarding the information content of the vulnerability disclosure announcement about what factors impact the cumulative abnormal returns of a vulnerability disclosure. Specifically, we pinpoint three characteristics namely, whether a patch is available, the source of disclosure and the discovery source. We measure our independent variables as follows; Patch = 0 if the vendor discloses a patch at the time of the announcement and 1 otherwise; Disclosure = 1 if the announcement is reported in industry sources like CERT and 0 if it is reported in popular press; Discovery = 1 if the vulnerability is discovered by the vendor itself and 0 if the vulnerability is first discovered by other firms like rivals or independent security analysts like eEye Digital Security. The descriptive statistics are:

Variable	Sub-type	Number (Percentage)
Disclosure	<i>CERT</i>	20 (17.5%)
	<i>Popular Press</i>	94 (82.5%)
Patch	<i>Patch Available</i>	87 (76.3%)
	<i>Patch Not Available</i>	27 (23.7%)
Discovery	<i>Self Discovery</i>	49 (43%)
	<i>Third Party Discovery</i>	65 (57%)

We develop the following regression model to test hypothesis H2 to H4.

$$CAR = \alpha_0 + \alpha_1 \cdot Patch + \alpha_2 \cdot Disclosure + \alpha_3 \cdot Discovery$$

The parameter estimates as well as the standard deviations and the t-value are given in the table below.

	Coefficient	Std Dev	t-value
<b>Patch</b>	-.0069	.0035	- 1.95
<b>Disclosure</b>	-.003	.0040	-0.72
<b>Discover</b>	.00115	.0030	0.38
<b>Constant</b>	-.0121	.0036	-3.32

This regression throws two interesting results: One, the non-availability of a patch at the time of disclosure significantly and negatively impacts the CAR. This is intuitive because if a firm does not release a patch at the time the discovery is made public, it gives hackers a chance to exploit the vulnerability to attack the firms' customers' IT resources and consequently the firm suffers a loss in customer goodwill and hence the future cash flows could be affected. Another interesting result is that the source of discovery does not significantly impact the CAR. This result is interesting because it suggests that the markets do not penalize vendors for failing to discover vulnerabilities in their own product. This could suggest a lack of effort on part of software vendors to invest in vulnerability discovery of their own products. This is also reflected in the fact that numerous third party firms like eEye Security, @Stake, DigiLabs are active in the market of discovering security vulnerabilities.

Our results corroborate prior analytical literature (Arora et al 2003) which showed that software vendors find it optimal to improve pre-launch quality but will under-invest in post launch bug-finding. By showing that the markets penalize a vendor if a bug is reported in its product, we can infer that vendors have high stakes in developing bug free software. But our second result, which shows that the market returns do not decline significantly more when third parties discover a flaw in a software product. Hence vendors might not have a strong incentive to invest in finding and reporting flaws in their own products. Currently, most independent security researchers find software bugs for free and hence software vendors are trying to push for legislation which forces the discoverer of the vulnerability to report to the vendor first so that the vendor has appropriate time to develop a patch for the product.

<sup>8</sup> For this section, we show our results only with a one day event window.

## 5. Conclusions

To the best of our knowledge, this is the first study to analyze the impact of product defects in the software industry. Unlike other industries, the software industry is perhaps the only one which has given rise to a parallel industry of small firms discovering and reporting flaws in other firms' products. We analyze the information content of the vulnerability disclosure classify vulnerabilities into various sub-types based on the source of the vulnerability disclosure, severity of the vulnerability, availability of a fix and source of vulnerability discovery.

Our results show that software vendors, on an average, lose about 0.76% market value when a vulnerability is disclosed. This has implications for software vendors to invest in improving the quality of their software. However, our model points at a possible under-investment in post launch quality improvements by the vendors. This is possibly an explanation of why there are numerous firms are in the business of discovering vulnerabilities in other vendors' software. Future analytical research could address the implications of this trend on consumer welfare.

By WISE 2004, we plan to extend this study to incorporate additional variables regarding the disclosure characteristics such as whether there were any known breaches due to the vulnerability or how severe the vulnerability is. We also plan to incorporate firm specific variables like firm size or degree of diversification as control variables.

## References

- Applewhite A (2004) 'Whose Bug Is It Anyway? The Battle over Handling Software Flaws' *IEEE Software*, **March/April 2004**, 94-97
- Arora, A., Caulkins, J.P. and R Telang, (2003). Provision of Software Quality in the Presence of Patching Technology, Carnegie Mellon University, working paper.
- Arora, A., Telang, R. and H Xu, (2004). 'Optimal Policy for Software Vulnerability Disclosure, Carnegie Mellon University, working paper.
- Campbell JY, Andrew WL and AC MacKinlay (1997) 'The Econometrics of Financial Markets' Princeton University Press
- Cavusoglu H, Mishra B and S Raghunathan (2002) 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' Working Paper
- Davidson WL III, DL Worrel (1992) 'The Effect of Product Recall Announcements on Shareholder Wealth' *Strategic Management Journal*, **13(6)**, 467-473
- Dolley J (1933) 'Characteristics and Procedure of Common Stock Split-Ups,' *Harvard Business Review*, 316-326
- Hendricks KB and Singhal VR (1996) 'Quality Awards and the Market Value of the Firm: An Empirical Investigation' *Management Science*, **42(2)**, 415-436
- Jarrel G and S Peltzman (1985) 'The Impact of Product Recalls on the Wealth of Sellers' *The Journal of Political Economy*, **93(1)**, 512-536
- Kannan K and R Telang (2004) 'Market for Software Vulnerabilities? Think Again.' Carnegie Mellon University, working paper.